sifma

INSIDER THREAT BEST PRACTICES GUIDE, 3rd EDITION

July 2024

TABLE OF CONTENTS

I. DISCLAIMER

This report was prepared to provide general guidance and assistance to organizations seeking to establish and implement an effective insider threat program within the financial services industry. Neither SIFMA or any of its members or any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process identified in this report or represents that its use would not infringe privately owned rights. This document shall not be construed as legal advice, and it is advised that the reader consult legal counsel when creating or maintaining an insider threat program. Whether and to what extent any organization adopts or implements any of the guidance or practices identified in this report is voluntary and dependent on the individual circumstances of the organization and its independent assessment of the considerations set forth in this report. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by SIFMA.

II. EXECUTIVE SUMMARY

Financial institutions have long been especially lucrative targets for insider attacks, but with the computerization of firm systems and assets, attacks can now be launched on a grander scale than ever before. Insider attacks on firms' electronic systems can result in financial and intellectual property theft, damaged or destroyed assets, and firm-wide disruption to internal systems and customer operations. Preventing and detecting attacks, however, has proven to be difficult, as insiders are often able to capitalize on their familiarity with firm systems to launch attacks without attracting notice. Further, the risk of unintentional insider incidents continues to increase as firms expand the number of personnel authorized to access sensitive information to meet business needs. At its core, an insider threat is just as much a human problem as it is a technological one. A systemized, targeted program is therefore necessary to combat insider threat risks.

The purpose of this report is threefold: (1) to assist financial firms in developing effective insider threat programs by identifying and discussing best practices that firms may choose to consider for voluntary adoption; (2) to help financial firms measure their insider threat program's effectiveness; and (3) to act as a reference for regulators to better understand the insider threat at financial institutions.

The Insider Threat Best Practices Guide was last published in 2018, but over the past several years, there have been significant developments warranting an updated edition. In particular, the report has been updated to reflect the changing insider threat landscape, including advancements in the use of anomaly detection, artificial intelligence, and big data techniques, evolving privacy issues including restrictions on employee surveillance and profiling, the use of automated decision making, and legal and practical barriers to performing employee background checks.

The voluntary practices identified in this report represent the financial industry's effort to be proactive in identifying what can be done to combat the increased risk of insider threats at financial institutions, and many of the best practices go beyond existing regulatory requirements. Nevertheless, as regulators continue to focus on cybersecurity and privacy at financial institutions, firms should continually monitor regulatory requirements and obtain legal advice regarding compliance with relevant regulations.

The core components of an insider threat protection program mirror those denoted in the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.[1] This structure encourages firms to individually assess threats most relevant to their firm and to develop a risk-based approach to resource allocation. The structure is also flexible enough to allow firms to scale implementation based on their firm's risk appetite, business models and available resources.

However, unlike cybersecurity programs, every component in an insider threat program must factor in

[1] https://www.nist.gov/cyberframework

human behavioral elements. While external cybersecurity threats can often be prevented or detected primarily through technical tools, those technical tools are insufficient to prevent many insider threats. In many cases, the only signals of an impending insider attack are commonly exhibited human behaviors that foreshadow the attacker's intent. An appropriately trained insider threat protection team leverages technical tools, such as network and desktop monitoring software to detect and investigate suspicious insider behavior—but those tools will often be useless without the training, counterintelligence skills, and guidance to use them properly. While all personnel in a firm have a role in maintaining an effective insider threat program, an insider threat protection team is essential to coordinate firm-wide prevention efforts and alert relevant personnel to suspected or detected threats. Effective practices for insider threat protection therefore involve both technical cybersecurity defenses, which typically reside within information technology, and human expertise, that resides across the firm.

While sophisticated monitoring tools and personnel screening techniques are critical to ensuring the effectiveness of an insider threat protection program, such tools and techniques are also accompanied by their own legal risks. Privacy and employment laws in the United States are generally permissive of employers' efforts to protect their assets, but electronic communications privacy laws and background check restrictions at the state and federal level impose some procedural hurdles. International laws, particularly in the European Union, are more restrictive, and in some cases may prohibit employers from taking some of the insider threat precautions recommended herein. Firms should therefore use the framework within this document as a reference while consulting with counsel to develop and implement an insider threat program that is effective and in compliance with applicable laws.

SUMMARY OF RECOMMENDED PRACTICES

Our research and work with members identified the following non-exhaustive list of practices that organizations can consider adopting as part of an effective insider threat program. This non-exhaustive list is intended to provide a framework for policies and practices that organizations may consider in developing and maintaining a program that best meets their individual circumstances. Organizations should only implement policies and practices that are appropriate for their respective firms and adhere to local, state, and federal guidance, as well as the board of directors and executive management to provide oversight of the insider threat program. In addition, some of these voluntary recommended practices can be implemented within the enterprise, rather than specifically as part of a separate insider threat program.

- Organize a cross-functional insider threat team with participation from Human Resources, Internal Audit, Privacy, Legal, Risk and Compliance, Supply Chain and Third-Party Risk Management, etc.
- An effective insider threat program will focus on deterrence, not just detection and is not designed to solely be a policy compliance function.
- Develop an insider risk protection strategy that considers the three key variables of (1) criticality, (2) vulnerability, and (3) source of potential threats.
- Develop criteria for anomalous behavior that focus the firm's insider threat program on intentional and unintentional insider threats.
- Develop robust policies that address insider threat risk with corresponding training and awareness programs for all personnel.
- Establish and enforce an effective cross-functional plan for managing incidents.
- Choose a risk-based framework and identify key metrics that can be used to assess the insider threat program, such as the NIST Cybersecurity Framework.
- Utilize technical tools, including network monitoring software, identity, and access management controls,

and data loss prevention tools to monitor employee behavior on firm networks and consider use of artificial intelligence and machine learning applications to identify or warn of insider threat risks.

- Do not rely exclusively on technology solutions; combine technical tools with human input, analysis, and intelligence to interpret technical data and identify anomalous insider behavior.
- Identify and scope relevant applicable Legal and Privacy requirements related to implementing an insider threat program and ensure that all insider program activities comply with applicable laws, rules, and regulations.
- Under advice from counsel and in compliance with applicable law (including the Fair Credit Reporting Act), conduct regular risk-based background checks on employees with access to financial accounts, highly sensitive or confidential information, or critical firm information systems.
- Ensure appropriate employee onboarding and termination procedures are developed and maintained.
- Develop appropriate due process and fairness procedures for disciplinary actions against employees to maintain morale, mitigate potential bad acts in response to disciplinary actions, and deter disgruntled insiders.
- Use robust identity and access management tools to ensure user access is appropriate for the employee's role.
- Stay abreast of industry trends and emerging insider threat tactics.

III. INTRODUCTION

Insider threats can be categorized in several groups from accidental, negligent, compromised, and malicious. One should consider motivation and intent along with capability and access when assessing a potential insider threat. Although the vast majority of insider risk activities are due to accidents or negligence, there are malicious insiders who are determined to steal sensitive information from the company or cause harm in other ways. Detection can be difficult as an insider's actions may appear legitimate on the surface.

According to the 2023 Ponemon Cost of Insider Threats Global Reports[2], insider incidents rose over 44% since 2020. Insiders are current or former employees, contractors and third parties who have authorized access to a company's most sensitive information.

The February 2024 updated set of NIST controls[3] are still insufficient in today's workplace. This is due to several factors, from an entrenched post-pandemic remote workforce, increased workloads that can lead to accidental disclosures of confidential information, to emerging technologies that are making it increasingly difficult to detect phishing, credential theft or data exfiltration.

Understanding the risks posed by a company's culture, control strength and ability to detect and thwart an insider threat is paramount to protecting a company's people and information. SIFMA recognizes companies' programs may have different maturity levels. The graphic below from DHS CISA outlines a set of standards firms can adopt to help build a robust insider threat program.

The SIFMA Insider Threat Best Practices Guide takes this into account and provides ideas and lessons learned from SIFMA members and external organizations focused on this topic (e.g., CERT Common Sense Guide to Mitigating Insider Threats[4], MITRE Insider Threat Framework[5], DOJ/FBI National Insider Threat Task Force (NITTF) Best Practices[6] et al) to help jumpstart and mature a program based on industry recommendations and lessons learned.

Source: Cybersecurity and Infrastructure Security Agency (CISA)

[2] Cost Of Insider Risks Global Report — 2023 | Ponemon-Sullivan Privacy Report (ponemonsullivanreport.com)
[3] https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
[4] New Edition of Common Sense Guide to Mitigating Insider Threats Released (cmu.edu)
[5] Insider Threat Framework Initiative | MITRE Insider Threat Research & Solutions
[6] National Insider Threat Task Force (NITTF) (dni.gov)

IV. WHERE TO BEGIN

A company's risk appetite is a crucial factor to consider when designing and implementing an effective insider threat program. How risk appetite influences the development of such a program includes:

1. RISK TOLERANCE LEVELS

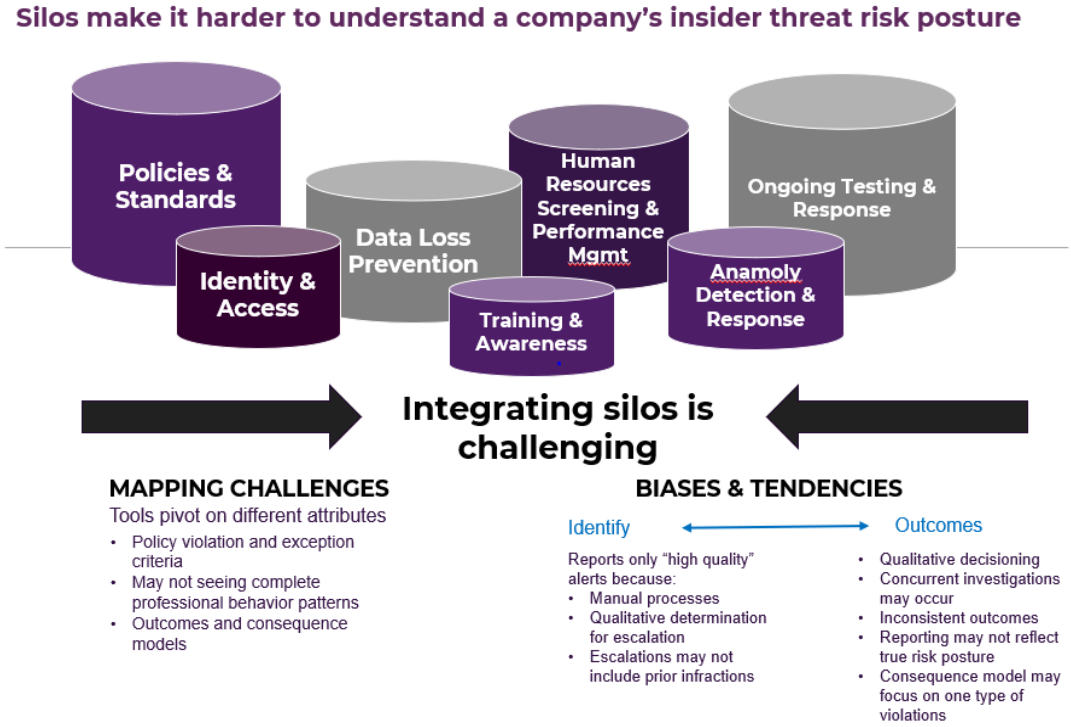
This defines tolerance for various risks, including those posed by insider threats. Organizations with a lower risk tolerance will invest more resources in preventing and mitigating insider risks while those with a higher tolerance may accept some level of risk as a cost of doing business and competitiveness.

2. CULTURE AND HUMAN CAPITAL MANAGEMENT

A company should consider cultural aspects, such as how it manages staff turnover, lay-offs and furloughs which can turn a trusted insider into a disgruntled and malicious employee.

Another consideration is how a company monitors its employees and contractors. Transparency is essential when a company decides to monitor badge access, keystrokes, and other monitoring capabilities in the workplace. According to CurrentWare[7], a lack of transparency and misuse of this information can contribute to negative perceptions by employees and could lead to disgruntlement. How a company views its employees' privacy while at work is also a crucial point to think about when building the program.

Another challenge is how companies integrate silos, whether cultural or due to multiple mergers and acquisitions. Breaking down the silos is an essential element to drive a program's success.



[7] CurrentWare Suite—PC Monitoring, DLP & Web Filtering Software

3. Resource Allocations

The company's risk appetite and budget will determine how it allocates resources to its Insider Threat program. Organizations with a low-risk appetite are more likely to allocate a larger budget, employ specialized personnel and implement advanced technologies to detect and protect its information and resources.

4. Program Scope

Risk appetite will influence the scope and speed of implementation of an insider threat program. Companies may have traditionally focused on external threat actors, while those with a lower risk appetite recognize the importance of addressing internal threat actors and will support and expand the program to encompass a broader range of insider risk factors.

5. Policy Development and Enforcement

Risk appetite will guide the development and enforcement of policies and standards that support the insider threat program. This includes Acceptable Use, Access Controls, Data Loss Prevention (DLP) controls as well as a consequence model for insider misconduct. In contrast, a company with a higher risk appetite may have less restrictive policies and standards.

6. Data Protection Requirements

Many traditional insider threat programs originated in a company's DLP program. Those with a low-risk appetite will ensure data is properly classified and restrict access rigorously while continually assessing the DLP policies based on insider activity, while those with a higher tolerance may adopt a more flexible mode of work.

7. Third (and fourth) Party Relationships

Companies with a minimal risk tolerance may choose their vendors and partners based on a shared risk profile and willingness to share insider threat results and effective practices with each other to continually strengthen the protection of information.

8. Regulatory Compliance

An industry's compliance requirements with law, rules and regulations tend to intersect with a company's risk appetite. Those industries, such as financial services, are more likely to adopt a strict compliance regimen to meet regulations and to ensure customer confidence.

A company's risk appetite is a critical factor when tailoring an insider threat program. Specific needs and objectives will align the program with the company's objectives and how the company will detect, mitigate, and prevent insider threats in a manner consistent with the company's strategic goals and risk tolerance.

It is important to note insider threat programs are not 'one size fits all.' Some companies have a large international footprint; others are U.S.-based only. A company may have a large remote workforce, while another requires all employees return to a specified workplace. One organization may have a stringent consequence model while another may focus on continual education. One must consider the individual needs of the company while building an insider threat program.

V. CLASSIFYING INSIDER THREATS

The most serious insider threats in the information age—and those that firms should prioritize and invest the most resources to prevent—involve individuals who misuse their access to systems, networks, and information in a manner that compromises the confidentiality, integrity, functionality, reliability or availability of those systems, networks, or information. The results of inadequate protections can be loss, alteration, or destruction of a firm's operational capabilities, as well as material loss of customer data, business records or intellectual property. These potential losses should be taken into account and explained when making a business case for investing in the development an insider threat prevention program.

Despite their technical modality, insider threats are, at their core, a human issue. Cybersecurity defenses focused on monitoring employee activities may prevent some attacks from causing significant harm to an organization, but human intelligence, monitoring, effective personnel controls, and good management oversight are necessary to identify the potential warning signs of insider activity, the appropriate method to intervene before an attack occurs, and the most efficient way to mitigate the effects if an attack does take place. An effective insider threat program, therefore, uses both cybersecurity defenses and designate-personnel to detect and contain insiders who pose a risk to the firm while mitigating the risk through administrative, investigative, technical, disciplinary, and legal safeguards. However, even with the most advanced detection tools, a motivated and sophisticated insider can bypass detection and controls. Hence, education is one of the most valuable insider threat prevention tactics an organization can use, a topic covered later in this paper.

WHO ARE THE INSIDERS?

There are various categories of "insiders." An insider can be defined as any individual (including current or former employees, contractors, or business partners) with the authorized ability to access an organization's internal systems and resources. The CERT Insider Threat Center at Carnegie Mellon University defines a "malicious insider" as an insider who (1) has or had authorized access to an organization's network, systems, or data, and (2) has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

Financial institutions must also consider potential negative reputational effects and regulatory compliance risks posed by insider threats. Not all insider threats stem from malicious motives or intentional actions. In some cases, insiders may unintentionally or negligently cause serious harm to the confidentiality, integrity, or availability of an organization's information or information systems by failing to adhere to firm policies or prudent information technology practices. The most common culprit is the negligent or accidental insider. According to the 2023 DTEX/Ponemon Cost of Insider Risks Global Report, 55% of incidents experienced by organizations represented in this research were due to employee negligence and the average annual incident remediation cost was $7.2 million. Not as frequent are incidents involving criminal or malicious insiders (25% of incidents) and credential theft (20% of incidents). However, the average cost per these incidents is more costly at $701,500 and $679,621, respectively. As shown in this research, the cost of insider risk varies significantly based on the type of incident. The activities that drive costs are monitoring & surveillance, investigation, escalation, incident response, containment, ex-post analysis and remediation.

The CERT Common Sense Guide to Mitigating Insider Threats (7th Ed.)[8] indicates that unintentional insider threats come in four main classes: accidental disclosure, phishing or social engineering, physical records disclosure, and lost, discarded, or stolen portable equipment. One of the goals of this report is to augment CERT recommendations with financial services-specific best practices. Financial firms seeking to implement best practices should ensure that their insider threat program covers unintentional threats as well as malicious ones. According to the SIFMA Benchmarking Survey, approximately 90% of responding firms reported that their insider threat programs account for "accidental" insider threats, although the methods for handling insider

[8] Common Sense Guide to Mitigating Insider Threats, Seventh Edition (cmu.edu)

threat investigations and ensuring appropriate employee accountability varied among firms.

Individuals who have intentionally carried out insider attacks tend to have one of several common motivations. Financial gain has always been a leading motivator, made increasingly appealing by digitized systems that lend themselves to the theft of vast quantities of customer data or intellectual property ("IP") assets to aid larger fraud schemes such as corporate or nation-state espionage to further ideological or political beliefs. Some insiders may be motivated by malice against employers or a desire to seek revenge by disrupting, undermining, or destroying company systems. Still others work on behalf of other entities, seeking to steal or destroy data to help the entity gain a competitive advantage or to harm the victim company's interests or reputation.

A number of studies have noted that perpetrators of malicious insider attacks share common characteristics. For instance, certain categories of employees (such as recent hires, contractors, paralegals, interns, and temporary employees) have been shown to be correlated with a higher risk of insider threat based on the nature of their position, the level of supervision over their work, or their access to confidential information. Behavioral characteristics can also help to predict potential insider threats. One survey of more than 500 executives of businesses, law enforcement, and government agencies indicated that insiders who had perpetrated cybercrimes most often displayed behaviors such as violation of IT policies, disruptive behavior, and poor performance reviews. Another study found that 80% of insiders who stole confidential or proprietary information were male, and over half of such insiders held technical positions.

A 2022 Ponemon study of 1,004 global IT security practitioners[9] found that malicious insiders use corporate email to steal sensitive data. 74% of respondents say malicious insiders emailed sensitive data to outside parties followed by scanning for open ports and vulnerabilities (62% of respondents) and accessing sensitive data not associated with the role or function (60% of respondents). To detect warning signs such as privilege abuse, firms have begun to implement analytical tools that log behavioral modeling.

Numerous academic studies have attempted to identify the psychological traits prevalent in insider threat incidents. Nevertheless, psychological, demographic, and occupational characteristics do not easily translate into a set of rules that can be applied to discover and predict insider attacks, and the relationship between such characteristics and unintentional insider threats is even more difficult to measure. Moreover, using such traits to profile insiders carries some degree of legal risk, particularly in EU member states where automated decision-making based on such profiles may be restricted; and firms must be careful to avoid illegal discrimination or disparate treatment of certain groups of employees when creating an insider threat profile. Therefore, firms should carefully weigh the legal risks of this type of profiling against its potential benefits before adopting it as a practice in their insider threat protection programs. Indeed, almost all efforts to identify and deter insiders from engaging in malicious activities will involve substantial legal issues, as well as considerations of company morale. Companies should be well- informed about profile trends of insider threat actors—but the bottom line is that an employee can become an insider threat, whether maliciously or unintentionally, from an almost infinite variety of backgrounds or starting points.

Verizon's 2023 Data Breach Investigation Report[10] showed that 74% of all breaches include human error by way of privilege misuse, use of stolen credentials or social engineering. 83% of breaches involved external actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches. IBM's 2023 Cost of a Data Breach Report [11] found that the average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% The average cost has increased 15.3% from USD 3.86 million in the 2020 report

[9] pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf (proofpoint.com)
[10] 2023 Data Breach Investigations Report | Verizon
[11] Cost of a data breach 2023 | IBM

ACCIDENTAL INSIDER THREATS

Accidental insider threats, also/ referred to as unintentional insider threats, refer to individuals within an organization who inadvertently, or due to lack of awareness, pose a security risk due to their actions, often without any malicious intent. These incidents typically result from human error or lack of awareness of a company's policies, standards, and procedures. Most company's acceptable use policies are designed with the accidental insider in mind.

Accidental insider threats can be classified into several categories:

1. **Data Mishandling**
   - Data Leakage: Employees may unintentionally leak sensitive information by sending emails to the wrong recipient(s), losing or misplacing physical documents, or sharing confidential files on public cloud storage.
   - Data Loss: Accidental deletion of critical data, either through misunderstanding or negligence, can lead to data loss incidents. Inappropriate storage of confidential information is also a common theme for accidental data loss or exposure.

2. **Phishing and Social Engineering**
   - Employees falling victim to phishing frauds or social engineering attacks can inadvertently compromise security by clicking on malicious links or downloading malware. This area will continue to become increasingly difficult to detect with the advent of Generative AI and deepfakes.

3. **Technology Misconfiguration**
   - Incorrectly configuring software, systems, or cloud services can create vulnerabilities. Accidental insider threats may unintentionally expose sensitive data or grant unauthorized access to systems due to misconfigurations. As more companies move to Software as a Service (SaaS) and other cloud services, misconfiguration will pose a particularly significant threat.

4. **Unintentional Insider Attacks**
   - Employees may inadvertently initiate security incidents while performing their job duties. For example, a system administrator might apply a software update without realizing it introduces a security risk/vulnerability.

5. **Unauthorized Access**
   - Employees may access data or systems without realizing they lack proper authorization, inadvertently violating security policies.
   - Managers may not, as a matter of practice, regularly review their teams' access to sensitive and confidential data and determine if access is still needed for the specific function.
   - Employees who are promoted or move to another department may retain legacy access to sensitive information that is no longer required for their new function.

6. **Poor Password Hygiene/Practices**
   - Weak or easily guessable passwords, reused across multiple accounts, can lead to unauthorized access when employees fall victim to credential stuffing attacks. This includes retaining the original password from a system (e.g., Password123).

7. **Failure to Follow Security Protocols**
   - Not adhering to established security protocols and procedures, such as bypassing multi-factor authentication or ignoring password complexity requirements, can inadvertently weaken an organization's security posture.

8. **Unencrypted Devices**
   - Storing sensitive data on unencrypted devices, such as laptops or USB drives, can result in accidental data exposure if the device is lost or stolen.

9. **Lack of Security Awareness and Training**
   - Employees who lack awareness of cybersecurity best practices may unknowingly engage in risky behavior, such as clicking on suspicious links, downloading unverified software, or sharing login credentials. Leaving workstations unattended without locking them can allow unauthorized individuals to access sensitive data or systems.
   - To address accidental insider threats, organizations should focus on comprehensive security awareness training, ongoing education, and the implementation of technical controls that can help mitigate the risks associated with human error. Encouraging a culture of cybersecurity awareness and providing clear guidelines and policies for data handling and system use can significantly reduce the likelihood of accidental insider threat incidents.

NEGLIGENT INSIDER THREATS

Like accidental insiders, a negligent insider poses risks based on one's lack of awareness or compliance with security policies. Negligent insiders may have a better understanding of a company's security protocols, but be careless in following them, or choose not to follow them at all. They may not understand why a security requirement exists, e.g., a company not allowing piggybacking into a building, or dismiss the requirement as trivial. While not malicious, these actions may be considered more willful or deliberate.

The key distinction is that "negligent" implies a degree of carelessness or disregard for protecting company information, systems, and people. A negligent insider does not always possess malicious motivation but may pose a security risk due to their lack of due diligence and discipline.

Examples of negligent insider threats include:

1. Human Error

- This often results from simple mistakes, such as emailing a confidential spreadsheet to the wrong recipient or misclassifying information.
- Allowing unknown resources to 'piggyback' into a building.

2. Data Mishandling

- Like an accidental insider, a negligent insider may neglect to follow security protocols, whether through carelessness or ignorance of company policies. Examples may include leaving confidential information on a company printer for an extended period or placing sensitive documents in a general trash receptable instead of a designated shredding receptacle.

3. Unsafe Online Behavior

- Engaging in risk online behavior, such as downloading unauthorized software, visiting suspicious websites, or sharing sensitive information online are examples of negligent insider risks.

COMPROMISED INSIDER THREATS

A compromised insider is an individual within an organization whose account, or access credentials, have been compromised by external threat actors. These individuals, unlike malicious insiders who act with motivation and intent, have become unwitting tools of malicious threat actors due to a variety of security breaches. Examples of a compromised insider are:

1. Unintentional Involvement

Compromised insiders do not willingly participate in any malicious activity. Involvement is entirely unintentional and often, without knowledge or consent.

2. External Manipulation

An individual's account or access credentials are typically accessed and manipulated by external threat actors. This includes hackers, cybercriminals, or organized crime. This example can also include geopolitical organizations. These actors tend to exploit vulnerabilities to gain unauthorized access. Methods include social engineering, not only through phishing to social engineering on social media sites or via conferences or other outside activities. The threat actor may be patient and take time to make the compromised insider feel

comfortable before asking for sensitive information.

A compromised insider's involvement is entirely unintentional, and they become instruments of malicious and threat actors due to compromise of their credentials.

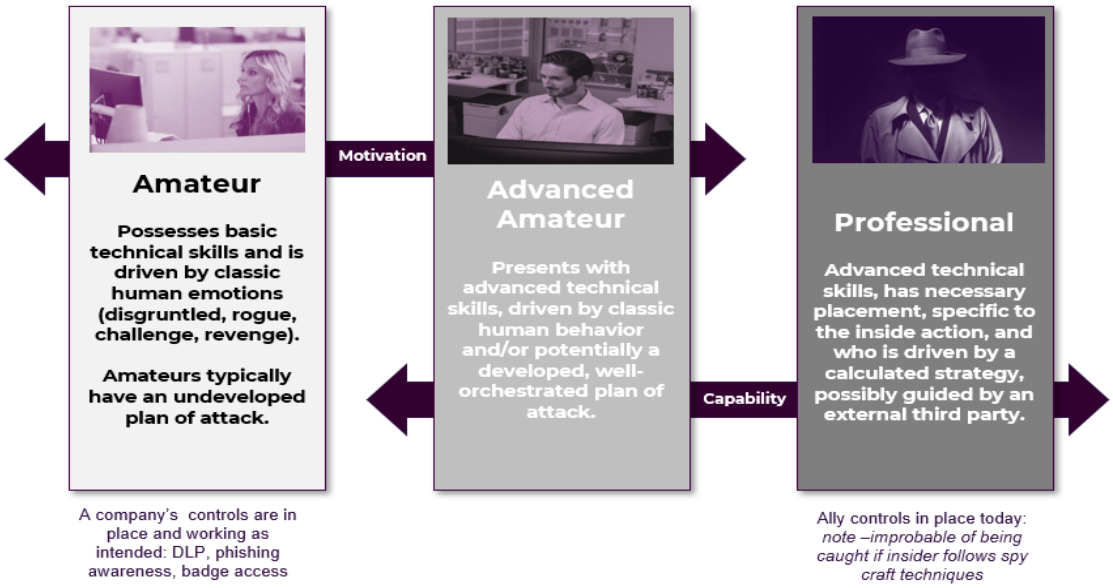
Malicious Insider Threats

While most insider threats are due to accidents or negligence, there are bad actors who specifically desire and intend to cause harm or steal a company's assets. These risks may be unique due to difficulty in detection due to the insider's authorized access that may look like legitimate activity. An insider threat program should consider an employee's motivation and capability when assessing if an insider threat activity is malicious.

A company may classify malicious insiders as amateur, advanced amateur and professional. The amateur is described as someone without a coordinated plan of attack but is motivated to cause harm. This motivation may be sporadic and not thought out, such as during a lay-off or frustration. A company's set of controls is typically built to detect malicious amateurs.

An advanced amateur may be more technically proficient, more socially aware of where controls could be bypassed or avoided and develop a coordinated plan of attack. Edward Snowden's actions could be considered advanced amateur due to his role, his social engineering success in getting colleagues to provide him with additional access, and a motivation to get information outside the network. Detection may be more difficult. There are tools now that focus on user behavior analytics that are beginning to highlight advanced amateurs' actions against their peer groups.

Finally, the professional insider has employment/placement within a company and may be driven by a planned and calculated strategy. The professional insider may be coached by an external third party and may not understand or know the full breadth of the information being exfiltrated and how it will be sold or used.



Courtesy of Bank of America

Summary

In short, although there are several types of insider threats, a company is responsible for its strategy, and successful execution of that strategy, to prevent, detect, and respond to these types of security risks to protect data and systems.

VI. INSIDER THREAT RISK LANDSCAPE

The following describes the evolving risk landscape faced by insider threat teams, especially given the post-pandemic shift to work from home environments and the use AI-powered attacks.

1. Remote Work

The continued prevalence of remote work can lead to increased insider threat risks. Employees working from home may have decreased security measures in place, making it easier for malicious insiders to access sensitive data without detection. Some companies have experienced dual employment issues as well as proxy interviews from remote workers.

2. Phishing, Smishing, Vishing and Credential Theft

Cybercriminals are becoming more sophisticated in their attacks, aiming to steal employee credentials. Insiders or external threat actors can then use these stolen credentials to access corporate systems with minimal detection. Malicious actors may time these late in the evening when an employee is checking a mobile device (but not the URL) or during a particularly busy time for the function.

3. AI-Powered Attacks

The use of artificial intelligence (AI) in cyberattacks is growing. Malicious insiders may leverage AI to automate and optimize their attacks, making them more difficult to detect and defend against. With the rapid advent of generative AI, the ability to detect a deepfake is becoming more difficult and could lead to compromise of a company's critical assets.

4. Supply Chain and Vendor Risks

Third-party vendors and suppliers may have access to an organization's systems and data. If these vendors have insiders who are compromised, it can lead to insider threats originating from external sources.

5. Insider Trading and Financial Fraud

In financial institutions, insider threats related to insider trading and financial fraud remain a concern. Employees with access to sensitive financial data may exploit their knowledge for personal gain.

6. Misconfigured Cloud Services

As organizations increasingly migrate to cloud environments, misconfigured access controls and inadequate security configurations can result in insider threats from accidental data exposure, or data leaks.

7. Workforce Changes

Staff turnover, layoffs, and furloughs can result in disenchanted employees who may be more inclined to engage in malicious insider activities or inadvertently expose data. If a company is forced to reduce its workforce, consideration should be given to whether impacted employees retain elevated or privileged access after announcement of termination.

8. **Personal Devices in the Workplace**

The use of personal devices for work purposes, known as Bring Your Own Device (BYOD), can introduce security vulnerabilities if not responsibly managed. Insiders may inadvertently or intentionally compromise sensitive data on personal devices as well as not maintain patches or updates.

9. **Social Engineering and Manipulation**

Insiders can be manipulated or coerced by external threat actors into conducting malicious activities. Social engineering tactics, such as extortion or impersonation, can play a significant role in these insider threats. It is important to remember that anyone at any level could be susceptible to being socially engineered.

10. **Detection Challenges**

Detecting insider threats can be challenging, as many activities may appear legitimate or take place in the normal course of business. The use of advanced analytics and behavioral monitoring is crucial but requires continuous refinement and adaptation to evolving threats as well as privacy considerations.

11. **Compliance and Regulatory Risks**

Non-compliance with data protection regulations can result in legal consequences for organizations. Insiders may inadvertently or intentionally violate these regulations, leading to legal and financial penalties. To mitigate these concerns, organizations must invest in comprehensive insider threat detection and prevention programs. This includes implementing robust access controls that are monitored and maintained, continuous monitoring, security awareness training, and fostering a culture of security throughout the workforce. Additionally, staying informed about emerging threats and adapting security strategies accordingly is essential in the ever-evolving landscape of insider threats.

VII. INSIDER THREAT AND ARTIFICIAL INTELLIGENCE

Generative AI (Gen AI) is a technological development that became more prevalent starting in the fall of 2022. Since that time, companies have rapidly adopted the power of using Gen AI in addition to the already established AI forms of machine learning and natural language processing. With Gen AI, however, the ability to create something malicious has become easier, thus making it increasingly difficult for security organizations to detect as well as stay current with controls and detection techniques.

The malicious use of AI-generated deepfakes is a significant concern. Threat actors can create highly convincing videos or audio recordings to impersonate individuals, potentially causing reputational damage or disseminating false information. Examples of how AI could be used to deceive an insider include the following:

1. **Social Engineering Attacks**

   Deepfake technology can be employed in social engineering attacks to manipulate employees, partners, or customers. Malicious actors may use deepfake personas to trick individuals into revealing sensitive information or performing actions that compromise security.

2. **Phishing and Credential Theft**

   Deepfakes can be used to enhance phishing campaigns. An attacker might impersonate a trusted individual within an organization through a convincing video message, prompting recipients to disclose login credentials or other sensitive data.

3. **Corporate Espionage**

   Deepfake technology could be exploited by insiders or external entities to steal sensitive corporate information or trade secrets. Using deepfakes, they can impersonate company executives or employees to gain unauthorized access.

4. **Legal and Ethical Dilemmas**

   The rise of deepfakes raises complex legal and ethical questions. Determining the authenticity of digital content becomes more challenging, and legislation has struggled to keep up with the rapid advancement of AI and deepfake technology.

VIII. CREATING A SECURITY AWARE CULTURE

Creating a "security aware" culture within a company is critical when developing an insider threat program. Educating employees and contractors on clear expectations of acceptable use, proper access management routines and data access, combined with an open door of "see something, say something," with no fear of retribution is key. Technology is rapidly evolving and with it, insider threat tactics and opportunities. Most insider risks are due to accidents or negligence. Understanding how to detect and prevent the several types of insider risks will bolster a company's security posture and create a culture of trust and transparency.

Losses and damage caused by "insiders," such as employees, contractors, and others authorized to access business information and systems have long been a problem for businesses in virtually every industry. Recent estimates show that the costs related to resolving insider threat activity are increasing and can be substantial. According to the Ponemon 2022 Cost of Insider Threats Benchmark Study, the financial services sector ranked highest in terms of total annualized costs associated with insider threats at approximately $21.3 million per company.

High profile incidents in the financial sector have shown that even the most secure organizations can face devastating losses caused by a knowledgeable and motivated insider who is not contained by adequate internal safeguards or sufficiently rigorous administrative standards and expectations. For example, in one incident, operations personnel at a sophisticated financial services firm used their access privileges to embezzle client funds after securing employment using faked names and identification. In another incident, a financial adviser transferred confidential information from over 500,000 client accounts to his personal computer, which was subsequently hacked, resulting in the disclosure of confidential information for thousands of firm clients.

Historically, insider activities at financial institutions most often involved employees who abused their access privileges or committed fraud to steal funds from customer accounts or the firm. However, because firms' operations and assets have been so thoroughly computerized, insider attacks on systems and networks are now a significantly greater threat than seen in the past, threatening significant disruptions to business operations and theft of trade secrets on top of the risks to customer and firm financial assets. Further, the expanding use of service providers by financial institutions to perform key operations or store sensitive data widens the playing field for potential bad actors. Financial firms have responded to the increasing insider threat.

RISK MANAGEMENT

Risk management is a critical process in every financial institution and can be leveraged in many contexts throughout an organization. To best comprehend risk management, it is worth identifying how it is defined and intersects with insider threats. Risk is commonly defined as the probability of loss or damage.[12] As illustrated in the Department of Defense Risk Model shown at right, risk management involves the intersection of three factors: criticality, vulnerability, and threat. "Criticality" can be defined as the quality of being of decisive importance with respect to an outcome. "Vulnerability" is the capability of or susceptibility to being compromised, exploited, damaged, or destroyed. "Threat" identifies who or what intends to take advantage of a particular vulnerability and what means they have to do so.

While an optimal risk management plan will account for all three of factors mentioned above, firms should particularly focus on areas where at least two of these factors overlap (segments 4, 6 and 7 as shown)

Therefore, the strategy for mitigating insider threat should:

- Take into account each of the factors in the risk model segment and their interaction therein as illustrated in the accompanying figure.
- Consider the content of and relationships among the risk model segments illustrated.
- Address the areas where at least two of the risk model segments (criticality, vulnerability, and threat) overlap.
- Ensure that there is a focus on reducing the number of vulnerabilities, especially those that are identified as part of a critical asset.
- Be mindful that how the firm defines criticality, vulnerability, and threat may be subject to change as the firm and the nature of the threats it faces continue to evolve. These elements must be reevaluated often, especially during disruptive operations or crisis situations.

RISK MODEL

1 Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure.

2 Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure.

3 Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information).

4 Critical assets for which there are known vulnerabilities, but no known threat exposure.

5 Critical assets for which there are known vulnerabilities and threat exposure.

6 Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability.

7 Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

Department of Defense Risk Model.

[12] CITE definition source.

Part of risk management must also be the measurement and weighing of relative costs and benefits. Implementation of many of the recommendations in this report almost invariably places additional constraints on users or systems. Such constraints may well negatively impact productivity. A serious cost/ benefit analysis must be done, weighing potential safety/security benefits against personal and organizational impacts. This analysis, however, is difficult; the "benefit" of security can be somewhat intangible or difficult to measure, as is the "cost" to personnel and organizations. Organizations should consider carefully how to conduct an effective and useful cost/benefit analysis of information security as part of an overall risk management strategy, taking into account the factors unique to their business.

Given the role of insider threat programs in overall risk management and the importance of employee cooperation with an insider threat program, firms should develop policies to address insider threat risk and set forth the responsibilities of employees with respect to the insider threat program.

IX. INSIDER THREAT INVESTIGATIVE CHALLENGES

Surveys of insider case studies reveal that individuals' concrete behaviors, rather than their demographic or psychological characteristics, are often the best indicators of their risk of being an insider threat. Suspicious behaviors can manifest themselves both as network security violations (e.g., failed log in attempts, downloading large amounts of data, altering coding on sensitive files) and as personnel issues (e.g., disputes with co-workers or superiors, threats, chronic absenteeism). Recent studies of insider threats further demonstrate that certain situational or environmental factors affecting the business may increase the likelihood of an insider attack. For example, businesses undergoing a merger, acquisition, or significant reorganization may have a higher proportion of employees that are disgruntled, stressed, or otherwise prone to destructive behavior due to uncertainty about their own future or a perceived lack of organizational control. Businesses that operate in different countries or employees from different cultural backgrounds must also be particularly vigilant about the way in which cultural differences may increase by risk of miscommunication and failure to identify the signs of a potential insider threat.

To monitor activities or behaviors that may signal an insider threat, firms should use both technical tools and human intelligence. Firms should utilize network monitoring software, appropriate identity and access management controls, and data loss prevention tools. Firms should also consider the use of artificial intelligence applications to identify or warn of insider threat risks and adopt confidential reporting mechanisms for employees and supervisors to report suspicious activity. Network monitoring software, artificial intelligence programs, and data loss prevention solutions are critical tools for detecting internal and external cyber threats and stemming the flow of information out of the business, but they are useful only to the extent that relevant staff can properly interpret the functions they perform and the data they generate. With new technologies, however, comes new opportunities to cause harm to a company's reputation or operations. For example, the use of AI provides an opportunity for insiders to poison a large language model or intentionally input malicious information for a different outcome or output. Identity and access management controls, even when fully automated, require prompt follow-through on the part of relevant personnel to ensure that access privileges are revoked for former employees or malicious insiders. Additionally, some policies (such as prohibiting the use of USBs or other external storage devices or limiting the number of individuals with systems administrator credentials) may require temporary exceptions for business reasons that must be closely monitored by the insider threat team to ensure that the exceptions are not abused.

Firms should establish criteria for anomalous behavior that focuses their insider threat program on intentional and unintentional insider threats. To decide what kinds of network patterns are anomalous and therefore potentially suspicious, the firm must first establish a network, applications, and data usage activity baseline. An individual familiar with the company's network usage should observe network activity over a given period of time and document all relevant data points, which may include communications between devices within the firm, virtual private network (VPN) users, ports and protocols, firewall alerts, printing activity, and bandwidth usage. Once a baseline is established and monitoring software is implemented, designated members of the insider threat team should monitor the network for anomalous activity, such as unfamiliar IP addresses attempting to access the network, unusually large data transfers, failed log-in attempts, large printing jobs or data transfers of privileged files. If a team member identifies anomalous activity, he or she should first investigate to see whether a legitimate explanation for the activity exists (e.g., forgotten passwords or training activities requiring printing of privileged materials). If no legitimate explanation is discovered, the team member should consult with the full insider threat team to discuss whether further monitoring or an expansion of the investigation is warranted. At this stage of the investigation, the employee and his or her manager should not be engaged or made aware of the investigation.

While an insider threat team can rely on software to monitor network activity in real time, it must rely on the firm's employees (managers and co-workers) to continuously monitor for personnel issues that may signal an

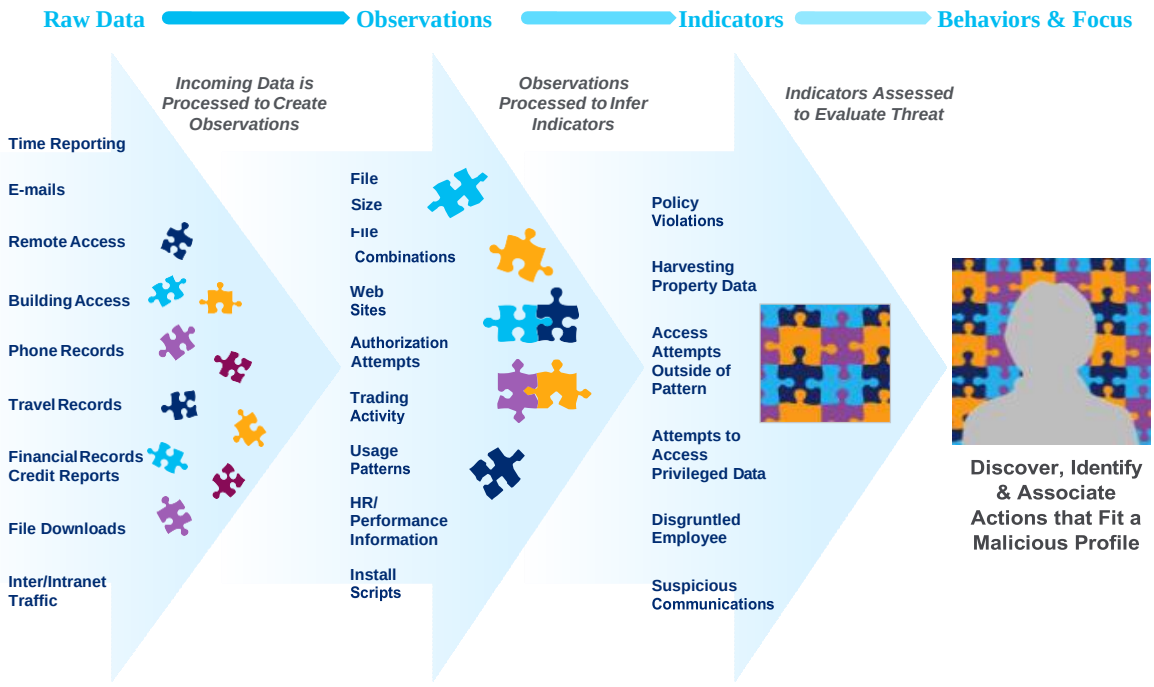
insider threat risk. Firms should therefore develop policies that address insider threat risk and corresponding training and awareness programs for all personnel. These policies should focus on practices that help personnel avoid unintentionally or negligently creating security vulnerabilities, such as keeping user credentials private, logging off all networks before leaving a device unattended, and restricting access to any sensitive files that they create. These policies should also clearly set forth the consequences for perpetrating, or assisting in the perpetration of, an insider attack. In addition, employees should receive training on how to identify indicators of potential insider threats.

Such training should stress the importance of reporting any suspicious behavior, policy violations, personnel conflicts, or any other signal of an insider threat risk. Firms should also institute confidential and, in jurisdictions where it is permitted, anonymous mechanisms for reporting, such as whistleblower hotlines. Information from any policies relevant to the insider threat program adopted by the firm should be incorporated into training for new employees, and the firm should send periodic reminders of every employee's duty to safeguard against and report potential threats.

PREDICTIVE MODELING FOR INSIDER THREAT PROTECTION

Putting the policy and human component together with technical controls and solutions into a single holistic model is one of the key challenges of building an effective program. The model described and displayed below starts with technical controls and data as the foundation of a predictive model that ultimately combines psycho-social and traditional cyber data to raise early red flags for further analysis. The confidence level that a firm puts in the predictive accuracy of such model will vary depending on the quality of the technical indicators captured, the ability of managers to correctly assess their employees, and the skill of the insider threat team to incorporate the policy and human components of the insider threat program into the technical model.

Understanding the Investigative Challenge of the Insider Threat



Incoming data processed to infer observations; observations processed to infer indicators; indicators assessed to gauge threat.

As illustrated above, combining policy and human elements with technical controls and solutions into a single, holistic model is one of the key challenges in the development of an effective program. The model, as depicted in the associated graphic above and in the following detail, begins with technical controls and data as the foundation of a predictive model. This process ultimately combines psycho-social and traditional cyber data to raise early red flags for further analysis.

At the highest level, the model consists of a repository of indicators and heuristic models of insider behavior. Indicators can be interpreted as examples of insider behavior and characteristics—a collection of inferred intentions and observed actions. This repository of information influences all the components of the insider threat model and therefore it should be regularly adjusted to reflect new findings produced by data collection, data fusion, and analysis. The goal is to create a multifaceted analysis process that allows the organization to move from data to observations, and then from indicators to behaviors, as illustrated.

Naturally, the reliance that a firm places on the predictive accuracy of such a model will fluctuate with the quality of the technical indicators captured, the ability of managers to accurately evaluate their employees, and the manner in which the organization can successfully incorporate the policy and human considerations of an insider threat program into the technical model.

It is worth noting that prioritization is a crucial component of this model because not all possible data can be collected or analyzed simultaneously and (e.g., HR records) may not be available instantaneously. As a result, firms need to implement a prioritized approach to data collection, analysis, and decision making where various pieces of information are collected and assessed for different individuals, depending on their positions and relative insider threat risk as determined by the model. With respect to that prioritization, threat feeds have been recognized as a potential data source. These feeds may include industry groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), intelligence feeds from government and law enforcement such as the FBI, or feeds from security companies. While a threat feed will not identify specific individuals to investigate, the data contained in the feed may highlight behavior warranting further investigation.

Ultimately, behaviors accumulate into a series of events leading to a particular objective, whether malicious or unintentional. The goal of any predictive model is to identify warning signs from actions, events, or behaviors that may result in harm or enhanced risk to the organization. Under this predictive model, such warning signs may be identified or inferred using pattern recognition or independent, model-based reasoning. Pattern recognition may be most helpful in identifying behavior that is typical of an insider threat risk, while model-based reasoning may be helpful in understanding the meaning or motivation behind identified anomalous behavior. In the end, the objective is to leverage the predictive model to appropriately interpret an insider's intentions and predict potential attacks, rather than rigidly applying a template to observed characteristics or behaviors.

Due to the complexity of regulatory requirements affecting program design and different financial activities, firms should engage legal counsel and compliance teams in investigation of potential insider incidents. Some of these regulatory requirements and restrictions, such as data localization issues and restrictions on data transfers, may present investigational challenges and increase the complexity of implementing an insider threat program on a global level. Cross-organizational participation, under the direction of counsel, will help mitigate the risk of failure to comply with the financial firm's regulatory obligations.

MONITORING TOOL CONSIDERATIONS

Insider threat programs use a variety of tools and tactics, from Data Loss Prevention (DLP) and access management policies, user activity monitoring and continual education. While these tools are essential for safeguarding an organization's sensitive data, they must be deployed carefully to balance security with privacy considerations.

As a company considers deploying these tools, the firm may want to consider the following:

1. **Data collection and monitoring**

   Insider threat detection tools often involve collecting and monitoring a wide range of data, including employee communications, system logs, access logs, badge logs and user behavior which may be used to detect intent. Excessive data collection or combining multiple data elements can infringe on an individual's privacy rights, therefore counsel shall be consulted prior to doing so. International, Federal, state and regional laws should be considered before an organization proceeds with data collection and monitoring.

2. **User Surveillance**

   Employee activities monitoring such as including keystrokes, website visits, file access and badge access may create an environment in which employees feel they are constantly surveilled. These activities, if used to try and "catch" a user doing something wrong, could result in a loss of trust and morale in the enterprise.

3. **Privacy Expectations**

   Employees should have a reasonable expectation of privacy in the workplace. Constant intrusive monitoring without consent and transparency with employees regarding how the monitoring will be used could lead to potential privacy violations.

4. **False Positives**

   Insider threat detection tools can generate false positives, flagging innocent employee activities as potential threats to the organization. Investigating these false alarms could potentially result in an unwarranted intrusion into the employee's privacy and should be considered. Ensuring the Insider Threat Program investigative unit has strong controls around employee information accessed and monitored and robust data protection policies regarding what has been accessed to determine if the activity is truly an insider threat should be part of the program's procedures and continually audited to drive compliance.

5. **Ethical Concerns**

   An ethical concern may arise when organizations use monitoring tools to gather information about an employee's personal life, behaviors and communications that are unrelated to the person's work function and activities.

Organizations may find that striking an appropriate balance between security and privacy is a challenge. Insider threat monitoring and detection should be proportional to the potential risks and aligned with the company's goals without infringing on an individual's right. Clear policies, transparent communications, and data access that have been developed and maintained with legal, compliance, and ethical considerations are best practices/key components of a successful insider threat program.

CONSEQUENCE MODELING

Consequence models are specific to an organization and should be individually tailored to its risk appetite. Not all incidents identified through an Insider Threat program require the same consequence. Violations range in severity and penalties are assigned accordingly - immediate termination, to intermediate discipline, to warnings. Some violations may not be a concern unless they are repeated.

Consequence model design should be in partnership with relevant internal stakeholders such as Human Resources and in consultation with the business.

An example of a consequence model related to failure to detect simulated phishing campaigns is below.
A single failure is an opportunity to educate the user, whereas continued failure increases the risk that the user could be susceptible to a malicious email and so the consequences increase as the failure rate increases.

Clicks	Recidivist Consequence Model for Simulated Phishing
Click per campaign	• In the moment training (pop-up) that includes awareness and best practices
2 clicks in rolling 6 months	• Mandatory online training (module 1) assigned with 30-day deadline to complete • Notification to direct manager / Assignment Contact • Notification to contingent worker vendor
3 clicks in rolling 6 months	• Mandatory online training (module 2) assigned with 30-day deadline to complete • Failure Notice to accompany mandatory training assignment • Optional Business Unit (BU) led discussions / training • Notification to direct managers / contingent assignment contact • Notification to Business Unit Information Security Officer (BUISO) • Notification to contingent worker vendor that the individual risks being taken off account
4 clicks in rolling 6 months	• Mandatory training live-session led by Insider Threat Team (scheduled twice a month) • Notification to direct managers / Assignment Contact • BUISO to work with senior management on additional education / action with documented decision point for any required evidence or tracking • Written escalation to senior risk lead / risk manager / BU manager (mandatory if training was avoided across 2 months) • BU decision on taking contingent worker off account with documented decision point for any required evidence or tracking
5 clicks +	• Decision on taking contingent worker off account with documented decision point for any required evidence or tracking • Letter of Education for inclusion in performance record issued by HR based on email notification to user who clicked and manager and BUISO • BUISO and manager conversation with HR occurs to determine extenuating circumstances

X. STRUCTURING AN INSIDER THREAT PROTECTION PROGRAM

While the complete elimination of insider attacks may be virtually impossible, an insider threat protection program can greatly reduce their prevalence and impact. As previously mentioned, cybersecurity defenses alone cannot adequately protect against insider threats. Rather, successful programs take a holistic approach involving a combination of technology, legal advice, policy development, physical security, risk awareness and training, organizational psychology/sociology, and counterintelligence resources. Senior representatives from these various functions can serve as members of an insider threat "working group" that can provide governance, oversight, and direction that accounts for the business model of the firm and all the functions that it performs. Although distinct from the insider threat team, which should be directly responsible for conducting insider threat investigations and routine monitoring, the working group should be consulted when developing new insider threat policies or responding to detected threats. Not surprisingly, this kind of integrated approach is most effective when the firm allocates sufficient personnel, technology, and financial resources to its success; therefore, visibility of the program to the board of directors and executive management is essential to receive the requisite support.

It is important for the board of directors and executive management to participate in the oversight and, where appropriate, the direction of a financial firms' insider threat program. According to the SIFMA Benchmarking Survey, approximately 70% of firms provide updates on their insider threat program to the board (or an appropriate committee thereof) on a monthly, quarterly, or semiannual basis. Such participation and oversight from the board is the best practice in the financial industry and quickly becoming a regulatory expectation.

The location of an insider threat team within an organization can vary. While some maintain a counter-intelligence unit, others create teams within their human resources or cybersecurity units. The SIFMA Benchmarking Survey indicated that while approximately 35% of firms place their insider threat program primarily in the Information Security branch of their organization, a wide variety of other functions and stakeholders typically participate in the program, including Legal (81% of firms), Compliance (73%), Privacy (70%) and Human Resources (81%). While structures can vary, it is the unit's separate identity that is most important.

Because insider threats may arise at all levels and throughout all functions of an organization, this separation enables an insider threat team to conduct independent, unbiased investigations. However, it is still important to reiterate that the team responsible for addressing the insider threat is able to call on the capabilities of other functions within the firm to accomplish its mission, such as information technology ("IT") for system activity monitoring, human resources ("HR") for background checks, and line managers for behavioral monitoring.

Although the insider threat team should maintain direct responsibility for implementing the insider threat protection program, every aspect of the organization must play its part—including IT, HR, legal counsel, management, physical security, audit, data owners, and software engineers. The insider threat team should facilitate communication across different functions within the firm and avoid acting in a "silo." Too often, individual units will respond to suspicious insider behavior in isolation: for example, a report that an employee angrily confronted a supervisor would typically be referred to HR, which may intervene or continue to observe the employee for signs of escalation of the dispute. However, heightened HR monitoring alone would not detect suspicious network activity that could signal an imminent insider attack. In this case, an insider threat team should be notified to ensure that comprehensive monitoring by IT, security, and other relevant departments is conducted in response. This coordinated, interdisciplinary approach ensures that threats are promptly addressed by both the insider threat team and the associated supporting functions no matter how they manifest.

Personnel assigned to insider threat protection are obviously not immune from posing an insider threat risk themselves. Organizations must therefore establish internal controls to maintain the integrity of their insider threat program. Firms should conduct regular independent reviews of their insider threat program to monitor its effectiveness. According to the SIFMA Benchmarking Survey, just over 50% of firms responded that their insider threat program is audited by Internal Audit only on an ad hoc basis or only as a part of other audited programs. Firms should also designate personnel to oversee the proper handling and use of records concerning the insider threat program, and to ensure that records generated by the program are accessible only on an as-needed basis.

Senior personnel should be responsible for regularly scheduled compliance reviews to ensure that program staff are following the insider threat policy guidelines and any applicable legal, privacy, and due process or civil liberties protections. The results of these reviews should be reported by internal audit staff to senior management and the board to ensure they are informed and involved sufficiently to ensure that issues are resolved in a timely and appropriate manner. To prevent unwarranted invasions of privacy, senior management, in consultation with legal counsel, should develop special access procedures for extremely sensitive information that might be sought in insider threat investigations, such as law enforcement records or records from past investigations.

SEVEN CORE STEPS TOWARDS IMPLEMENTING AN INSIDER THREAT PROTECTION PROGRAM

Firms may consider the NIST Cybersecurity Framework when developing the core elements of an Insider Threat Program.[6] The steps outlined in the NIST Cybersecurity Framework for prioritizing, scoping, assessing, and improving a cybersecurity program are universal—as is the application of a continuous improvement process that is critical to keeping security and risk programs fresh and relevant. In addition, as firms implement the NIST Cybersecurity Framework, many of the steps will overlap with other risk practices. Below are the seven steps that firms should follow in developing the core elements of an Insider Threat Program, modified slightly to call out key items specific to insider risk.

7 CORE STEPS	
Step 1	Prioritize and Scope. The organization identifies its business/mission objectives for its insider threat program, high-level organizational priorities, and associated risk tolerances.
Step 2	Orient. Once the scope of the program has been determined for the business, the organization identifies related systems and assets, regulatory requirements, legal constraints, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.
Step 3	Assess Current State. The organization develops a current state for their insider threat program.
Step 4	Conduct a Risk Assessment. The organization analyzes the operational environment in order to discern the likelihood of an insider-driven event and the impact that the event could have on the organization.
Step 5	Create a Target State. The organization develops a future state for their insider threat program.
Step 6	Determine, Analyze, and Prioritize Gaps. The organization compares the current state to the target state to determine gaps. It creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the target state.
Step 7	Implement Action Plan. The organization determines which actions to take to address the gaps identified-in the previous step. After mitigation steps have been taken, the organization monitors its current practices against the target state.

This guide is meant only to provide a general framework for implementing an insider threat protection program. Outside experts can provide more tailored, detailed assistance and feedback. In addition to private

consultants, there are non-profit and government resources that can provide assistance.

The Department of Homeland Security (DHS) and Department of Defense (DOD) also offer shorter awareness courses on protecting critical infrastructure against insider threats; for more information, contact the National Cybersecurity and Communications Integration Center Analysis team at NCCIC@hq.dhs.gov.

AN INSIDER THREAT MATURITY MODEL

Financial institutions are prime targets for insider attacks, posing risks such as theft, asset damage, and disruption to operations. Detecting and preventing these attacks is challenging due to insiders' familiarity with systems and the increasing risk of unintentional incidents. To combat these threats, a structured and targeted insider protection program is crucial. A key component of any program is an assessment or maturity model evaluation. A maturity model provides a framework to assess and enhance an organization's capabilities in managing insider events effectively. It serves as a roadmap to evaluate the current state, identify areas for improvement, and advance the maturity level over time.

The maturity model consists of stages that help define the current state of potential applicable insider risks for your organization. Depending on the scope of the program for your organization, these risk areas may include espionage, employee conduct, employee fraud, data theft, physical theft, workplace safety, privilege misuse, sabotage, reputational damage, and dangerous combinations of access. We suggest the following high-level stages and minimum criteria of a maturity model for consideration when assessing an insider protection program:

1. Foundational Stage - Awareness and Fundamentals:
    - Basic understanding of insider risks and their impact.
    - Implementation of fundamental controls and security policies.
    - Initial incident response capabilities, primarily reactive.
    - Informal communication and ad-hoc processes for addressing insider risks and threats.
2. Developing Stage - Program Establishment and Collaboration:
    - Formalization of an insider protection program with dedicated personnel.
    - Enhanced awareness through training and education programs.
    - Adoption of proactive monitoring and detection measures.
    - Collaboration with stakeholders to establish policies and procedures.
3. Enhancement Stage - Strengthening Controls and Response:
    - Expanded scope to cover a broader range of insider risks and threats.
    - Implementation of data loss prevention technologies and advanced access controls.
    - Integration of threat intelligence and information sharing mechanisms.
    - Formal incident response plan and process, including a dedicated team, notification thresholds, and decision tree.
4. Optimization Stage - Integrated Risk Management:
    - Integration of the insider protection program with broader risk management frameworks.
    - Continuous monitoring and analysis of user activities using advanced analytics.
    - Collaboration with external entities for information sharing and benchmarking.
    - Periodic evaluation and improvement based on feedback and metrics.
5. Transformation Stage - Proactive and Adaptive Risk Management:
    - Proactive identification and assessment of insider risks using predictive analytics.
    - Adaptive controls and dynamic response mechanisms based on real-time monitoring.
    - Integration of the insider threat protection program with other security domains.
    - Continuous improvement through regular (e.g., annual) risk assessments and innovation.

These stages provide a roadmap for organizations to assess their current maturity level, identify areas for improvement, and strategically advance their insider threat protection programs. The previously mentioned non-profit organizations and educational institutions may be consulted as resources.

Using the above maturity model maturity elements, customizing a maturity model to an organization's unique context may be beneficial. To customize, firms may consider extracting recommendations from

multiple best practice guides, identifying common categories, defining maturity levels, and implementing the recommendations accordingly. Involving subject matter experts with insider risk and threat knowledge ensures the model's effectiveness and alignment with organizational needs.

To add clarification, a customized maturity model may be created by performing the following steps:

1. Extract the recommendations from best practice guides, such as the guides from CERT and CISA. The goal is to achieve a 'critical mass' of guidance that eliminates any potential omissions or biases in individual best practice documents.

2. Identify common categories within the recommendations. For example: 'vetting', 'monitoring,' incident response,' and so on.

3. Identify the maturity levels that will be used in the maturity model. Another document that defines and describes five useful maturity levels is the '*Cybersecurity Assessment Tool*'[13] from the Federal Financial Institutions Examination Council (FFIEC).

4. For each category identified in step 2, place the recommendations identified in step 1 into the maturity levels identified in step 3. Where duplicate recommendations exist because of the use of multiple best practice guides, select a single recommendation that best captures the spirit of the collective guidance. This also has the benefit of reducing the overall number of recommendations to a manageable number.

5. Use subject matter experts with knowledge of insider threats to reach a consensus view regarding the placement of the recommendations within the maturity model levels. This exercise could involve parties external to the organization, such as other organizations or information-sharing groups.

Implementing a maturity model empowers financial institutions to effectively manage insider risks. By following the stages of maturity and adopting industry best practices, organizations can enhance their capabilities in preventing, detecting, and responding to insider events. Regular assessments and evaluations, whether through an internal or external model or a combination, enable organizations to proactively mitigate insider risks and safeguard their sensitive assets and operations.

PROGRAM CONTROLS

Along with presenting core steps that focus on prioritizing, scoping, assessing, and improving a cybersecurity program, the NIST Framework also provides a set of activities to achieve specific cybersecurity outcomes. To recap, the NIST Framework's "core" components—Identify, Protect, Detect, Respond and Recover—presents key cybersecurity outcomes identified by the industry as helpful in managing cybersecurity risk.

The NIST Framework Core elements, as described in the chart below which define key controls normally associated with Insider Threat Programs, work together as follows. Categories are the subdivisions of a core component that group cybersecurity outcomes into programmatic needs and particular activities. Subcategories further divide a category into specific outcomes of technical or management activities. Informative References are specific sections of standards, guidelines, and practices common amongst critical infrastructure sectors that illustrate methodologies that can be leveraged to achieve outcomes associated with each subcategory. Please note that the Informative References are not intended to be an exhaustive list, but rather a starting point based on input

[13] FFIEC Cybersecurity Awareness

SIFMA received from an initial set of stakeholders.

Identify (ID)		
Category	Subcategories	Informative References
Asset Management (ID.AM): Ensure that the data, personnel, devices, systems, and facilities at risk of insider attack are identified and prioritized	**Know and Protect Your Assets:** Conduct a physical asset inventory. Identify the functions of asset owners and the types of data on the system(s). Identify and document software configurations. Prioritize assets and data to identify high-value targets.	Common Sense Guide, 4th Ed., Best Practice #6 Common Sense Guide, 5th Ed., Best Practice #1 NIST Cybersecurity Framework (ID.AM-1, 2, 4) DoD Insider Threat Mitigation, Appendix A, Rec. 2.10
	Criticality: Determine what assets are most critical to the proper execution of the organization's business goals. Items to be considered are: • Systems (software, hardware, devices) • Data & Intellectual Property • Personnel • Third party Providers • Partnerships	NIST Cybersecurity Framework (ID.AM-5) DoD Insider Threat Mitigation, Appendix A, Rec. 1.10
	Security Agreements: Define explicit security agreements with all third parties, including access restrictions and monitoring capabilities.	Common Sense Guide, 4th Ed., Best Practice #9 NIST Cybersecurity Framework (ID.AM-6; PR.AT-3)

Identify (ID) continued		
Category	Subcategories	Informative References
Governance (ID. GV): Structure an insider threat team and develop corresponding policies and procedures for monitoring and management	**Develop a Formalized Insider Threat Program:** Establish policies and procedures for addressing insider threats that include but are not limited to policies setting forth responsibilities with respect to HR, Legal, Security, and Internal Audit. **Structure**: Determine the location of the insider threat team within the organization **Staff**: Hire new personnel with counterintelligence experience to staff the insider threat team, or train existing employees in relevant skills **Policies and Procedures**: Assign monitoring and investigation roles and responsibilities within team; establish policies and procedures for conducting investigations. Ensure oversight on the program is established at the board level. **Clearly Document and Consistently Enforce Policies and Controls**: Ensure that senior management enforces and complies with all policies. Train employees on all policies and procedures and secure their agreement to comply.	AFCEA Insider Threat: Protecting U.S. Business Secrets, pp. 2-4, 6 Common Sense Guide, 5th Ed., Best Practices #2 and #3 FFIEC CAT, Domain 1, Resources
	Designation of Corporate Sponsor: Firms should designate a senior officer who will be principally responsible for establishing and operating an insider threat program that will link into other areas and functions within the organization (e.g., Human Resources, Information Technology, etc.).	Minimum Standards for Executive Branch Insider Threat Program, Section D
	Global Governance: Ensure that the legal and regulatory requirements of each region and country in which the firm operates are understood and managed, including laws relating to privacy and civil liberties. Adjust policies, procedures and practices to account for cultural differences across regions.	Best Practices Against Insider Threats in All Nations International Implementation of Best Practices FFIEC CAT, Domain 1, Governance
	Communication to Personnel: After an insider threat program is established, communicate its existence and associated policies and procedures to employees. **Incorporate Malicious and Unintentional Insider Threat Awareness Training**: Train employees continuously—be creative about training methods to increase security awareness.	Common Sense Guide, 4th Ed., Best Practice #16 DoD Insider Threat Mitigation, Appendix A, Rec. 3.1 AFCEA Insider Threat: Protecting U.S. Business Secrets, pp. 6-8 FFIEC CAT, Domain 1, Training and Culture Common Sense Guide, 5th Ed., Best Practice #9

Identify (ID) continued		
Category	Subcategories	Informative References
Risk Assessment (ID.RA): Understand the risk that insiders pose to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Vulnerabilities**: Identify the vulnerabilities within critical assets that could make them susceptible to an insider attack. **Threats**: Identify external threats that could be the source of an attack delivered by an insider in addition to the conditions that could lead to an organization employee or resource becoming a threat. **Impacts**: Apply threats (both internally driven and externally driven but internally supported) to critical systems and vulnerabilities in order to assess the risk to the organization and the possible impacts to the execution of the business and achievement of its goals. **Consider threats from insiders and business partners in enterprise-wide risk assessments**: Avoid direct connections with the information systems of business partners if possible; restrict access only to responsible administrators; ensure that business partners have conducted background investigations on employees with access to the firm's information systems or data.	National Risk Estimate DoD Insider Threat Mitigation, Section 2.6, Risk Management, pages 7-8 Common Sense Guide, 5th Ed., Best Practice #6 FFIEC CAT, Domain 1, Risk Management
	Third party risk: Assess threats from business partners, vendors, and other third parties with whom the firm interacts, and integrate a mitigation strategy for such threats within the enterprise-wide risk program. **Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities**: Ensure that service providers meet or exceed your organization's security practices. Control or eliminate remote administrative access to hosts providing cloud or virtual services.	Common Sense Guide, 4th Ed., Best Practice #1 Spotlight On Insider Threat: Trusted Business Partners, pp. 12-14 National Risk Estimate Common Sense Guide, 5th Ed., Best Practice #16 FFIEC CAT, Domain 4, Connections and Relationship Management

Identify (ID) continued		
Category	Subcategories	Informative References
Risk Management Strategy (ID. RM): Establish policies and procedures to identify kinds of behaviors that indicate insider activity	**Suspicious network and application activity**: Identify behaviors that could indicate suspicious insider activity if they occur more frequently than network baseline. Establish a list of indicators that could tip investigators to suspicious behaviors. **Be especially vigilant regarding social media:** Within applicable legal constraints, establish a social media policy that defines acceptable uses of social media and information that should not be discussed online. Conduct social media awareness training for employees.	Human Behavior, Insider Threat and Awareness Symantec White Paper Behavioral Risk Indicators Common Sense Guide, 4th Ed., Best Practice #16 Common Sense Guide, 5th Ed., Best Practice #7
	Concerning Behaviors: Create profile of behaviors and characteristics that may indicate that an individual is an insider threat. Develop models showing appropriate access to assets and behavior with respect to such assets for each type of employee. Create a comprehensive list of system and user behavior attributes that can be monitored to establish normal and abnormal patterns to enable anomaly and misuse detection. **Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior**: Where legally possible, conduct background checks on employees with access to firm funds or confidential information. Encourage employees to report suspicious behavior to appropriate personnel and investigate and document all issues of suspicious or disruptive behavior. **Anticipate and manage negative issues in the work environment**: Enhance monitoring of employees with an impending or ongoing personnel issue. Regularly review audit logs to detect activities outside of the employee's normal scope of work.	Predictive Modeling for Insider Threat Mitigation, at 9 FBI: Detecting and Deterring an Insider Spy Understanding the Insider Threat, pp. 90-91 DoD Insider Threat Mitigation, Appendix A, Rec. 6.8 Common Sense Guide, 5th Ed., Best Practices #4 and #5
	Sources of Information: Identify sources of raw data that can be used to extract patterns of behavior. Start by re purposing existing data from within the organizations systems and move to external sources of data to capture an individual's "digital exhaust" to which observations can be applied. **Deploy solutions for monitoring employee actions and correlating information from multiple data sources**: Implement rules within the SIEM system to automate alerts. Create strong log management policies and procedures. Regularly monitor the SIEM system.	DoD Insider Threat Mitigation, Appendix A, Recs. 1.3, 2.7 Common Sense Guide, 5th Ed., Best Practice #12
	Legal risk analysis: Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.	National Risk Estimate, Recommendation #5, page iii

Protect (PR)		
Category	Subcategories	Informative References
Access Control (PR.AC): Implement appropriate technical and administrative safeguards to ensure that access to assets and systems are limited to authorized users.	**Technical safeguards:** Strengthen cybersecurity standards in accordance with NIST Cybersecurity Framework. Manage remote access from both internal and external parties. Implement controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. Require contractors who use information systems by contract to meet minimum standards for technical safeguards and ensure compliance with such standards by routine audits. **Institute stringent access controls and monitoring policies on privileged users**: Conduct periodic account reviews to avoid privilege creep. Employees should have sufficient access rights to perform their everyday duties, and no more. Promptly update access permissions when an employee changes their role. **Institutionalize system change controls**: Periodically review configuration baselines against actual production systems. Ensure that changes are approved with a verified business need.	Common Sense Guide, 4th Ed., Best Practice #13 NIST Cybersecurity Framework (PR.AC-3; PR.MA-2) SEC Cybersecurity Risk Alert, p. 3 Common Sense Guide, 5th Ed. Best Practices #11 and #17
	Administrative safeguards: Implement processes and policies to limit access rights/credentials of all users, but especially privileged users, to ensure that only the minimum amount necessary is provided. Establish personnel security vetting procedures commensurate with an individual's level of information system access. **Implement strict password and account management policies and practices**: Define password requirements and train users on creating strong passwords. Additionally, perform audits of account creation and password changes by system administrators. Ensure all shared accounts are absolutely necessary and are addressed in a risk management decision.	Common Sense Guide, 4th Ed., Best Practices # 7, 8, 10 NIST Cybersecurity Framework (PR.AC 1-5) DoD Insider Threat Mitigation, Appendix A, Recs. 5.3, 2.3 Common Sense Guide, 5th Ed. Best Practice #10
	Off-boarding procedures: Implement standardized, comprehensive off-boarding procedures to ensure all access to company information is terminated upon employees' departure, including: • Termination of physical and electronic access rights • Changing passwords to all systems and data that the employee had access to, including shared accounts, files, and folders • Collect all equipment given to employee • Deleting remote access tools from employees' personal devices (e.g., RSA tokens)	Common Sense Guide, 4th Ed., Best Practice #14 NIST Cybersecurity Framework (PR.AC-1-3)
	Toxic Combinations of Entitlements: Seek out and remove conflicts of system access permissions that allows a user to break the law, violate rules of ethics, damage customers' trust, or even create the appearance of impropriety and ensure that segregation of duties analysis is performed to prevent its occurrence in the future. **Enforce separation of duties and least privilege**: Carefully audit user access permissions. Remove permissions that are no longer needed. Establish account management policies and procedures that limit administrative accounts to the minimum necessary privileges.	Identity and Access Management Information Risk in Financial Institutions Common Sense Guide, 5th Ed., Best Practice #15

Protect (PR) continued		
Category	Subcategories	Informative References
Awareness and Training (PR. AT): Implement programs to alert personnel to insider threat risks and consequences	**Education and Training**: Ensure that employees, contractors, and other personnel receive regular training and updates on topics relevant to mitigating insider threats, including: • Protocols for handling sensitive information, including IP and customer information • Responsibilities and processes for alerting management of suspicious activities • Handling of critical assets and physical and electronic access controls. Establish mandatory minimum standards for security education, awareness and training programs related to the insider threat. Ensure training is delivered on a regular basis to existing employees and is a part of all new hire training packages. Document attendance and compliance similar to other mandatory training requirements.	Common Sense Guide, 4th Ed., Best Practice #3 NERC CIP-004 DoD Insider Threat Mitigation, Appendix A, Rec. 3.3 SEC Cybersecurity Risk Alert, p. 3 Common Sense Guide, 5th Ed., Best Practices #7, 8, and 9
	Notice and consent for computer use policy: Upon hiring, and annually thereafter, require personnel to read and acknowledge their agreement to a computer use policy. The policy should indicate that any activity on any firm computer, electronic device (including company-owned mobile devices) or firm owned network (i.e., employees under BYOD program connecting to the firm's network or systems) is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Computer use policies should state explicitly that users do not have any expectation of privacy on work computers and devices. Mandate use of "warning banners" or other on-line messages that serve to raise the awareness to the need for secure and appropriate system usage, and that highlight recent observed misuse and its consequences.	Minimum Standards for Executive Branch Insider Threat Programs, Section H.3 DoD Insider Threat Mitigation, Appendix A, Recommendation 4.2
	Awareness programs: Highlight importance of preventing and detecting insider threats through periodic emails, memos, and/or announcements. Potential awareness topics include: • Reporting suspected insider activity to insider threat team • Methodologies of adversaries to recruit trusted insiders and collect sensitive information ("social engineering"), and steps that employees can take to protect themselves against such threats • Indicators of insider threat behavior • How to safely use social media	Minimum Standards for Executive Branch Insider Threat Programs, Section I.1.a-c How to Protect Insiders from Social Engineering Threats Common Sense Guide, 4th Ed., Best Practice 18
Information Protection Processes and Procedures (PR. IP): Maintain policies, processes and procedures to protect systems and assets from insider threats	**Policy Maintenance and Enforcement**: Clearly document and consistently enforce policies and controls **Backup data**: Ensure data backups are available and recovery processes account for the actions of malicious insiders. **Structure management and tasks to minimize insider stress and mistakes**: Establish a work culture that measures success based on appropriate metrics for the work environment. Encourage employees to think through projects, actions, and statements before committing to them.	Common Sense Guide, 4th Ed., Best Practice #2 Common Sense Guide, 4th Ed., Best Practice #17 Common Sense Guide, 5th Ed., Best Practice #8

Protect (PR) continued		
Category	Subcategories	Informative References
Protective Technology (PR.PT): Use technical security solutions to safeguard data that could potentially be exploited by insiders	**Control implementation**: Implement controls to prevent the exfiltration, manipulation, or changes to the integrity of critical data and files. **Close the doors to unauthorized data exfiltration**: Establish a cloud computing policy; restrict and monitor what employees store in the cloud. Inventory all connections to the company's data and restrict data transfer protocols to employees with a justifiable business need. Monitor the use of data transfer protocols and removable media. Establish policies to govern data transfers.	Best Practices and Controls for Mitigating Insider Threats, Slide 17 Common Sense Guide, 4th Ed., Best Practice #19 NIST Cybersecurity Framework (PR.DS-5) Common Sense Guide, 5th Ed., Best Practice #19 FFIEC CAT, Domain 3, Preventative Controls

Detect (DE)		
Category	Subcategories	Informative References
Anomalies and Events (DE. AE): Implement network and application monitoring tools, allocating the most resources to systems identified as "critical" in risk assessment	**Establish a baseline of normal behavior for both networks and employees:** Monitor networks over a designated period to determine a "normal" baseline of network activity. Baseline should be periodically evaluated to account for changes in technology use among personnel (e.g., influx of millennial employees may result in greater mobile device and social network use).	Common Sense Guide, 4th Ed., Best Practice #17 SEC Cybersecurity Risk Alert, p. 5 Common Sense Guide, 5th Ed., Best Practice #14
	Monitor Audit Logs: Develop tools for effective scanning and analysis of system and network audit logs to detect anomalous system and insider activity. **Monitor and control remote access from all end points, including mobile devices:** Disable remote access for employees that have separated from the organization. Include mobile devices as a part of the risk assessment.	DoD Insider Threat Mitigation, Appendix A, Recommendation 6.2 Common Sense Guide, 5th Ed., Best Practice #13
	Technical infrastructure: Where possible, implement monitoring software on the application layer in order to distinguish user behavior from automated machine behavior (e.g., routine browser cookie deletion). Useful tools include: • Full-packet sensors to investigate actions or inform response activities • Web content sensors to track risky internet use • Updated virus/malware scanners • Log correlation engines or system information event management (SIEM systems to log, monitor, and audit employee actions) • Systems to log, monitor, and audit employee actions and response activities on the application layer in order to distinguish user behavior from something produced by an automated machine	Common Sense Guide, 4th Ed., Best Practice #12 NIST Cybersecurity Framework (DE.CM-1-7) Human Behavior, Insider Threat, and Awareness FFIEC CAT, Domain 3, Detective Controls and Corrective Controls

Detect (DE) continued		
Category	Subcategories	Informative References
Security Continuous Monitoring (DE.CM): Designate appropriate personnel for insider threat mitigation team and implement continuous intelligence monitoring	**Insider Threat Mitigation Personnel**: Larger firms will benefit from a separate unit staffed by specially trained counterintelligence personnel. Individuals with experience in government counterintelligence are particularly valuable. Smaller firms for which a separate counterintelligence unit is not practical should still have employees designated for insider threat monitoring and investigations. Such employees should ideally have experience or training in: • Conducting personnel investigations • Restricting details of inquiries to relevant staff • Determining when it is appropriate to involve outside experts and law enforcement in investigations • Conducting a forensics analysis of an incident	Minimum Standards for Executive Branch Insider Threat Program (Point F) AFCEA Insider Threat: Protecting U.S. Business Secrets, p. 6
	Resource Allocation: Institute more stringent monitoring policies on privileged users and high-risk personnel.	Common Sense Guide, 4th Ed., Best Practice #10 NIST Cybersecurity Framework (DE.CM-3) FFIEC CAT, Domain 2, Monitoring and Analyzing
	Continuous Evaluation Program: Instead of re-evaluating employees at pre-set durations as one-time events based on their access and criticality, establish a program where employees are constantly monitored, and data is collected at regular intervals in small segments to look for changes over a longer period of time. Use surveys of employees and data collection in order to catalog life events and changes as they occur.	Suitability and Security Clearance Report Common Sense Guide, 4th Ed., Best Practice #5 DoD Insider Threat Mitigation, Appendix A, Recommendation 2.7
	Increase Awareness of Potential Threats: Gain new intelligence about possible threats through information sharing with government agencies and other private organizations Report instances of insider threats at your organization to DHS, FBI, and Secret Service Capitalize on information sharing programs run by DOD, DHS and FBI Consider participation in information depositories when/if they are developed by Congress Build relationships with local and state law enforcement and monitor local data sources as consolidated reporting is limited currently **Maintain Employee Morale**: In order to maintain a positive firm culture and to avoid alienating potential insiders, firms should establish due process procedures to create a fair disciplinary process. It is important to structure and implement insider threat programs in a way that avoids giving disgruntled insiders cause or motivation to carry out an attack against the firm. Consider explaining how the firm's insider threat practices are developed and implemented in a proportionate manner to help reduce impact on workplace privacy.	DOJ/FTC Antitrust Policy Statement Suitability and Security Clearance Report FFIEC CAT, Domain 2, Threat Intelligence, and Information Sharing

Detect (DE) continued		
Category	Subcategories	Informative References
Detection Processes (DE. DP): Implement means for reporting and discovering suspicious insider behavior	**Cybervetting**: Continually monitor employees' suitability to hold positions involving access to sensitive information by monitoring their digital footprint and activities on the internet, within appropriate legal restrictions. This will provide insights into their current situation and inform additional investigations as necessary.	Developing a Cybervetting Strategy
	Reporting Mechanisms: Develop systems through which personnel can report – anonymously, if desired – suspicious behaviors that may indicate insider activities, or security flaws that are vulnerable to exploitation by insiders. Such systems may include a whistleblower hotline, online reporting portals, or an employee designated to receiving tips. Establish mechanisms through which customers may report fraudulent transactions or other suspicious activity on their accounts (e.g., unauthorized access attempts). Ensure existing programs are linked to the insider threat analysis activities. Make use of existing data collection platforms and repurpose collected information for analysis.	Your Role in Combating the Insider Threat

Respond (RS)		
Category	Subcategories	Informative References
Communications (RS.CO): Establish, memorialize, and standardize investigation and response procedures to include interaction with law enforcement	**Investigation Procedures**: Establish procedures for conducting an investigation that cover: • Reviewing affected systems and re-creating the incident • Interviewing suspects and witnesses • Documenting evidence and findings in a centralized system • Delegating investigative responsibilities among relevant personnel • Sharing information related to the investigation only on a need-to-know basis	NIST Cybersecurity Framework, RS.CO-1 - RS.CO-2 Electronic Crime Scene Investigation Prosecuting Computer Crimes
	Decision Tree: Create a decision tree that outlines how to respond to investigation findings. The tree should address: • Intervening vs. continuing to monitor concerning behavior • When to involve non-insider threat team personnel in the investigation • When to escalate incidents up the management chain within the organization • Circumstances warranting consultation with third-party experts and/or legal counsel • Situations warranting notification to law enforcement	NIST Cybersecurity Framework RS.CO-3 to RS.CO-5 FFIEC CAT, Domain 5, Escalation & Reporting

Respond (RS) continued		
Category	Subcategories	Informative References
Analysis (RS. AN): Classify incident to determine appropriate investigative procedure	**Type of insider**: Determine whether the insider incident was a result of unintentional or intentional activity. An attack that was unintentionally enabled by an insider – e.g., through the use of their access credentials – should be further investigated to determine whether a malicious insider facilitated the attack. • Implement tools for a rapid and effective audit of a host computer system to detect any anomalies in its programs and files. • Develop capabilities to conduct forensic analyses of intrusions.	DoD Insider Threat Mitigation, Appendix A, Recommendations 7.1, 7.2
	Type of Attack: Determine the type of attack in order to assess the scope of the attack, information potentially affected, and the appropriate personnel to involve.	NIST Cybersecurity Framework RS.AN-4
Mitigation (RS. MI): Prevent expansion of event by addressing its cause	**Eradicate Cyber Vulnerability**: Work with IT, outside firms, and/or law enforcement, as appropriate, to eliminate any malware or remediate any security vulnerabilities introduced into the system that is an active or possible future compromise.	NIST Cybersecurity Framework RS.MI-1 to RS.MI-3 FFIEC CAT, Domain 5, Detection, Response, & Mitigation
	Personnel Action: Remove access from the person suspected to remove the risk of continued or new malicious activity. Determine what disciplinary or legal action should be taken against the person(s) responsible for the incident. Where appropriate, consider legal action to recover or enjoin the use of stolen information. Ensure that management invokes minor sanctions for low level infractions of the stated security policy, in order to demonstrate the organization's commitment to the policy and vigilance in the enforcement of its principles. **Develop a comprehensive employee termination procedure**: Develop an enterprise-wide checklist to use when someone separates from the organization. Track all accounts assigned to each employee. Collect all the departing employee's company-owned equipment before the employee leaves the organization. Archive and block access to all accounts associated with the employee.	DoD Insider Threat Mitigation, Appendix A, Recommendation 4.3 Common Sense Guide, 5th Ed., Best Practice #20

Recover (RC)		
Category	Subcategories	Informative References
Recovery Planning (RC. RP): Execute recovery processes and procedures to control the scope of the incident and restore affected data	**Isolate and Restore**: Isolate any system compromised by the attack to prevent damage to other systems. In accordance with the firm's system recovery plan, restore damaged or destroyed data by retrieving backup tapes and, when necessary, engaging IT or outside forensic professionals to recover backup files on servers and hard drives. **Implement secure backup and recovery processes**: Store backup media off-site. Ensure that the media is protected from unauthorized access and can only be retrieved by a small number of individuals. Ensure that configurations of network infrastructure devices are part of the backup and recovery plan.	NIST Cybersecurity Framework RC.RP-1 Common Sense Guide, 5th Ed., Best Practice #18

Recover (RC) continued		
Category	Subcategories	Informative References
Improvements (RC.IM): Evaluate incident and incorporate lessons learned into future activities	**Incident Evaluation**: Meet with senior management and other appropriate personnel to discuss potential improvements to prevent similar incidents in the future. Consider engaging independent auditors to evaluate security and monitoring systems to identify weaknesses and suggest improvements.	NIST Cybersecurity Framework RC.IM-1, RC.IM-2
Recovery Planning (RC. RP): Execute recovery processes and procedures to control the scope of the incident and restore affected data	**Public Relations**: Work with internal and external PR personnel to develop company's public response to an incident. Designate individuals authorized to speak on behalf of the organization in regard to the incident and inform others of policy on speaking to outsiders regarding the incident.	NIST Cybersecurity Framework RC.RP-1
	Internal Communication: Communicate recovery activities internally and inform individuals of any changes in policies or procedures designed to prevent future incidents.	NIST Cybersecurity Framework RC.RP-3
	Regulatory Reporting: As required by regulatory reporting, post the incident to the firm's financial reports. Inform state and regulatory authorities of the incident as required by law.	SEC Cybersecurity Risk Alert, p. 7

XI. MEASURING INSIDER THREAT PROGRAM EFFECTIVENESS

Firms may consider measuring their insider threat programs with metrics developed and assessed under the NIST Framework. For example, according to a SIFMA Benchmarking Survey, over half of responding firms reported that they align their insider threat programs leveraging elements from the NIST Cybersecurity Framework, Carnegie Mellon University's CERT Best Practices Guide, and MITRE's Insider Threat Framework. Within the frameworks chosen by the firm, the insider threat team should establish a system of management and key operational metrics to evaluate, on an ongoing basis, the implementation and effectiveness of their insider threat program. Please note that these are suggested metrics, and it is up to your organization to use the metrics that best fit the specific insider threat program.

Although developed as an aid for cybersecurity defense programs, the National Institute of Standards and Technology (NIST) Cybersecurity Framework's "core" components—Identify, Protect, Detect, Respond, Recover—are a useful framework for implementing an insider threat program control. They can also serve as a consistent set of terms for communication and integration of insider threat risks into a firm's enterprise risk management program. The NIST Cybersecurity Framework takes a risk-based approach, informed by the relevant threats and based on the resources available and the overall business model of the firm, and it can therefore be adapted to create or improve a cybersecurity program or an insider threat protection program. The key tasks for each component are described in more detail in section IV.

While best practices documents on the topic of insider threats typically recommend that firms identify key metrics that can be used to assess their insider programs over time, there is no consensus regarding what metrics should be utilized. Part of the difficulty is that the universe of possible metrics is extremely large, could encompass any possible aspect of an insider threat program – or even beyond the program itself in related areas such as identity and access management, network security, backups, and such. Ultimately, the metrics chosen will be dependent upon the maturity and structure of an organization's program.

Ideally, metrics should have the following properties[14]:

- **Clear**: the metric is straightforward to understand.
- **Purposeful**: the metric enables or supports risk-management decisions.
- **Practical**: the data used to calculate the metric can be obtained without undue difficulty.
- **Justified**: the rationale for the metric is either self-evident or provided alongside the metric.
- **Measurable**: the metric is strictly quantifiable (no ambiguous "traffic light" ratings and such-like).
- **Relative**: the metric is expressed in a manner that enables trending over time without revising the data. For example, "percentage of workforce" is insensitive to changes in workforce size.
- **Time-bound**: the metric is measured over a distinct time period to enable trends to be identified. For example, measured daily, weekly, etc.
- **Standardizable**: the metric can be broadly standardized, enabling comparison between firms.

One additional consideration is how the data is presented, meaning what data graphics or other displays best fit the intended audience. It is likely that organizations will need to generate several different metrics; operational metrics will likely need to convey low-level details, whereas board-level metrics will likely need to convey the big picture and trends over time.

[14] This list is partially based on the blog post '*You Only Get 3 Metrics – Which Ones Would You Pick?*' by Phil Venables at https://www.philvenables.com/post/you-only-get-3-metrics-which-ones-would-you-pick.

Below, several examples of program metrics are provided. These metrics are a balanced set that covers various important program areas. Please note that while these metrics satisfy the criteria for good metrics as described above, it is up to your organization to identify and use the metrics that best fit your specific insider threat program. Additional metric ideas are available in Appendix B.

Metric	Rationale
Number of background checks conducted for new hires over time alongside the number of people that do not get hired because of background checks over time.	Measures key vetting control.
Percentage of workforce who have completed insider threat training over time.	Measures key behavioral control.
Number of emails / data elements prevented from leaving by DLP controls over time.	Measures key technical control.
Number of HR disciplinary actions such as performance reviews over time.	Measures behavioral precursors to insider incidents.
Number of EAP (Employee Assistance Program) interventions over time.	Measures workforce stability.
Number of true positive insider incidents over time broken down by intentional/unintentional, employees/contractors, business unit, etc.	Measures insider risk.
Number of tickets/escalations created over time broken down by type.	Measures operational trends.
Number of changes made to controls based upon lessons learned and post-mortem activities.	Measures effectiveness of program continuous improvement.
Percentage of workforce that leaves the firm over time.	Measures key variable in risk of intellectual property theft.

Insider threat risks often converge around the point of employee onboarding or separation/termination. As a result, firms should identify and follow appropriate onboarding and termination procedures for employees. These procedures should be developed in conjunction with the firm's insider threat program in order to ensure that risks are appropriately addressed by human resources and information technology staff in the normal course of business. For example, in the onboarding process, it is important to promptly grant access privileges to information systems for new employees to prevent them from seeking unauthorized access to information necessary for their work.

Likewise, it is important to promptly remove access privileges from separated employees and ensure that they do not have physical or electronic information resources in their possession upon leaving. When an employee is suspected of misusing sensitive information, it is important that the firm rigorously follow its termination procedures in order to maintain confidentiality and prevent further compromise of sensitive information. Further, although artificial intelligence applications may be helpful in screening and hiring processes, firms should be careful to avoid unlawful discrimination against job applicants or employees when making choices about the

input of data into screening algorithms.

As third-party service providers play a growing role in the financial industry, financial firms must also incorporate effective oversight of them into their insider threat programs. Third parties can be a source of significant cybersecurity vulnerabilities including insider threats. Consequently, supply chain risks and third-party service provider supervision have received increasing attention from federal regulators. For example, FINRA expects firms to perform pre-contract diligence on service providers, establish contractual terms to protect sensitive information and systems, include service providers in risk assessments, and establish and monitor service provider entitlements.[15] The SEC has asked its examiners to focus on firm practices and controls related to service provider management, including monitoring and oversight of service providers.[16]

The OCC requires banks to conduct independent reviews of vendors so that the bank's management can effectively manage cybersecurity risks,[17] and the Federal Reserve Board recommends the establishment of a risk management program that addresses ongoing monitoring of service providers.[18] Firms should take these and other obligations into account when implementing insider threat programs and evaluating insider threat vulnerability.

As noted elsewhere in this guide, an insider threat program cannot be developed in a vacuum. Because insider threat detection and prevention necessarily require some degree of intrusion into insiders' background and work habits, firms must consider privacy and employment laws when developing program policies and procedures. Legal risks associated with implementing insider threat protection programs in the workplace may be more significant in jurisdictions with more prescriptive laws related to privacy and data profiling, such as the EU. In the U.S., legal concerns and potential litigation involving defamation, retaliation, or wrongful termination are also important factors to consider. Section XII details some of these legal requirements and risks.

The Case Studies section in Appendix A is a compilation of real-world examples illustrating how insider threats occur and the potential damage they can inflict. These case studies can be a useful tool in emphasizing the importance of an insider threat protection program to senior management or the board, as well as identifying potential areas of weakness in programs. They can also be helpful aids in bringing the threats "alive" to the employees of a firm and "personalizing" the risk

[15] Regulatory Notice 21-29 | FINRA.org
[16] Proposed rule: Outsourcing by Investment Advisers (sec.gov)
[17] Third-Party Relationships: Interagency Guidance on Risk Management | OCC
[18] Federal Register :: Interagency Guidance on Third-Party Relationships: Risk Management

XII. LEGAL RISKS

Developing insider risk programs requires balancing of potential competing legal obligations. Importantly, regulators expect, and often require, robust controls against insider risk. However, these regulators and the laws and regulations they enforce also require firms to protect the privacy rights of stakeholders. Firms can certainly mitigate the risk of potentially significant theft and system damage with insider threat programs but should ensure that they appropriately and regularly evaluate the legal risks associated with those programs. The legal risks will differ based on applicable jurisdiction, stakeholders, data, technologies, among other factors.

In the United States, firms' monitoring practices and their insider programs are subject to federal and state laws and regulations. Many of those laws and regulations are sectoral. For example, the federal Electronic Communications Privacy Act ("ECPA"), state privacy laws, and tort laws limit the types of electronic communications monitoring that may be conducted. These laws include exceptions that may allow workplace monitoring, but generally require adequate notice of monitoring practices in order to claim those exceptions. Background checks, a key element of many insider programs, are also regulated under the Fair Credit Reporting Act ("FCRA"), as well as certain state and federal laws that impose restrictions on the scope of such background checks on job applicants.

In Europe and other non-U.S. jurisdictions, monitoring insiders is subject to greater scrutiny than in the U.S.. In contrast to the U.S., employee monitoring practices in those jurisdictions are closely regulated by data privacy laws that are based on, or closely aligned with, the EU's General Data Protection Regulation (the "GDPR"). Consequently, it is important to consider that, in many jurisdictions, employees have a stronger right to, and expectation of, privacy in the workplace compared to the U.S. The balance between the employer's legitimate interest to protect its business by monitoring for and investigating insider threats and the employee's expectation of privacy requires nuanced analysis that can be complex to navigate, and present burdensome path to compliance.

This section outlines key laws and legal risks that may be applicable to a firm's monitoring practices and insider threat program. This section addresses key laws and legal risks in the U.S., Hong Kong, India, the UK, the EU and Germany (as an example of an EU Member State). Depending on the facts and circumstances relevant to a particular insider threat program and practices, there may be other applicable laws and regulations.

This section is for informational purposes only and therefore is not intended to provide, and should not be construed as providing, legal advice. Prior to implementing any insider threat program, firms should engage in a comprehensive legal analysis and should consult with their own legal counsel about the particular facts and relevant compliance concerns.

UNITED STATES

ELECTRONIC COMMUNICATIONS MONITORING – FEDERAL LAW

Real Time Monitoring

In the U.S., the major federal law governing firms' monitoring practices and electronic communications privacy is the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 et seq. Title I of ECPA, also known as the Wiretap Act, prohibits the intentional "interception" and disclosure of wire, oral, and electronic communications, including email and telephone conversations, unless one of the Act's exceptions apply. § 2511(1)(a). Courts generally interpret the term "interception" as the acquisition of communications contemporaneously with their transmission; thus, the restrictions of the Wiretap Act apply to real-time monitoring programs, such as web traffic monitors and keystroke loggers. See, e.g., Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission") (citations omitted).

Importantly, the Cybersecurity Information Sharing Act of 2015 ("CISA 2015") provides a narrow exception allowing private entities to monitor information systems, regardless of any other federal or state restrictions, for cybersecurity purposes. 6 U.S.C. § 1503. It is important to note that this exception allows for monitoring only for the purpose of enhancing cybersecurity. If employee monitoring is used for judging productivity, the exception does not apply[19]. Id. Additionally, to encourage private entities to share cyber threat information with the federal government, CISA 2015 also preempts any state data privacy laws that would restrict or regulate such sharing.[20] Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, Department of Homeland Security (Oct. 15, 2021) (hereafter "DOJ/DHS Guidance on CISA 2015" or the "Guidance"), https://www.cisa.gov/sites/default/files/publications/Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015.pdf.

Under the DOJ/DHS Guidance on CISA 2015, private employee information can only be shared in those circumstances in which such information is necessary to describe or identify threats to information and information systems.[21] Id. at 5. The Guidance also advises that certain information must be redacted prior to sharing if not directly related to the cybersecurity threat, including HR data, consumer information and history, and protected health information as defined by HIPAA[22]. Id. at 10. Firms should consult with their legal counsel prior to sharing any private information with federal agencies to ensure that such information falls within the CISA 2015 exception.

The Wiretap Act also includes several key exceptions that firms should evaluate when assessing whether their real-time monitoring is potentially lawful. First, under the "provider exception" it is not unlawful for a "a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."[23] § 2511(2)(a)(i). Few courts have closely interpreted the provider exception; however, it is generally interpreted to permit employers that provide employees with internet and email service to monitor those services to the extent that they are used in the ordinary course of the employers' business.

Second, employers that provide internet or email service through a third party, or those that wish to monitor internet use that falls outside of the ordinary course of business, may wish to rely instead on the "consent exception." The consent exception allows the interception of communications where at least one party to the communication consents to the interception, and the communication is not used to commit a crime or tort.[24] § 2511(2)(d). Although courts have disagreed as to the definition of "consent" in the absence of explicit warnings or policies about monitoring, they have consistently agreed that employees consent to monitoring when memorialized policies or banners on web browsers permit it. *See, e.g., United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002) (professor had consented to monitoring where university's network use policy provided for periodic network monitoring); *United States v. Greiner*, 2007 WL 2261642, at *1 (9th Cir. 2007) (employee deemed to have consented to monitoring of remote network use where warning banner

[19] Id.
[20] Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, Department of Homeland Security (Oct. 15, 2021) (hereafter "DOJ/DHS Guidance on CISA 2015" or the "Guidance"), https://www.cisa.gov/sites/default/files/publications/Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015.pdf.
[21] Id. at 5.
[22] Id. at 10.
[23] § 2511(2)(a)(i).
[24] § 2511(2)(d).

provided for monitoring); *United States v. Cormack*, No. CR ELH-19-0450, 2021 WL 2187016, at *10 (D. Md. May 28, 2021) (defendant had no reasonable expectation of privacy when "told repeatedly that the [employer] owned the computer system and the data stored on it; the work computer was to be used for authorized work-related purposes only; and that usage is subject to monitoring").

Firms can therefore help protect themselves against potential liability under the Wiretap Act by developing a network use policy that clearly provides for the possibility of monitoring and requiring employees to provide their written consent to the policy. The Department of Justice has suggested that a banner notice on business-owned computers warning that network activity is subject to monitoring may be the most effective way to "generate consent to real-time monitoring" and "the retrieval of stored files and records pursuant to SCA." See Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009), Appendix A, p. 209, available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

Title II of ECPA, also known as the Stored Communications Act (SCA), prohibits intentionally accessing communications in electronic storage without, or in excess of, authorization. 18 U.S.C. § 2701(a). Although courts have disagreed on the meaning of "electronic storage" as used in the SCA, for compliance purposes firms should consider all emails to be potentially within the statute's scope. However, firms that provide their own email services to employees may access emails stored in work-provided accounts under an exception allowing access authorized by the entity providing the email service. § 2701(c)(1); *see also Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (holding that an employer's search of email stored on its own system fell within the service provider exception of § 2701(c)); *Meyer v. Mittal*, No. 3:21-CV-00621-HZ, 2023 WL 3004761, at *11 (D. Or. Apr. 17, 2023) (noting that "[a] few courts have followed or signaled agreement with the approach" that when emails are stored on the employer's server, the "the employer was the provider of the service and thus could read the emails".) It is unclear, however, whether this "provider exception" applies to firms that use a third-party email provider. Therefore, such firms can further shield themselves from liability by obtaining employees' consent to access stored emails. § 2701(c)(2).

As with the consent exception to the Wiretap Act, firms should disclose their email access policy to employees and obtain their signed agreement to the policy. Employers should not, however, attempt to access employees' private, web-based email accounts—by guessing passwords or otherwise—as courts have found that obtaining electronic communications through such access violates the SCA. *See, e.g., Fischer v. Mt. Olive Lutheran Church, Inc.*, 207 F. Supp. 2d 914, 920 (W.D. Wis. 2002), *Brown Jordan Int'l, Inc. v. Carmicle*, No. 0:14-CV-60629, 2016 WL 815827 (S.D. Fla. Mar. 2, 2016), aff'd, 846 F.3d 1167 (11th Cir. 2017) (an employee violated the SCA by accessing coworker's emails using a generic password provided to all employees.)

NLRB Protected Activity

Employers should be aware of additional restrictions on employee surveillance imposed by the National Labor Relations Act ("NLRA"). Section 7 of the NLRA provides employees with "the right to self-organization, to form, join or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purposes of collective bargaining or other mutual aid or protection . . ." 29 U.S.C. § 157. Decisions by the National Labor Relations Board ("NLRB") make clear that the right of employees to engage in protected, concerted activities limits the ability of employers to monitor or intercept employee's communications via the Internet or social media. For example, employers should not encourage supervisors to "friend" employees on social media, and employers should refrain from creating an impression of surveillance by making statements from which an employee might reasonably assume that his or her protected activities are being monitored. See Interfering with Employee

Rights (Section 7 & 8(a)(1)), National Labor Relations Board, https://www.nlrb.gov/about-nlrb/rights-we-protect/the-law/interfering-with-employee-rights-section-7-8a1. However, written policies proscribing unlawful behavior are permissible, and such policies may encourage employees to bring complaints or concerns to supervisors. *See NLRB v. Starbucks Corp*., 2012 WL 1624276 (C.A.2) (May 10, 2012).

In 2022, the NLRB issued a memo reiterating its commitment to protecting employees from intrusive or abusive electronic monitoring. Memorandum from Office of General Counsel Regarding Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights, National Labor Relations Board Memorandum GC 23-02 (Oct. 31, 2022) (hereafter "NLRB Memo"), https://apps.nlrb.gov/link/document.aspx/09031d45838de7e0. As outlined in the NLRB Memo, employers should be conscious of Section 7 rights when implementing new technologies to monitor and manage employees. The NLRB is especially concerned with monitoring that continues after employees leave work, such as tracking conducted through employer-issued mobile devices. The NLRB Memo also emphasizes that "it is well established that an employer violates [NLRB rules] if it institutes new monitoring technologies in response to activity protected by Section 7; utilizes technologies already in place for the purpose of discovering that activity, including by reviewing security-camera footage or employees' social-media accounts; or creates the impression that it is doing such things." Id. at 3.

Duty to Monitor

In contrast to legal restrictions related to the implementation of insider threat programs, firms must consider potential legal obligations to monitor their systems and employees for insider threats. This includes obligations to monitor and analyze employee access to confidential customer data under the U.S. Securities and Exchange Commission's ("SEC") Regulation S-P (the SEC "Safeguards Rule," 17 C.F.R. § 248), as well as legal obligations relating to the retention of records to comply with record-keeping requirements (see, e.g., "Records to Be Made by Certain Exchange Members, Brokers and Dealers," 17 C.F.R. § 240.17a-3, and "Records to Be Preserved by Certain Exchange Members, Brokers and Dealers," 17 C.F.R. § 240.17a-4). SEC's Office of Compliance Inspections and Examinations (OCIE) has "highlighted information security as a key risk for security market participants and has included it as a key element in its examination program." Cybersecurity and Resiliency Observations, Securities and Exchange Commission Office of Compliance Inspections and Examinations (Jan. 13, 2020), https://www.sec.gov/files/OCIE Cybersecurity and Resiliency Observations.pdf.

The OCIE encourages firms to create "an insider threat program to identify suspicious behaviors, including escalating issues to senior leadership as appropriate." Id at 5.

Many financial institutions are subject to additional laws and regulations affecting the privacy and security of consumer data, including the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and the corresponding Interagency Guidelines (see the OCC version, 12 C.F.R. 30), the FTC Safeguards Rule (16 C.F.R. § 682), the Consumer Financial Protection Bureau's ("CFPB") "Regulation P" (12 C.F.R. §§ 1016.13-14), and the SEC and FTC Identity Theft Red Flags Rules (see the SEC's Regulation S-ID, 17 C.F.R. § 162, and the FTC rule, 16 C.F.R. § 681), and comparable rules issued by the Commodity Futures Trading Commission ("CFTC"). The Federal Financial Institutions Examination Council's ("FFIEC") Cybersecurity Assessment Tool ("CAT") sets forth explicit regulatory expectations with respect to insider threat programs, including controls that a firm should have in place at the "evolving," "intermediate," or "advanced" levels. For example, the FFIEC CAT indicates that firms at the "evolving" level should have processes in place to monitor potential insider activity that could lead to data theft or destruction and have processes in place to alert the incident response team when potential insider activity has been detected. At the "intermediate" level, the FFIEC CAT expects that a firm would develop new technologies to detect and block insider threats in real time. At the "advanced" level, a firm should have automated tools to proactively identify high-risk insider behavior or data mining by insider threats.

Guidance published by the U.S. Cybersecurity & Infrastructure Security Agency ("CISA") highlights the

regulatory focus on insider threats. CISA emphasizes that a "committee of stakeholders for program governance and leadership" is an important part of successful insider threat mitigation programs. It recommends forming a multi-disciplinary governance group that would be in a position to "receive information pertinent to the background, conduct, and activities of trusted insiders," and would be responsible for reviewing the organization's insider threat policies and procedures. Insider Threat Mitigation Guide, Cybersecurity and Infrastructure Security Agency (Nov. 2020), https://www.cisa.gov/sites/default/files/2022-11/Insider Threat Mitigation Guide_Final_508.pdf. CISA recommends that maintaining a relationship with law enforcement agencies "may make the entire mitigation and management process more effective when an incident occurs," and that the "need to establish these relationships… applies to organizations of all sizes and maturity levels." Id. at 34.

Firms should note that, even lacking specific applicable regulatory requirements, lax practices could give rise to enforcement under broad rules governing unfair or deceptive practices. In 2023, the FTC brought an enforcement action against a home security company for security failures that included granting employees "unmonitored access" to user data. Complaint at 7, Fed. Trade Comm'n v. Ring LLC, Case No. 1:23-cv-01549 (D.C., May 31, 2023). The FTC also brought a 2023 enforcement action against an online retailer following a breach that exposed the personal information of millions of customers. Complaint, Drizly, LLC, Fed. Trade Comm'n Docket No. C-4780 (Jan. 9, 2023). In the Drizly order, the FTC noted that the company "failed to monitor and terminate [an] executive's access" to its code repositories, even when such access was no longer needed, which led to a malicious actor gaining access to the executive's account. It also noted a previous incident in which an employee posted his company credentials to a public repository, which has also led to a minor breach. Id. at 4. The FTC Drizly complaint stressed the companies' lack of "policies, procedures, and technical measures to address the security practices of employees" as a component of a failure of security that constituted unfair or deceptive practices. Id. at 5.

Considering the growing number of high-profile insider incidents in the financial services industry, additional regulatory requirements at both the federal and state level may be established in the near future.

ELECTRONIC COMMUNICATIONS MONITORING – STATE LAW

States and local jurisdictions have enacted a variety of laws that have implications for employers' implementation of insider threat programs. As addressed below, these laws cover and include electronic monitoring in the workplace, wiretap statutes, restrictions on credit checks, anti-discrimination laws, and laws restricting the ability of employers to use certain information, such as the lawful outside activities of employees, social media accounts, or salary history of prospective employees.

State Law Limitations on Monitoring

Several states have enacted statutes that specifically address electronic monitoring in the workplace. Nebraska permits employers to intercept employees' communications without their consent. Neb. Rev. Stat. § 86-702(2)(a). Connecticut, Delaware, and New York, by contrast, require private employers to inform employees of any monitoring. Conn. Gen. Stat. Ann. § 31-48d; Del. Code Ann. tit. 19, § 7-705; N.Y. Civ. Rights Law § 52-C. While providing employees notice of monitoring is always a best practice, as noted above, firms that operate in Connecticut, Delaware, and New York should be especially careful to fully disclose their monitoring policies. In California, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), provides employees with the same rights concerning their data as consumers. For example, businesses must provide notice to employees of how employee data is collected and used, employees are able to access the personal information that employers collect, and employees have the right to limit the use of their sensitive personal information. Cal. Civ. Code § 1798.

Nearly every state has enacted a law analogous to the federal Wiretap Act. While most state wiretap statutes mirror the federal law's requirements and exceptions, a dozen states—California, Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania and

Washington—require the consent of all parties to a communication for monitoring to be legal under the statutes' consent exceptions. In theory, a firm could violate all-party consent wiretap statutes if it intercepts messages received by an employee from a third party who was not warned of the monitoring. However, the state courts that have considered the issue have interpreted their respective statutes to allow such interceptions. See, e.g., State v. Townsend, 105 Wash. App. 622, 20 P.3d 1027, 1031 (2001) (noting that "[a] person sends an e mail message with the expectation that it will be read and perhaps printed by another person … that person thus implicitly consents to having the message recorded on the addressee's computer"); see also Restuccia v. Burk Tech., No. 95-2125, 1996 Mass. Super. LEXIS 367 (Mass. Super. Ct. Nov. 4, 1996) (dismissing a Massachusetts wiretap act claim brought against an employer, reasoning that the employer's email monitoring was not unlawful because it was in the "ordinary course of business"). Nevertheless, firms located in states requiring consent of all parties to a communication should consult with legal counsel to determine the best way to protect themselves against claims under all-party consent wiretap statutes, and they should consider including a monitoring warning in all emails sent from company email addresses.

Most states recognize the tort of intrusion upon seclusion that generally imposes liability for intentional intrusions upon the plaintiff's solitude or private affairs that would be highly offensive to a reasonable person. See Restatement (Second) of Torts § 652A (1977). A number of plaintiffs have attempted to bring intrusion upon seclusion actions against employers for electronic monitoring, but the vast majority are unsuccessful because of the tort's requirement that the employee has "an objectively reasonable expectation" of privacy in the place of intrusion. Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 490 (1998). It is well-settled that courts have found that workplaces are not sufficiently private spaces for an intrusion upon seclusion to occur. *See, e.g., Marrs v. Marriott Corp.*, 830 F. Supp. 274, 283 (D. Md. 1992) (finding "no support for the conclusion that [the plaintiff] had a reasonable expectation of privacy in an open office."); *Jackson v. Nationwide Credit, Inc.*, 206 Ga. App. 810, 812, 426 S.E.2d 630, 632 (1992) (stating that its it not an "unreasonable intrusion" for an employer to monitor telephones when all employees were advised that telephones were monitored). To bolster these defenses, however, employers should ensure that their notices of electronic monitoring are sufficiently clear and publicized such that employees cannot claim that they have a reasonable expectation of privacy in their online activities or telephone conversations in the workplace.

Some states have enacted laws restricting the ability of employers to base employment decisions on certain activities of employees or prospective employees outside of the workplace. For example, New York prohibits employers from refusing to hire, or otherwise discriminating against, individuals (in terms of compensation, promotion, or other privileges) because of the individual's political activities outside of work, legal use of consumable products outside of work hours, recreational activities outside of work hours, or union membership. N.Y. Lab. Law § 201-d.

Financial institutions should also be aware that some local jurisdictions, including prominent financial centers like New York City and Philadelphia, have passed local laws restricting the ability of employers to conduct inquiries into the salary history of potential employees and from seeking to obtain such information by searching public records. For example, in May 2017, New York City passed Local Law 67 that prohibits employers from inquiring about a prospective employee's salary history during all stages of the interview process. If the employer already knows the applicant's past salary information, Local Law 67 prohibits the employer from relying on such information in determining the potential candidate's pay. Similar laws have been passed in California, Massachusetts, Delaware, and Oregon.

State Law – Duty to Monitor

Some states also require firms to implement policies, procedures, and controls to monitor employees, as well as contractors and other persons, who have access to systems and data. For example, the New York Department of Financial Services' cybersecurity regulation requires covered entities to "implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users." 23 NYCRR 500.14(a); 23 NYCRR 500.1(b) (defining "authorized user" to mean "any employee, contractor, agent or other person that participates in the business operations of a covered entity and is authorized to access and use any information systems and data of the covered entity"). Further, the regulations require "effective continuous monitoring, or other systems to detect on, an ongoing basis, changes in information systems that may create or indicate vulnerabilities." 23 NYCRR 500.05. In the absence of effective continuous monitoring, entities covered by the regulation must conduct annual penetration testing and bi-annual vulnerability assessments. Id.

State attorneys general have also brought enforcement actions against companies for failing to properly monitor their information systems. In 2023, a healthcare company paid $2.5 million to settle charges over improper data security controls brought by the New Jersey, Florida, and Oregon Attorneys General following a data breach. Assurance of Voluntary Compliance, In the Matter of EyeMed Vision Care LL, (May 16, 2023). The company's failure to properly monitor employee email access and to identify "when a user searched and what a user searched for" was one of the key failures cited in the complaint. Id.

BACKGROUND CHECKS AND SCREENING

Criminal background checks, and to some extent, financial background checks, have long been a routine part of the hiring process at most firms. A candidate's financial history may be indicative of the candidate's character, as well as the candidate's propensity to commit insider theft or fraud. Employers may therefore wish to obtain a consumer report or an investigative consumer report about a prospective employee. As individuals have increasingly shared information about themselves online, some firms have also begun to incorporate online searches into their screening processes as well. Taken together, background checks and screening can uncover information critical to determining whether a prospective employee poses an insider threat risk. However, the scope of such screening is not unlimited—federal and state laws in the United States regulate the gathering of information about certain aspects of candidates' backgrounds. The following is a brief summary of laws and regulations that restrict what information employers can investigate in screening prospective employees.

The Fair Credit Reporting Act

In the United States, the procurement of third-party background check reports is governed by the Fair Credit Reporting Act ("FCRA"), as amended by the Fair and Accurate Credit Transactions Act (FACTA). Although FCRA only applies to consumer reports obtained from consumer reporting agencies (CRAs), some states—most notably California—have enacted more restrictive state statutes that apply to institutions that might not otherwise be CRAs under FCRA, including employers doing their own searches in-house. See, e.g., Investigative Consumer Reporting Act (ICRAA- CA Civil Code § 1786. In some instances, California law is broader than FCRA. Firms operating in California should consult local counsel to develop a background check policy.

Further, FCRA disclosure and consumer authorization requirements apply to employment reports with data obtained from public records. Employers should minimize their risk of exposure by complying with FCRA standards for all types of financial background investigations and screening and consult with legal counsel to determine whether conducting background checks or using them for employment decisions may be subject to additional restrictions under state law.

FCRA does not generally restrict what information may be obtained in background checks, but rather how it is obtained. The law applies to any information obtained in a consumer report, which is broadly defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living . . .." 15 U.S.C. § 1681a(d)(1). An employer must provide a clear, conspicuous, written notice to an applicant or current employee (separate from the job application) and obtain his or her consent to conduct the background check or obtain a report. § 1681b(b)(2). Notice and consent to an applicant can extend to reports obtained throughout the course of employment, if the notice clearly states so. See Using Consumer Reports: What Employers Need to Know, FTC (Jan. 2012). This type of "blanket authorization" may prevent the problem of disgruntled insiders acting out upon receiving notice that the employer has requested their consumer reports.

Should the firm decide to deny employment based on the contents of the report, it must inform the applicant of its decision in a "pre-adverse action" letter, and upon finalization of the decision, a second letter explaining the applicant's rights, including the right to dispute the report with the CRA and the right to request a re-investigation. §§ 1681m(a); 1681b(b)(3). The FTC has also advised that applicants should be given a reasonable opportunity to review and discuss the report between when the first and second letters are sent. FTC Staff Opinion Letter, Lewis (06-11-98). Employers should consult the statutory provisions directly and obtain legal advice to ensure that they have implemented reasonable procedures to comply with all of the applicable provisions of FCRA.

Investigative consumer reports, though more onerous to obtain, may reveal more information about a job candidate or employee than a typical consumer report. In addition to the information included in consumer reports, investigative reports contain information obtained from interviews with neighbors, friends, associates, or acquaintances of the report subject. FCRA imposes extra requirements for such reports, including that notice must be provided within three days after a report is requested, § 1681d(a)(1)(A), and it must include a summary of the individual's rights under FCRA. § 1681d(a)(1)(B). Additionally, upon a timely request, the employer must provide a complete and accurate disclosure of the nature and scope of the investigation. § 1681d(b). Although there are no prohibitions against obtaining blanket authorizations from prospective employees to procure investigative reports in the future, such authorizations carry greater practical compliance risks, as they may not sufficiently describe the "nature and scope" of future investigations or give meaning to a future employee's rights.

Notably, however, the FACTA amended FCRA to allow employers to hire outside investigators to conduct investigations into certain types of employee wrongdoing. The amended FCRA provision exempts communications that would otherwise be "investigative consumer reports" from the notice requirements for such reports if the purpose for the communication is to investigate suspected misconduct related to the employer or to comply with federal, state, or local laws; rules of a self-regulatory organization; or any preexisting written policy of an employer. 15 U.S.C. § 168la(y)(1). However, to qualify for this exemption, the report must not be made for the purpose of investigating creditworthiness, and it cannot be provided to any person except the employer, the government, a self-regulatory organization, or as required by law. Id. However, if an employer takes adverse action based on this type of report, it must provide the affected employee with a summary of the nature and substance of the report, although it need not disclose its sources of information. § 168la(y)(2).

RESTRICTIONS ON EMPLOYER CREDIT CHECKS

A number of cities and states restrict the ability of employers to conduct credit checks on job applicants and current employees. For example, New York City prohibits employers from requesting or

using the credit history (including creditworthiness, credit capacity, payment history, credit accounts, bankruptcies, credit card debt, and other elements) of job applicants and employees to make employment-related decisions. In California, most prospective employers are prohibited from using consumer credit reports to make employment decisions, unless the position in question has one of several enumerated characteristics (including, for example, positions that are managerial, that involve access to confidential or proprietary information, or that involve authorization to transfer money on behalf of the employer). Notably, financial institutions covered by the federal Gramm-Leach-Bliley Act are exempt from this requirement under California law. Nevertheless, in circumstances where using a credit report is permissible in California, the law requires the employer to provide written notice to the person to whom the credit report belongs of the specific reason for obtaining the report. Other states with credit and background check restrictions include Colorado, Connecticut, Delaware, District of Columbia, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont, and Washington. Many state laws include an exemption for financial institutions, but firms should be aware of the requirements of these laws and how they might affect the implementation of an insider threat program.

Restrictions on Criminal History Checks

At the federal level, the Civil Rights Act of 1964 makes it illegal to check the background of applicants and employees when the decision is based on the individual's race, national origin, color, sex, religion, disability, genetic information (including family medical history), or age. Many states and local jurisdictions have similar anti-discrimination statutes in place. Some states have also enacted laws to specifically address when criminal history checks can be run on applicants or employees and how criminal history information can and cannot be used by employers. Additionally, as discussed above, checking applicant and employee backgrounds is also subject to limitations under the Fair Credit Reporting Act. The Equal Employment Opportunity Commission (EEOC) has issued guidance stating that considering an individual's criminal history may, under certain circumstances, violate Title VII of the Civil Rights Act because national data suggests that criminal history exclusions have a disparate impact on certain racial and ethnic minorities. See Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e et seq., No. 915.002 (April 25, 2012), https://www.eeoc.gov/laws/guidance/arrest_conviction.cfm (the "Guidance").

The Guidance states that an employer policy of excluding applicants based on their criminal histories violates Title VII unless the policy of exclusion is "job related and consistent with business necessity," based on the nature and gravity of the crime, the time elapsed since the crime was committed, and the nature of the job. Moreover, where such screening is used, employers must provide an opportunity for the individual to demonstrate that exclusion should not be applied to his or her particular circumstances. The Guidance also takes the position that arrest warrants cannot justify exclusion unless the conduct underlying the arrest renders the individual "unfit for the position in question." Notably, the EEOC acknowledges that in some industries, criminal background checks may be required by law, and compliance with federal laws and regulations is a defense to a charge of discrimination. Title VII also does not preempt federal statutes governing eligibility for occupational licenses or registrations in the financial industry.

As noted, at the state and local levels, some jurisdictions have enacted statutes that specifically limit the ability of employers to make inquiries into applicant and employee criminal history information. For example, under N.Y. Corr. L. § 752, employers may not discriminate against applicants with one or more criminal convictions unless the convictions directly relate to the position, or hiring the applicant would place others at an unreasonable risk of harm. Under the New York City Fair Chance Act and other state and local so-called "ban the box" laws, employers may not ask employees about their criminal history or run criminal

history background check reports until after extending a conditional offer of employment.

Firms must carefully weigh the benefit of criminal screening for the job in question with the potential risks of violating Title VII and ensure that their policies are developed and applied in such a manner that they do not engage in prohibited discrimination against employees or applicants. Although the appropriate way to comply will vary according to the particular circumstances, firms may consider limiting their exclusion policies to crimes that could cause harm to the firm—for instance, cybercrime, fraud, insider trading, or theft—and provide excluded individuals with an opportunity to contest the exclusion.

Social Media

While examining publicly available social media profiles can be an informative part of applicant screening, firms should be mindful that at least half of the 50 states have workplace privacy laws that prohibit employers from seeking access to an employee's personal online account (such as a social media account) or requiring employees to log into personal online accounts in the employer's presence. These statutes generally prohibit employers from requiring and/or requesting employees or applicants to 1) disclose a username or password from a personal social media account, 2) "friend" an employer, 3) access their personal profiles in the presence of an employer, and/or 4) change their privacy settings to allow employers to view a profile. See, e.g., Cal. Lab. Code § 980; Md. Code Ann., Lab. & Empl. § 3-712; 820 ILCS 55/10; Nev. Stat. Rev. § 613.135; N.Y. Legis. Assemb. A.836 (eff. March 12, 2024). A majority of these laws permit state agencies to fine non-compliant employers, and some create a private right of action for affected individuals. See, e.g., N.J. Stat. Ann. §§ 34:6B-9 (authorizing civil penalties of up to $1,000 for the first violation and $3,500 for each subsequent violation); Wash. Rev. Code § 49.44.200-205 (authorizing a private right of action to recover actual damages, a penalty of $500, and attorneys' fees and costs).

Most state social media statutes contain language clarifying that the laws do not prohibit employers from complying with federal, state, or self-regulatory organization (SRO) obligations. States that do not contain this exception in its broadest form—such as California, Colorado, and Maryland—have other exceptions that excuse compliance for investigations related to securities violations. Thus, these laws generally should not impede compliance with future federal government or self-regulatory organization standards for cyber risk protection. Further, these laws generally do not limit the employer's right to maintain lawful workplace policies regarding use of the employer's electronic equipment or email systems or to monitor usage of such equipment and systems.

Firms should consider putting safeguards in place to ensure that their human resources and other personnel involved in the hiring process are reviewing candidate social media consistently and in a manner that complies with applicable laws. For example, employees should be instructed to use only publicly visible online information to screen job candidates and check up on current employees. Employers must also ensure that information obtained about an employee's outside activities is not used to discriminate against employees or applicants in a way that violates anti-discrimination laws. To limit risks and to ensure a consistent approach to social media screening, some employers elect to engage third-party vendors to conduct social media background screenings and instruct its own employees to refrain from checking candidate social media themselves. If a vendor is engaged for this purpose, employers must comply with applicable FCRA disclosure and consumer authorization requirements.

WHISTLEBLOWER CONSIDERATIONS

In August 2011, pursuant to its mandate under Dodd-Frank, the SEC implemented rules to encourage and protect whistleblowers to report possible violations of the securities law. Under these whistleblower

protection rules, also known as Exchange Act Rule 21F-17, firms are prohibited from taking any action to impede an individual from communicating directly with SEC staff, including by "enforcing, or threatening to enforce, a confidentiality agreement." Exchange Act Rule 21F-17. Since 2011, the SEC has instituted more than twenty enforcement actions for a violation of Rule 21F-17. See, e.g., D.E. Shaw & Co, L.P., Exchange Act Release No. 98641 (Sept. 29, 2023); KBR Inc., Exchange Act Release No. 74619 (Apr. 1, 2015) (SEC's first enforcement action for a violation of Rule 21F-17 due to use of a restrictive confidentiality agreement). Firms should be aware of protections that are granted to whistleblowers and ensure that their insider threat programs comply with applicable whistleblower regulations.

The SEC rules define "whistleblower" broadly, and no actual violation needs to have occurred for whistleblower protection rules to apply. Any information that is related to a "potential" violation is covered. Firms should note that whistleblower protections only apply to employees who communicate with government agencies such as the SEC, meaning that communications to media or other sources are generally not protected.

Any contracts that employees sign that impose a duty of confidentiality on the employees should also provide an exception for voluntary communications with the SEC, and employees should never be prohibited or discouraged from making such disclosures. Further, employees that do communicate with the SEC should never face disciplinary actions or other negative consequences for the communications. Insider threat programs should consider these requirements and ensure that any language that ensures the protection of firm data creates an exception for protected whistleblower communications. If such programs uncover a whistleblower, firms should work with their legal counsel to confirm whether the whistleblower engaged in protected activity and if so, that their rights are protected.

OTHER JURISDICTIONS

Other countries' privacy and employment regulations and protections often differ significantly from those of the U.S. While firms should always consult local counsel in foreign jurisdictions where they intend to implement an insider threat mitigation program, this section provides a general overview of some of the principal laws that may impact such programs in Germany (as an example of an EU Member State), the UK, India, and Hong Kong.

The following chart summarizes some of the major foreign cybercrime, privacy, and human resources laws in these jurisdictions that are applicable to insider threat mitigation programs:

Law Category	Germany/EU	United Kingdom	India	Hong Kong
Cybercrime	Budapest Convention on Cybercrime[25] Criminal Code	The Computer Misuse Act 1990[27] Budapest Convention on Cybercrime	Information Technology	Computer Crimes Ordinance (No.

[25] Convention on Cybercrime, ETS No. 185, 23 November 2001, available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (last visited on February 21, 2024).

[27] Available at https://www.legislation.gov.uk/ukpga/1990/18/contents.

	(Strafgesetzbuch)[26]	Investigatory Powers Act 2016[28]	Act 2000[29] Indian Penal Code 1860[30]	23 of 1993)[31]
Privacy	EU General Data Protection Regulation (GDPR)[32] Federal Data Protection Act (Bundesdaten schutzgesetz)[33]	UK Data Protection Act 2018[34] The UK General Data Protection Regulation (UK GDPR)	The Information Technology (reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[35] Digital Personal Data Protection Act 2023[36] [Not in force as of the date of publication.]	Personal Data (Privacy) Ordinance (Cap. 486)[37]
Human Resources	Works Constitution Act (Betriebsverfas	Human Rights Act 1998[41] UK Equality Act	The Indian Contract Act 1872[45] The Indian	Employment Ordinance (Cap. 57)[49]

[26] Strafgesetzbuch **(**StGB) (Criminal Code), 13 November 1998 (Federal Law Gazette I, p. 3322), available at: https://www.gesetze-im-internet.de/englisch_stgb/ (last visited on February 21, 2024).

[28] Available at https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[29] Available at https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C.

[30] Available at https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362.

[31] Available at https://www.elegislation.gov.hk/hk/cap200!en@2021-10-08T00:00:00?INDEX_CS=N.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. (L 119) 1 (4 May 2016), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (last visited on February 21, 2024).

[33] Bundesdatenschutzgesetz (BDSG) (Federal Data Protection Act), 30 June 2017 (Federal Law Gazette I p. 2097), available at: https://www.gesetze-im-internet.de/englisch_bdsg/ (last visited on February 21, 2024).

[34] Available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[35] Available at https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules.

[36] Available at https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[37] Available at https://www.elegislation.gov.hk/hk/cap486.

[41] Available at https://www.legislation.gov.uk/ukpga/1998/42/contents.

[45] Available at https://www.indiacode.nic.in/bitstream/123456789/2187/2/A187209.pdf.

[49] Available at https://www.elegislation.gov.hk/hk/cap57.

	sungsgesetz)[38] General Act on Equal Treatment (Allgemeines Gleichbehandlungsgesetz)[39] Whistleblower Protection Act (Hinweisgeberschutzgesetz)[40]	2010[42] Employment Rights Act 1996[43] Public Interest Disclosure Act 1998[44]	Penal Code 1860 Rights of Persons with Disabilities Act 2016[46] Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal Act) 2013[47] Equal Remuneration Act, 1976[48]	

THE EU: The GDPR

The European Union's GDPR is an expansive data protection law reflecting that data protection is a fundamental individual right. The GDPR governs all EU Member States, without the need for a domestic implementing act. Charter of Fundamental Rights of the European Union, Art. 8, 2012 O.J. (C 326/391), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (last visited on February, 21 2024).

The EU GDPR seeks to protect this right. The EU GDPR is uniform law in the EU and governs all EU

38 Betriebsverfassungsgesetz (BetrVG) (Works Constitution Act), 25 September 2001 (Federal Law Gazette I, p. 2518), available at: https://www.gesetze-im-internet.de/englisch_betrvg/englisch_betrvg.html (last visited on February 21, 2024).

39 Allgemeines Gleichbehandlungsgesetz (AGG) (General Act on Equal Treatment), 14 August 2006 (Federal Law Gazette I, p. 1897), available at: https://www.gesetze-im-internet.de/englisch_agg/ (last visited on February 21, 2024).

40 Hinweisgeberschutzgesetz (HinSchG) (Whistleblower Protection Act), 31 May 2023 (Federal Law Gazette I, Nr. 140), available at: https://www.gesetze-im-internet.de/hinschg/BJNR08C0B0023.html (in German) (last visited on February 21, 2024).

42 The U.K. Equality Act, available at https://www.legislation.gov.uk/ukpga/2010/15/contents.

43 Available at https://www.legislation.gov.uk/ukpga/1996/18/contents.

44 Available at https://www.legislation.gov.uk/ukpga/1998/23/contents.

46 Available at https://www.indiacode.nic.in/bitstream/123456789/15939/1/the_rights_of_persons_with_disabilities_act%2C_2016.pdf.

47 Available at https://www.indiacode.nic.in/handle/123456789/2104?sam_handle=123456789/1362#:~:text=An%20Act%20to%20provide%20protection,connected%20therewith%20or%20incidental%20thereto.&text=Notification%3A,%2C%202013%2C%20vide%20notification%20No.

48 Available at:. https://labour.delhi.gov.in/labour/equal-remuneration-act-1976#:~:text=The%20Act%20provides%20that%20no,in%20such%20establishment%20or%20employment.

Member States, without the need for a domestic implementing act.

The GDPR applies to the processing of personal data of individuals ("data subjects"), irrespective of the individual's nationality. Personal data includes any information relating to an identifiable individual and may relate to name, address, or identifiers such as Internet Protocol addresses, biometric information, including behavioral traits, or workplace performance. The GDPR is technologically neutral and applies to the processing of personal data by automated means, as well as to manual processing if the personal data is to be contained in a filing system.

The GDPR's reach is vast and extends beyond the EU's borders. First, it applies to organizations established in the EU/European Economic Area ("EEA"), irrespective of whether the processing of data occurs in or outside of the region. Second, it applies to organizations established outside the EU/EEA, if the organizations offer goods or services to individuals in the EU/EEA or monitor their behavior from abroad.

The EU GDPR imposes responsibilities on "data controllers," who determine the means and purposes of the processing of personal data, and "data processors," who carry out processing activities on behalf of controllers. The processing of personal data is guided by principles such as lawfulness, transparency, purpose limitation, data minimization, storage limitation, integrity, and confidentiality.

The GDPR provides for several legally permissible uses of individual data including the necessity for the performance of a contract (including an employment contract) and the necessity for the legitimate interest of the controller unless the interest is overridden by the individual interest in data protection. Informed consent by an individual that was freely granted is also a legally permissible exception unless it is revoked with future effect. The processing of sensitive personal data, such as biometric or health data, requires additional legal bases/permissions.

Individuals have data subject rights, such as the right to information prior to the processing,, the right to access, and to have their personal data permanently erased. If the processing is based on the legitimate interest of the controller, the individual can also object to the processing, unless the controller can show compelling legitimate interests. The controller and processor must implement appropriate technical and organizational measures to ensure processing complies with the EU GDPR. Such measures may include restricting access to personal data or training staff.

Regarding the security of processing, the controller and processor shall implement appropriate technical and organizational protection measures, including ensuring that any person who has access to personal data does not process it except on instructions from the controller. The controller must notify the data protection authority within 72 hours at the latest if a personal data breach occurs and rises to the level of a likely risk to the rights and freedoms of the data subject, such as the risk of identity theft or fraud. If the breach is likely to result in a high data protection risk, the breach must be communicated to the individual without undue delay. The controller conducts a data protection impact assessment if the processing is likely to result in a high risk to data protection rights. Such risk stems, e.g., from a systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling. When conducting the assessment, the controller shall seek the advice of the data protection officer.

An organization is required to appoint a data protection officer if the core activities of the controller or processor consist of processing operations that require regular and systematic monitoring of individuals on a large scale. As determined by the regulators, large-scale processing includes the processing of customer data by a bank in the regular course of business. See Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ("DPOs") (WP 243 rev.01), December 13, 2016 as revised and adopted on 5 April 2017,

p. 8, available at https://ec.europa.eu/newsroom/article29/items/612048 (last visited on February 21, 2024).

The controller conducts a data protection impact assessment if the processing is likely to result in a high risk to data protection rights. Such risk stems, e.g., from a systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling. When conducting the assessment, the controller shall seek the advice of the data protection officer.

Data transfers to non-EU countries are only permitted if the recipient can ensure the perpetuation of EU GDPR standards. Compliance can be demonstrated if the recipient resides in a jurisdiction that benefits from an EU adequacy decision or by implementing appropriate safeguards such as entering into standard contractual clauses. If these requirements cannot be met, a data transfer may rely on narrowly construed exceptions, such as the necessity of the organization to defend its case in a court outside of the EU/EEA.

Data protection authorities in every EU Member State monitor and enforce the EU GDPR. A failure to comply with the EU GDPR may result, depending on the nature of the infringement, in administrative fines of up to 20 million euros or 4% of the annual (group) turnover, whichever is higher. EU Member States' criminal laws provide criminal sanctions for certain data protection violations. In addition, the data subject who has suffered pecuniary or non-pecuniary damage has a right to compensation from the controller or processor.

The GDPR has provisions specifically applying to the employment context. Regarding the processing of personal data in an employment context, the EU GDPR permits Member States to enact more specific rules. The EU Whistleblower Directive, as implemented by EU Member States, protects the employee reporting on breaches of EU data protection or cybersecurity violations from any kind of retaliation. Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 on the protection of persons who report breaches of Union law, O.J. (L 305) 17, 26.11.2019, available at: https://eur-lex.europa.eu/EN/legal-content/summary/protection-of-persons-who-report-breaches-of-eu-law.html#:~:text=WHAT%20IS%20THE%20AIM%20OF,or%20omissions%20and%20abusive%20practices (last visited on February 21, 2024). The expected effect of the new law is that more infringements come to the attention of the authorities.

A financial firm's insider threat program must comply with the EU GDPR, as may be specified by Member State legislation. National regulators, also when convening in the European Data Protection Board, issue guidance, which, with case law, specifies the framework. Relevant guidance also in the employee context includes the European Data Protection Board, Guidelines 05/2020 on Consent under Regulation (EU) 2016/679, 4 May 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited on February 21, 2024) and European Data Protection Board, Guidelines 3/2019 on the Processing of Personal Data Through Video Devices, January 29, 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (last visited on February 21, 2024). When structuring an insider threat program, it is important to consider that employees in the EU have a high expectation of employer data protection compliance. The balance between the employer's legitimate interest to protect its business and the employee's expectation of privacy often tips in favor of the employee.

In line with the transparency principle, the employee has the rights to be informed about the monitoring, its specified legitimate purpose, and to access the information collected. The data minimization principle calls for the collection of no more information than is necessary in relation to the purpose and for storage for no longer than is required.

Employee consent is viewed critically by European regulators as a valid legal basis because of the typical power imbalance between the employer and the employee may affect the voluntariness of employee consent. See European Data Protection Board, Guidelines 05/2020 on Consent under Regulation (EU) 2016/679, May 4, 2020, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en (last visited on February 21, 2024). Rather, the necessity to perform the employment contract or the legitimate interest of the employer may form the legal basis for the monitoring.

In all cases, the monitoring of employees must be a proportionate response to the risks faced by an employer with the least intrusive method being employed.

Data protection authorities enforce the EU standards in the context of monitoring employees vigorously: In 2023, the French Data Protection Authority (Commission Nationale Informatique & Libertés) imposed a 32 million euros fine on an Amazon entity in France managing the group's warehouses in France. In the agency's view, the collection of employees' personal data using a scanner to document their work performance in great detail was "excessively intrusive", lacked a lawful basis, was not transparent, and violated the principle of data minimization

EU Whistleblower Directive

Another piece of potentially relevant legislation for companies to consider is the EU Whistleblower Directive, which protects the employee reporting on breaches of EU data protection or cybersecurity violations from any kind of retaliation. The Directive must be implemented within each Member State jurisdiction through local implementing legislation, and countries can "gold plate" the Directive by imposing even stricter requirements at a national level, so it is important to consult the local law of each relevant jurisdiction. The expected effect of the new law is that more infringements come to the attention of the authorities.

Germany: Employee Data Protection

The primary source of data protection legislation in the EU Member State of Germany is the EU GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. (L 119) 1 (May 4, 2016), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (last visited on February 21, 2024). The Federal Data Protection Act (*Bundesdatenschutzgesetz*, "BDSG") complements the EU GDPR and calls, e.g., for the appointment of a data protection officer if, as a rule, a controller continuously employs at least 20 persons dealing with the automated processing of personal data.

Sec. 26 BDSG specifies the data protection requirements in the employment context. Following a 2023 ruling of the European Court of Justice, however, it is unclear whether this provision is still applicable or if the more general legal bases of the EU GDPR apply, such as the legitimate interest of the employer not overridden by employee interest or the necessity for performing the employment contract. Bundesdatenschutzgesetz (BDSG) (Federal Data Protection Act), June 30, 2017 (Federal Law Gazette I p. 2097), available at: https://www.gesetze-im-internet.de/englisch_bdsg/ (last visited on February 21, 2024).

Either way, in many instances, the employer has to strike a balance between their interest in data processing and the employee's interest in the protection of their data. Freely given and informed employee consent can also form a legal basis for employee data processing. In practice, such consent is rarely used because German data protection authorities are concerned about the voluntariness of employee consent, and the employee can revoke their consent at any time with future effect.

Employee Monitoring

Unlike the legal framework in the United States, where employees have a limited expectation of privacy in their use of company Information Technology assets and systems, EU laws provide strong protection of data protection rights. For example, sec. 26 BDSG requires that any collection and use of employees' personal data during an investigation be supported by a documented suspicion that the collection is necessary, and that the employee does not have an overriding interest in prohibiting collection. The employer has to determine the monitoring purpose specifically prior to the investigation and choose the least intrusive method. Thus, open monitoring prevails over secret monitoring, and permanent surveillance is generally not permitted.

For example, the use of keyloggers is only permitted if there is concrete suspicion of a criminal offence or a serious breach of duty. Bundesarbeitsgericht (Federal Labor Court), 2 AZR 681/16, ECLI:DE:BAG:2017:270717.U.2AZR681.16.0, July 27, 2017, available at https://www.bundesarbeitsgericht.de/entscheidung/2-azr-681-16/ (last visited on February 21, 2024). Similar high standards apply to the monitoring of email accounts, and there are additional hurdles if the private use of emails is not prohibited.

In the context of video surveillance, the German Data Protection Conference (*Datenschutzkonferenz*) convening the German Data Protection Authorities, issued guidance that details the balancing of interests also in the employment context. Datenschutzkonferenz, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, July 17, 2020, available at: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html (last visited on February 21, 2024).

Companies allowing employees to use their personal devices to perform their responsibilities under the employment contract should adopt organizational and technical measures to efficiently protect employment-related data. Such measures may include software tools that separate professional and personal data on the employee's device.

In the financial industry, more specific standards may apply for the monitoring for risk management purposes and are outlined, for example, in the Banking Act (*Kreditwesengesetz*). Kreditwesengesetz (KWG) (Banking Act), September 9, 1998 (Federal Law Gazette I, p. 2776), available at: https://www.gesetze-im-internet.de/kredwg/ (in German), (last visited on February 21, 2024). Employers with a Works Council under the Works Constitution Act (*Betriebsverfassungsgesetz*), representing the interest of employees, have to respect the co-determination right of the body when introducing and using technical devices designed to monitor the behavior or performance of employees. Betriebsverfassungsgesetz (BetrVG) (Works Constitution Act), September 25, 2001 (Federal Law Gazette I, p. 2518), available at: https://www.gesetze-im-internet.de/englisch_betrvg/englisch_betrvg.html (last visited on February 21, 2024).

Background Checks

Background checks are generally permitted to the extent that the employer is entitled to obtain the information directly from the applicant, i.e., information that is directly linked to the position and relevant to the work performed. Within these limits, employers may, for example, check the background of an applicant by contacting their previous employers. Employers are not entitled to obtain an applicant's credit or criminal record directly from the relevant registers.

The General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz*) prohibits employment discrimination based on ethnic origin, gender, disability, religion, belief, age, and sexual orientation and may limit the scope of background checks, such as seeking information about union membership. Allgemeines Gleichbehandlungsgesetz (AGG) (General Act on Equal Treatment), August 14, 2006 (Federal Law Gazette

I, p. 1897), available at: https://www.gesetze-im-internet.de/englisch_agg/ (last visited on February 21, 2024).

Employee Termination and Disciplinary Measures

The breach of employee duties can result in disciplinary measures or termination. The Works Council must be consulted before each dismissal. See sec. 102 Betriebsverfassungsgesetz (BetrVG) (Works Constitution Act), September 25, 2001 (Federal Law Gazette I, p. 2518), available at: https://www.gesetze-im-internet.de/englisch_betrvg/englisch_betrvg.html (last visited on February 21, 2024). Evidence regarding employee misconduct may be inadmissible in subsequent termination proceedings if collected in violation of data protection laws. Bundesarbeitsgericht (Federal Labor Court), 2 AZR 296/22, ECLI:DE:BAG:2023:290623.U.2AZR296.22.0, June 29, 2023, available at https://www.bundesarbeitsgericht.de/entscheidung/2-azr-296-22/ (last visited on February 21, 2024).

Whistleblowing

The Whistleblower Protection Act protects broadly defined employees who report work-related breaches of data protection, cybersecurity, and related crimes from retaliation. Hinweisgeberschutzgesetz (HinSchG) (Whistleblower Protection Act), May 31, 2023 (Federal Law Gazette I, Nr. 140), available at: https://www.gesetze-im-internet.de/hinschg/BJNR08C0B0023.html (in German) (last visited on February 21, 2024). It is an administrative offense if a person hinders reporting or takes retaliatory measures.

Sanctions for Violations

The primary sanctions for data protection violations under the GDPR and the Federal Data Protection Act are administrative fines and damages. Violations of the General Equal Treatment Act may result in damages, with the employer having the burden to disprove the discrimination if facts so indicate.

UNITED KINGDOM Employee Data Protection

UK data protection law is governed by the Data Protection Act 2018 ("DPA 2018") which, *inter alia*, incorporates the General Data Protection Regulation into UK law (the "UK GDPR"). *See* Section 22 DPA 2018. While there are some minor differences between the two, the UK GDPR is almost identical to the GDPR. The UK's data protection authority is The Information Commissioner's Office (the "ICO").

The EU GDPR considerations outlined above therefore also apply in the UK. In particular, businesses should be mindful that the UK data protection law does not prevent them from monitoring or investigating employees, but they must do so in a way that is compliant with data protection requirements. It is important to remember that UK employees have a stronger right to, and expectation of, privacy in the workplace compared to American employees. The balance between the employer's legitimate interest to protect its business and the employee's expectation of privacy often tips in favor of the employee.

Background Checks

Employers may wish to conduct pre-employment background checks on individuals to help determine that they are not a threat to the business. The extent and nature of the information sought must be relevant to and justified by the position and proportionate to the risks faced. The aim should be to obtain specific information, as opposed to a general "fishing" exercise, that is based on reliable sources. The ICO's Employment Practices Code (the "Code") further recommends that:

- it is made clear to applicants very early on in the recruitment process that vetting will take place, including explaining how the vetting will be conducted;
- ideally, the checks themselves should be left to very late in the recruitment process, so that only successful applicants who have been selected for employment are subject to the background check; and

criminal offence data is only sought if it is relevant to the job being filled.

The Information Commissioner's Office, The Employment Practices Code, November 2011, as updated, "the Code". Available at:
.

Further, enquiries to third parties about an applicant's background should be confined to situations where there are particular and significant risks to the employer, clients, customers, or others and where there is no less intrusive and reasonably practicable alternative. See the Code, page 15.

Employee Monitoring

Many of the same considerations for employee monitoring in Germany also apply in the UK. While employee monitoring is not prohibited in the UK, and the ICO acknowledges that employees largely recognize that employers carry out checks on the quality and quantity of their work, the monitoring must be conducted in a way that is lawful and fair to workers, i.e., it must be necessary and proportionate. The ICO has published detailed guidance for employers in the form of the Code, and specific guidance on the monitoring of workers (the "Monitoring Guidance"). The Information Commissioner's Office, Employment practices and data protection: monitoring workers, October 2023. Available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/).

Any collection and use of employees' personal data during an investigation should be supported by a documented suspicion that the collection is necessary, and that the employee does not have an overriding interest in prohibiting collection. See Article 6(1)(f) UK GDPR. The employer must determine the monitoring purpose specifically prior to the investigation and choose the least intrusive method. See Article 5(1)(b) and Article 5(1)(f) UK GDPR. Thus, open monitoring prevails over secret monitoring, and permanent surveillance is generally not permitted. For example, the use of keyloggers is generally only permitted in very narrow circumstances, such as if there is concrete suspicion of a criminal offence or a serious breach of duty. Similar high standards apply to the monitoring of email accounts. The monitoring must also be conducted transparently and be addressed in any applicable employment policy or privacy policy. See Article 13 & 14 UK GDPR.

What constitutes necessary and proportionate employment monitoring has also shifted in recent years due to the rise in people working from home. The ICO recommends that businesses who monitor workers remotely should keep in mind that workers' expectations of privacy are likely to be higher at home than in the workplace. UK ICO, Monitoring Guidance, "Data protection and monitoring workers - can we monitor workers?" In particular, the risks of capturing family and private life information are higher as they can be inadvertently captured. Employers should be mindful of these differences when considering whether their monitoring activities are necessary and proportionate in the given context.

There are additional hurdles if employees use their private mobile devices or personal social media or instant messaging accounts for work-related purposes. This can be a particularly tricky area to navigate if the business does not have a policy making clear that there is no expectation of privacy in relation to business-related messages on employees' devices, including a contractual right (in the employment agreement) or blanket attestation form (signed by employees prior to an investigation) permitting the employer to access such messages. Notwithstanding such permission, businesses allowing employees to use their personal devices to perform their responsibilities under the employment contract should adopt organizational and technical measures to efficiently protect employment-related data. Such measures may include software tools that separate professional and personal data on the employee's device. The Monitoring Guidance recommends that employers avoid monitoring personal devices or accounts, and only review them where the reason (e.g., suspected criminal activity) is sufficient to justify the degree of intrusion involved. UK ICO, Monitoring Guidance, "Specific data protection considerations for different ways or methods of monitoring workers."

Finally, in the financial industry, more specific standards may apply for the monitoring of risk management purposes. Businesses should also be mindful that if the monitoring involves the interception of communications, the interception is not unlawful under section 3 of the Investigatory Powers Act 2016. Interceptions will be unlawful if the interceptor does not have lawful authority to carry out the interception and does not otherwise have a right to control the operation or use of the system the communication was intercepted from, or otherwise have express or implied consent to intercept the communication.

Employee Termination and Disciplinary Measures

A breach of employee duties can result in disciplinary measures or dismissal, provided they are implemented in accordance with any established company disciplinary procedures. Careful consideration should also be given to the potential termination of an employee with more than two years' service, as they might have the right not to be unfairly dismissed under the UK Employment Rights Act 1996 (the "ERA").

In order for an employee dismissal to be fair in the UK, the ERA requires the employer to have (1) a potentially fair reason for dismissing the employee; and (2) acted reasonably in the circumstances. The Advisory, Conciliation and Arbitration Service ("ACAS") has issued a Code of Practice on Disciplinary and Grievance Procedures (the "ACAS Code"), which applies to misconduct dismissals. Employers should consider this code when taking a decision to dismiss an employee. ACAS, Code of Practice on Disciplinary and Grievance Procedures, March 2015. Available at https://www.acas.org.uk/acas-code-of-practice-for-disciplinary-and-grievance-procedures/html

Potentially fair reasons for dismissal in an insider risk context may include that (1) the conduct of the employee is illegal or violates company policy; (2) the employee's continued employment would breach a statutory duty or restriction; or (3) "some other substantial reason."

Once a potentially fair reason is established, the employer must demonstrate that they acted reasonably based on the circumstances. An employer cannot dismiss someone simply based on "concerning behaviors" that has not been investigated properly. Rather, the employer must demonstrate that the dismissal is substantively fair and procedurally fair:

- Substantial fairness**:** the decision to dismiss an employee must be within the range of reasonable responses that a reasonable employer in those circumstances would adopt. This will depend on the severity of the employee's conduct.
- Procedural fairness: an employer must also follow a fair procedure when investigating allegations of misconduct and considering dismissing employees. This may include:
  - Appropriately investigating the issues or allegations, such as reviewing evidence, speaking to witnesses, and producing a report;
  - Informing the employee of the issues in writing;
  - Ensuring the employee is made aware of their right to be accompanied;
  - Conducting a disciplinary hearing or meeting with the employee;
  - Informing the employee of the decision in writing; and
  - Giving the employee a chance to appeal.

Whistleblowing

The Public Interest Disclosure Act 1998 grants legal protection to individuals (whistleblowers) who raise concerns of potential wrongdoing in the workplace. It covers individuals who disclose information which, in their reasonable belief, is made in the public interest and tends to show that *inter alia* a criminal offence or failure to comply with a legal obligation (including regulatory requirement) has, or is likely, to occur. If an individual makes such a "protected disclosure" they are protected from detrimental treatment by the employer,

including dismissal.

Such protection could, therefore, extend to employees who surface concerns as whistleblowers relating to cybersecurity incidents and related crimes, and would therefore protect them against any retaliation. This requirement can be particularly tricky to navigate because a whistleblower may not always identify as, or realize they are entitled to the protection of, a whistleblower when they make a disclosure. Businesses should therefore be continuously mindful of whether such protections could apply.

Sanctions for Violations

The UK GDPR gives individuals a right to receive compensation if they have suffered harm as a result of a business breaching one of its obligations under the UK GDPR; it is therefore a narrow right. See Article 82 UK GDPR. Further, employees who have been unfairly dismissed may be entitled to compensation or even reinstatement of their role. See Chapter II of the ERA.

INDIA Employee Data Protection

India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the "IT Rules"), issued under the Information Technology Act 2000, regulate the collection, processing, and use of personal information by organizations in India. Adopting a similar definition to the GDPR, the IT Rules define personal information as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person."

The IT Rules permit businesses to process individuals' non-sensitive personal data. However, written consent of the individual is required if a business processes their sensitive personal data (such as account passwords, and financial and medical information) in addition to other restrictions.

It is important to note, though, that India's data protection framework is set to be significantly overhauled by the new Digital Personal Data Protection Act 2023 ("DPDPA"). The DPDPA was enacted on 11 August 2023, however, as of the date of publication of this chapter, its provisions are yet to come into force. While this is expected to happen in 2024, there is no fixed date for implementation.

The processing of employee personal data is recognized as "legitimate use" for the purpose of data processing. Consequently, the personal data of employees can be processed, without the need to obtain consent, where one of the following applies: (i) the processing is for the purposes of their employment; or (ii) the processing is related to safeguarding the employer from loss or liability; or (iii) for the provision of any service or benefit sought by a data principal (i.e., data subject) who is an employee. See Section 7(i) DPDPA.

Where data is collected and processed under these DPDPA provisions, the data controller must implement reasonable security safeguards as well as appropriate technical and organizational measures to prevent personal data breaches. See Section 8(4)-(5) DPDPA. There is no prescribed data retention period under the DPDPA. Therefore, to the extent that an employer is able to justify the duration of retention of employee personal data (e.g., safeguarding the employer against loss or liability), they may retain it for such a specific period of time.

Employment Law

Indian employment law does not include provisions that directly govern employee screening. However, as noted above, under the current IT Rules, an individual's written, informed consent should be obtained before collecting any sensitive personal information or data. As a result, credit or financial checks, fingerprinting, and medical screening should be obtained only after obtaining such consent.

Although India has a Persons with Disabilities Act, it is much weaker than analogous protections in the United States, and some employers have conditioned employment on successful medical testing. Women are

protected by the Industrial Law and the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act and the Equal Remuneration Act, 1976. Additionally, government employees are protected by Article 15 of the Indian Constitution, which prohibits state discrimination based on "religion, race, caste, sex, or place of birth."

Background Checks

Background checks are generally permitted under Indian law, provided they are carried out in compliance with Indian data protection laws. In practice, the lack of centralized and updated information in India can make conducting checks difficult. To alleviate concerns surrounding background checks for IT professionals, the Indian National Association of Software and Service Companies (NASSCOM) created a National Skills Registry, and other industries have followed suit. Available at https://nationalskillsregistry.com/aboutus.htm#:~:text=National%20Skills%20Registry%20is%20a,along%2Dwith%20background%20check%20reports.

Whistleblowing

In India, there is no law that mandates the implementation of whistleblower protections in private, unlisted companies. The implementation of such protections is at the discretion of each company. While the Whistle Blowers Protection Act 2014 provides a mechanism for the reporting of illegal and unethical whistleblowing practices within organizations, the Act is limited to public sector undertakings and public servants. Similarly, the Companies Act 2013 obliges certain listed companies to incorporate minimum protections through whistleblower policies.

HONG KONG Employee Data Protection

The key privacy law in Hong Kong applicable to monitoring employees is The Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), which is overseen by the Office of Privacy Commissioner for Personal Data (the "PDPC").

The PDPO sets out the six Data Protection Principles ("DPPs") that are the basic requirements that data users must comply with in the handling of personal data, including employees' personal data collected during monitoring activities. While contravention of the DPPs is not an offence, the Privacy Commissioner may serve an enforcement notice on data users for contravention of the DPPs, and contravention of such a notice does constitute an offence.

The PDPC has issued a Code of Practice on Human Resource Management (the "Code") that is designed to give practical guidance to data users who handle personal data in performing human resource management functions and activities, including conducting background checks on potential employees. Office of Privacy Commissioner for Personal Data, Code of Practice on Human Resource Management, June 2001. Available at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/ehrm_e.pdf. Failure to abide by the mandatory provisions of the Code will weigh unfavorably against the data user concerned in any case that comes before the PDPC.

The PDPC has also issued privacy guidelines on Monitoring and Personal Data Privacy at Work" (the "Monitoring Guidelines"). Office of Privacy Commissioner for Personal Data, Privacy Guidelines: Monitoring and Personal Data Privacy at Work, December 2004. Available at https://www.pcpd.org.hk/english/publications/files/monguide_e.pdf.Although the Monitoring Guidelines are only best practice and businesses are not obliged to follow them, the DPDC would consider their adherence (among other factors) when determining whether there has been a breach of the DPPs.

Employers must ensure that they do not contravene the DPPs while monitoring employee's online activities. In particular, employers must ensure that (i) monitoring is only carried out to the extent necessary to deal with their legitimate business purpose, see DPP 1(1)(a) & (b), (ii) personal data collected in the course of monitoring are kept to an absolute minimum and by means that are fair in the circumstances, see DPP 1(1)(c) & (2)(b), and (iii) a written privacy policy on employee monitoring has been implemented and practicable steps have been taken to communicate that policy to employees. See DPP 1(3) & DPP 5. It should be noted that in any investigation by the PDPC, employers may be called upon to explain and prove, among other things, that they have complied with the above requirements.

The Monitoring Guidelines recommend employers undertake a systematic assessment before determining whether employee monitoring is the best option given the risks and activities that the employer seeks to manage. If the employer does decide to monitor, the Monitoring Guidelines recommend the implementation of a comprehensive written privacy policy that governs personal data management practices relating to employee monitoring (i.e., an Employee Monitoring Policy). See Section 3.2 of the Monitoring Guidelines for further details on the information included in the Employee Monitoring Policy.

A data subject may institute civil proceedings in the Hong Kong courts claiming damages under section 66 of the PDPO. While there has been no case in Hong Kong where an employee (or former employee) has successfully claimed for damages against the employer in relation to the use of workplace monitoring, the PDPC has held that an employer who logged into the employee's computer to collect cookies without notifying her amounted to unfair collection of personal data in breach of DPP 1(2). Further, the PDPO also held that the employer had not taken all practicable steps to ensure that the employee was aware of the monitoring policy, thus in breach of DPP 5. Numerous complaints also are made every year to the Enforcement & Complaints Section of the PDPC, some of which result in corrective action by the regulator.

Background Checks

There are generally no constraints on conducting background checks of potential employees. Nevertheless, an employer must ensure that when conducting background checks, it does not collect personal data that is excessive in relation to the purpose and that the selection method employed for data collection is not unfair. See DPP 1(c) & (2). Moreover, paragraph 2.7.2 of the Code (non-mandatory provisions) provides that "[a]s a matter of good practice, an employer should inform a job applicant before the selection method is used of its relevance to the selection process and the personal data to be collected by the chosen method."

Employee Termination and Disciplinary Measures

Generally, an employer is only permitted to summarily terminate employment in the event of the employee's misconduct being so serious or grave that it amounts to a rejection of the employee's contractual obligations. Where an employer terminates the employment of an employee without sufficient cause, the employer's unlawful action will amount to wrongful termination. There is no statutory requirement in Hong Kong regarding a fair process prior to dismissal, and it is not mandatory for employers to implement grievance and disciplinary procedures. However, the Hong Kong Labor Department does recommend including such procedures in its "Guide to Good People Management Practices". Hong Kong Labor Department, Guide to Good People Management Practices, June 2019. Available at https://www.labour.gov.hk/eng/public/wcp/practice.pdf. Such procedures will be important to support that an employee's termination was in good faith and was due to the behavior or performance of the individual rather than some other potentially unlawful reason, such as discrimination.

Whistleblowing

In Hong Kong there is no specific legislation for the protection of employee whistleblowers. Moreover,

while listed companies are encouraged to implement whistleblowing policies and procedures under the Code on Corporate Governance Practices in the Main Board Listing Rules, there is no legal obligation for employers to do so.

APPENDIX A- CASE STUDIES

Details regarding actual cases of insider attacks are often difficult to come by, given that organizations typically try to keep such incidents confidential where possible. However, we have developed a set of anonymized case studies of reported insider incidents that have recently occurred at financial institutions. These case studies were selected not only as cautionary tales of the damage that insiders can inflict by exploiting firm systems, but also as teaching tools to highlight common types of risks that may be overlooked. Accordingly, each summary is accompanied by key take-away points and suggestions as to how firms can guard against similar types of incidents. We encourage you to use these in training and communication opportunities within your firm as they drive home some of the challenges firms face in this area and help bring the risks alive with real-world incidents.

CASE #1

An application manager at a large bank managed an application that supported a commercial banking division focused on mergers & acquisitions. The app manager discovered he could see information about pre-deals in negotiation when he logged in.

During the same time, the app manager began to date a young woman and as the relationship progressed, so did the relationship with her father. When they discussed his job, the father asked the app manager more about what he could see in the unannounced merger or acquisition fields of the application.

The app manager began to pass "love notes" to his girlfriend that were insider deal tips to be given to the girlfriend's father. The father began to successfully conduct trades based on the information provided by the application manager. As the application manager realized the success as well as the ease of extracting pre-announced information, he shared with friends at other firms via code words and encrypted messages to try and avoid detection.

Over a period of three years, the insider trading ring made around $5M. A third party alerted law enforcement and the bank to these activities. This application manager had authorized access to the information as part of his day-to-day job. The application manager discovered a way around this reporting to try and avoid detection.. He could 'hover' over the pre-announcement fields to garner the information thinking he could not be detected. It was discovered the application manager was inside the application much longer than anyone else in his peer group, and even longer than the businesspeople responsible for the deal. When the insider was caught, he shared information about the insider trading ring with law enforcement. All were convicted of insider trading and received jail terms.

CASE #2

A senior engineer was interested in exfiltrating several confidential and strategic files from a large bank to use at another organization. The information contained details of a large strategic platform that could provide a significant competitive advantage for the company.

The senior engineer was well-regarded at the company and had authorized access to not only information of his current role but had retained access from prior roles as well. This allowed the senior engineer to retain files from his prior roles that were related to the strategic platform.

He compressed the files into a zip file on his company laptop. Through a process called steganography, the senior engineer created an innocuous sounding PowerPoint presentation "Family Vacations" and embedded the zip file containing confidential and strategic architecture renderings, source code and other information into an image in the PowerPoint and attempted to email the presentation to himself.

The Insider Threat team had developed a Splunk query to detect this methodology and was to identify the files attempting to be sent out.

When interviewed by the investigation team, the senior engineer feigned innocence and denied knowing about the embedded files. He told the investigators he was planning to resign from the company and wanted to take his family photos with him. The insider threat team proceeded to take the engineer's PowerPoint and demonstrated the extraction of confidential information. The senior engineer then admitted he planned to use this information at his new job.

CASE #3

DATA THEFT

Summary: Employee at a financial institution accessed and stole personally identifiable information and leaked the data to identity thieves.

Cause of the Incident: An insider at a financial institution used their access to customer banking records and stole customers' personally identifiable information, including names, addresses, Social Security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, email addresses, mother's maiden names, PINs and account balances, and sold the data to identity thieves. In one case, the identity thieves ordered boxes of checks and had them delivered to a UPS outlet to be picked up. They also allegedly contacted the financial institution via telephone and moved the victim's money into an account they controlled.

Action Taken: The financial institution discovered the theft of funds and contacted law enforcement. Ninety-five suspects associated with the identity theft ring were arrested by law enforcement.

Result: This breach affected hundreds of customers and the institution lost more than $10 million to the criminals.

Take-away: Track employee behavior on company systems and implement appropriate controls around access to sensitive information. Monitor employee access to consumer data for suspicious activity, including abnormally high volume of access to different consumer accounts.

CASE #4

POST-THEFT BREACH

Summary: Financial adviser impermissibly accessed and transferred data regarding client accounts to his personal server where it was thereafter obtained by Russian hackers and posted online.

Cause of the Incident: A financial adviser at a financial services company obtained confidential information for more than 500,000 client accounts without permission and uploaded the data to a personal server at his home. The insider used the data for his personal advantage in talks about a new job with competitors of the company. Russian hackers then obtained the client account information and posted it online.

Action Taken: The company discovered information for thousands of clients had been published online.

Result: The company investigated and fired the insider. The insider was arrested and pleaded guilty to one count of unauthorized access to a computer. Prosecutors sought a sentence of over three years in prison, but a federal judge sentenced the insider to three years' probation and $600,000 in restitution to the financial institution.

Take-away: Network monitoring software should be configured to alert monitoring personnel to high-volume data transfers. External transfer of sensitive files should be disabled for all users, with limited exceptions for designated positions where necessary. Implement an entitlement management function and put controls on what end-user can browse.

CASE #5

INSIDER TRADING

Summary: A corporate broker at a global financial services company passed confidential information on upcoming deals to a conspirator.

Cause of the Incident: The insider was a corporate broker at a global financial services company. The insider gleaned information on upcoming deals from his work and passed the information to accomplices, who would then place trades.

Action Taken: Regulatory authorities initiated an almost decade-long investigation into the suspicious behavior of the insider and his accomplices.

Result: The insider was convicted and sentenced to four-and-a-half years in prison. Another accomplice was sentenced to three-and-a-half years after being convicted of conspiracy to commit insider trading.

Take-away: Train employees on prohibitions against insider trading. Implement and enforce policies against sharing confidential nonpublic information. Install information security tools and behavioral analytics platforms.

CASE #6

NETWORK TAKEDOWN

Summary: Upon notice of unsatisfactory work performance, a computer engineer wiped company routers, shutting down 90% of networks.

Cause of the Incident: The insider was a computer engineer at a global financial services company. After having a discussion with his supervisor about his unsatisfactory work performance, the insider intentionally transmitted a code and command to core global control center routers within the company's internal network, and by transmitting that code, erased the running configuration files in the routers, resulting in a loss of connectivity to approximately 90% of all company networks across North America.

Action Taken: The company reported the employee to law enforcement.

Result: The insider pleaded guilty to intentional damage to a computer and was sentenced to almost 2 years in prison.

Take-away: Employees with poor performance reviews are at a higher risk of becoming insider threats. Human resources personnel, managers, and supervisors should receive training about the company's termination procedures, insider threat program and assist in monitoring potential insider threats. Implement disaster recovery plans and better router governance.

CASE #7

UNAUTHORIZED DATA SHARING

Summary: Insider used contacts at the Federal Reserve to obtain confidential regulatory and government information to help advise company clients.

Cause of the Incident: An employee at a financial services company illegally obtained confidential regulatory information from a friend at a Federal Reserve Bank. The insider employee used the confidential information to help clients of the financial services company.

Action Taken: The company's compliance team spotted the breach in a report prepared by the insider and alerted the Federal Reserve.

Result: The insider was barred from the banking industry by the Federal Reserve Board of Governors. The company settled with the New York State Department of Financial Services for $50 million for failing to supervise the insider.

Take-away: Companies should implement and enforce policies against unauthorized sharing of information. To the extent permitted by law, companies should monitor employee communications on firm systems for illegal or suspicious activity.

CASE #8

FALSE IDENTIFICATION DOCUMENTS

Summary: Two individuals used false identification documents and faked qualifications to obtain jobs at a financial services company, allowing them to steal client funds.

Cause of the Incident: Insiders used fake documents to obtain employment at a financial services company as operations personnel. The insiders diverted client money online and transferred it to private bank accounts that were opened using falsified documents. The company had outsourced its human resources functions to a foreign firm that did not conduct background checks before hiring the employees.

Action Taken: The financial firm conducted an internal investigation after receiving a complaint from a client. The firm reported the embezzlement to the police and attempted to recover the stolen money from the insiders.

Result: The insiders were arrested by police after a manhunt.

Take-away: To the extent permitted by law, companies should conduct background checks on all personnel who may have access to firm funds and confidential information on firm systems. Firms should also monitor suspicious transfers of funds.

APPENDIX B – METRICS IDEAS

	A	B	C	D	E
1	**Metric**	**Topic**	**Malicious/ Non-Malicious**	**Type**	**KPI/KRI**
2	# of users logging in outside their normal working hours	Analytics	Both	Operational	KRI
3	# of privileged users connecting servers they don't normally log in	Analytics	Both	Operational	KRI
4	# of unauthorized web uploads (may be already covered in DLP KRIs)	Analytics	Both	Operational	KRI
5	# of users logging in remotely from geo-locations they generally don't login from	Analytics	Both	Operational	KRI
6	# of users printed unusual number of documents (compared their normal usage)	Analytics	Both	Governance	KRI
7	Insider threats generated by source (fron INSA metrics whitepaper)	Analytics	Both	Operational	KRI
8	Average risk score per employee (from INSA metrics whitepaper)	Analytics	Both	Operational	KRI
9	# of emails / data elements prevented from leaving by DLP controls	Controls	Both	Operational	KRI
10	# of identified cases where deprovisioning did not occur and an incident occurred	Controls	Both	Governance	KRI
11	# of unauthorized changes in the environment	Controls	Malicious	Governance	KRI
12	% of change management driven changes that are reviewed	Controls	N/A	Governance	KPI
13	# of changes made to controls based upon lessons learned and post-mortem activities	Controls	N/A	Governance	KPI
14	#/% of individuals with policy exceptions (USB, cloud storage, web, etc.)	Controls	N/A	Governance	KRI
15	# of verified insider threat cases that were not identified internally but through law enforcement	Controls	Both	Governance	KRI
16	% job description reviews completed defining and confirming roles, responsibilities, skills, and certifications	Controls	N/A	Governance	KPI
17	% monitoring coverage of confidential data shared with external parties	Controls	N/A	Governance	KPI

	A	B	C	D	E
18	% of known vulnerabilities identified as primary root cause of insider-directed incidents	Controls	N/A	Governance	KPI
19	% of security defects identified in inspections and incident post-mortems confirmed by test as effectively mitigated	Controls	N/A	Governance	KPI
20	% the alerting rule results in an investigation closed with action	Controls	Both	Operational	KPI
21	% of alerting rules in align with framework and priorities-(effective and efficient)	Controls	N/A	Operational	KPI
22	% of alerting rules by program (exfiltration, excessive entitlements, data mining….)	Controls	N/A	Operational	KPI
23	% of data sources feeding alerting rules	Controls	N/A	Operational	KPI
24	# of employee assistance program interventions over time	EAP	Non-malicious	Governance	KRI
25	# of people making use of HR EAP	EAP	Non-malicious	Governance	KRI
26	Trends of EAP usage (depression, anxiety, family legal, etc.)	EAP	Non-malicious	Governance	KRI
27	# of entitlement review revocations over time	Entitlements	N/A	Operational	KPI
28	#/% of identities that are or are not certified for access	Entitlements	Both	Governance	KRI
29	# of active accounts shared between employees	Entitlements	Both	Governance	KRI
30	# of data (bytes) exfilled to external parties	Entitlements	Both	Operational	KRI
31	# of background checks conducted for new hires	Hiring	N/A	Board	KPI
32	# of people that do not get hired based upon background checks	Hiring	N/A	Board	KPI
33	% of workforce that leave the Firm over time	Incidents	Non-malicious	Board	KRI
34	# of true positive DLP incidents over time - intentional	Incidents	Malicious	Operational	KRI
35	# of true positive DLP incidents over time - unintentional	Incidents	Non-malicious	Operational	KRI
36	# of true positive non-DLP insider incidents over time - intentional	Incidents	Malicious	Operational	KRI
37	# of true positive non-DLP insider incidents over time - unintentional	Incidents	Non-malicious	Operational	KRI

	A	B	C	D	E
38	Type of tickets/escalations (email, web, conduct, print, usb, acceptable use, physical security, etc.)	Incidents	Both	Operational	KRI
39	% of aggregate loss by critical application or business process by quarter/annual	Incidents	Both	Operational	KRI
40	# of verified cases by critical application or business process by quarter/annual	Incidents	Both	Operational	KPI
41	% of repeat offenders (quarterly/semiannual/annual) - same policy	Incidents	Both	Governance	KRI
42	% of repeat offenders (quarterly/semiannual/annual) - different policies	Incidents	Both	Governance	KRI
43	% of negligent cases out of total # of verified investigations	Incidents	Non-malicious	Governance	KRI
44	% of unintentional cases out of total # of verified investigations	Incidents	Non-malicious	Governance	KRI
45	% of malicious cases out of total # of verified investigations	Incidents	Malicious	Governance	KRI
46	% of cases on employees v. contractors	Incidents	Both	Operational	KRI
47	# of cases on contractors for each contracting firm- In total and per 100 contractors	Incidents	Both	Operational	KRI
48	% of cases on employees by business line- In total and per 100 employees	Incidents	Both	Operational	KRI
49	# of cases of work-from-home v. in-office	Incidents	Both	Operational	KRI
50	Trends of action taken against employee/contractor	Incidents	Both	Governance	KRI
51	Trends of threat actor activity (account sharing, email home, internet upload, offline file transfer….)	Incidents	Both	Governance	KRI
52	Trends in motivation (convenience, fear, financial, grudge….)	Incidents	Both	Governance	KRI
53	Trends in tactics- (defensive evasion, credential sharing….)	Incidents	Malicious	Governance	KRI
54	% of cases from each population (interns, executive, leavers, watch listers….)	Incidents	Both	Governance	KRI

	A	B	C	D	E
55	% of alert incidents ticketed by an analyst for investigation	Incidents	Both	Operational	KPI
56	# security events triaged	Incidents	Both	Operational	KRI
57	# security events requiring engagements	Incidents	Both	Operational	KRI
58	# declared security incidents escalated	Incidents	Both	Governance	KRI
59	# security events/incidents escalated to HR	Incidents	Both	Governance	KRI
60	# security events/incidents escalated to Compliance	Incidents	Both	Governance	KRI
61	# security events/incidents escalated to Cyber Defense Center	Incidents	Both	Governance	KRI
62	# escalated events/incidents resolved as Substantiated	Incidents	Malicious	Governance	KRI
63	# escalated events/incidents resolved as Unsubstantiated	Incidents	Non-malicious	Governance	KRI
64	# escalated events/incidents resolved as Insufficient Information Available	Incidents	Both	Governance	KRI
65	# Unsubstantiated Substantiated events triaged	Incidents	Both	Operational	KRI
66	# Substantiated events/Malicious	Incidents	Malicious	Governance	KRI
67	# Substantiated events/Malicious (Fraud)	Incidents	Malicious	Governance	KRI
68	# Substantiated events/Malicious (Theft)	Incidents	Malicious	Governance	KRI
69	# Substantiated events/Malicious (IT Sabotage)	Incidents	Malicious	Governance	KRI
70	# Substantiated events/Malicious (OT Sabotage)	Incidents	Malicious	Governance	KRI
71	# Substantiated events/Malicious (Other Sabotage)	Incidents	Malicious	Governance	KRI
72	# Substantiated events/Malicious (Leaker)	Incidents	Malicious	Governance	KRI
73	# Substantiated events/Malicious (Violence)	Incidents	Malicious	Governance	KRI
74	# Substantiated events/Not Malicious (Accident)	Incidents	Non-malicious	Governance	KRI
75	# Substantiated events/Not Malicious (Negligence)	Incidents	Non-malicious	Governance	KRI
76	# Substantiated events/Not Malicious (Victim)	Incidents	Non-malicious	Governance	KRI
77	# Substantiated events/incidents by target	Incidents	Both	Governance	KRI
78	# Escalated events/incidents resulting in criminal referrals	Incidents	Malicious	Board	KRI
79	# Escalated events/incidents resulting in remediation and/or restitution action by type	Incidents	Both	Governance	KRI
80	$ value of recovered assets resulting from escalated cases	Incidents	Both	Governance	KPI
81	$ value of restitution resulting from escalated cases	Incidents	Both	Governance	KRI

	A	B	C	D	E
82	$ value of cost avoidance resulting from escalated cases	Incidents	Both	Governance	KPI
83	# escalated cases resulting in risk reduction	Incidents	Both	Governance	KRI
84	# escalated cases resulting in process improvements	Incidents	Both	Governance	KPI
85	% reduction in Mean Time To Detect	Incidents	Both	Operational	KRI
86	% reduction in Mean Time To Respond	Incidents	Both	Operational	KRI
87	% Reduction in Mean Time To Resolve	Incidents	Both	Operational	KRI
88	Volume of events systematically detected versus user reported	Incidents	Both	Operational	KRI
89	Tracking of common root causes and counts of cases associated with them to help prioritize remediation efforts	Incidents	Both	Governance	KPI
90	# of physical security incidents	Incidents	Both	Governance	KRI
91	# of privacy laws which apply (GDPR, California rules….)	Legal/Regulatory	N/A	Board	KPI
92	% of workforce that are simulated phishing repeat offenders over time	Simulated phishing	Both	Governance	KRI
93	% of privileged access users that are simulated phishing repeat offenders over time	Simulated phishing	Both	Governance	KRI
94	% of managers/supervisors who have completed insider threat training over time	Training	Non-malicious	Governance	KPI
95	# of int'l travelers/# of total int'l travelers who did not take Secure Traveler training	Training	N/A	Governance	KRI
96	% of test subjects who after 12 months of service retain principle elements of security responsibilities delivered in training	Training	N/A	Governance	KPI
97	# of HR disciplinary actions over time	Worker behavior	Both	Governance	KRI
98	#/% of individuals who have performance reviews	Worker behavior	Both	Operational	KRI
99	#/% of escalations/cases for departing individuals	Worker behavior	Both	Operational	KRI
100	#/% of events that required legal/HR intervention	Worker behavior	Both	Governance	KRI
101	Escalations by department/unit/manager or whatever makes sense	Worker behavior	Both	Operational	KRI
102	# of verified insider threat investigations by manager	Worker behavior	Both	Operational	KPI

WWW.SIFMA.ORG