sifma

# CYBERSECURITY

## INSIDER THREAT BEST PRACTICES GUIDE, 2ND EDITION
## FEBRUARY 2018

**PREPARED BY SIFMA WITH THE ASSISTANCE OF SIDLEY AUSTIN LLP**

## 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. Neither SIFMA or any of its members nor Sidley Austin LLP, 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 disclosed, or represents that its use would not infringe privately owned rights. 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 or Sidley Austin LLP. The views and opinions of the authors expressed herein do not necessarily state or reflect those of the financial services sector.

## 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, insider threat is just as much a human problem as it is a technology 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; (2) to act as a reference for regulators to better understand the insider threat at financial institutions; and (3) to help financial firms measure their insider threat program's effectiveness.

The Insider Threat Best Practices Guide was first published in 2014, but over the past four 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 and big data techniques, evolving privacy issues including restrictions on employee surveillance and the use of automated decision making and profiling in the European Union, and legal and practical barriers to performing employee background checks. SIFMA also conducted a survey of its members regarding their insider threat programs, and we have updated the Guide to reflect the current state of the industry.

The best 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 mitigation program mirror those denoted in the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. 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 business models and available resources.

However, unlike in a general cybersecurity program, every component in an insider threat mitigation program must have a distinctly human element. 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 mitigation team with counterintelligence skills can leverage technical tools, such as network 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 mitigation team is essential to coordinate firm-wide prevention efforts and alert relevant personnel to suspected or detected threats. Best practices for insider threat mitigation 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 mitigation 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. Laws abroad—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 starting point while consulting with local counsel to develop and implement an insider threat program that is effective and in compliance with applicable law.

## SUMMARY OF BEST PRACTICES

During the course of our research and industry benchmarking activities, the following best practices have been developed. The purpose of this non-exhaustive list is to provide a framework of how to develop and maintain an effective insider threat program. These guidelines reflect surveyed financial services firms and do not wholly represent all suggested best practices. We advise that you only implement the best practices that are appropriate for your firm and adhere to local, state and federal law.

- Engage the board of directors and executive management to provide oversight of the insider threat program.
- Organize a dedicated insider threat team to implement the insider threat program.
- Develop an insider risk mitigation strategy that takes into account the three key variables of (1) criticality, (2) vulnerability, and (3) source of potential threats. For further detail, please refer to page 9.
- 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 and corresponding training and awareness programs for all personnel.
- Establish and enforce effective information security policies, including a firm-wide written information security and incident response plan.
- 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.
- Encourage cross-organizational participation in the insider threat program, including Human Resources and Internal Audit, et al.
- 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 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 requirements related to implementing an insider threat program, and ensure that all insider program activities comply with applicable law.
- 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.
- Incorporate appropriate employee onboarding and termination procedures into the insider threat program.
- Develop appropriate due process and fairness procedures for disciplinary actions against employees to maintain morale and mitigate the effect of disciplinary actions in creating disgruntled insiders.

## III. INTRODUCTION

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. Moreover, the losses and damage can be substantial. In September 2014, the FBI noted that damages from insider incidents in its recent investigations ranged from $5,000 to $3 million, including losses from the value of stolen data, costs of information technology services and the implementation of countermeasures, legal fees, loss of revenue and/or customers, and credit monitoring services for employees and customers affected by the incident. More recent estimates show that the losses are increasing: according to the Ponemon 2016 Cost of Insider Threats Benchmark Study, the financial services sector ranked highest in terms of total annualized losses associated with insider threats at approximately $5.4 million per company. Moreover, although external threats are still the most significant source of data breaches, Verizon's 2017 Data Breach Investigations Report states that approximately 25% of breaches across all sectors are caused by insiders. Verizon emphasizes that it is important for organizations to focus less on job title and more on the level of access when attempting to assess potential insider threats. 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 the firm's 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. In a recent benchmarking survey conducted by SIFMA approximately 70% of responding firms reported that they established an insider threat program within the last three years.

The most serious insider threats in the digital 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 designated intelligence 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.

## WHO ARE THE INSIDERS?

An insider is 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 CERT Common Sense Guide to Mitigating Insider Threats (5th Ed.) 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 accidental insider 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 popular motivator, made all the more 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. 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) correlate 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 Ponemon study of 693 U.S. IT personnel found that over 73% of them think it is very likely or likely that privileged users believe they are empowered to access all of the information they can view, and 65% believe that privileged users access sensitive or confidential data for curiosity only. In order to detect warning signs such as privilege abuse, firms have begun to implement analytical tools that log behavioral modeling. According to the SIFMA Benchmarking Survey, approximately 70% of firms indicated that they use behavioral modeling or other analytical tools as a part of their insider threat program. Approximately 90% of responding firms using such tools use a combination of third party and in-house tools.

Numerous academic studies have attempted to identify the psychological traits prevalent in insider spies. 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 is 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 mitigation 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.

## RISK MANAGEMENT

Risk management is a critical process in every financial institution and can be leveraged in many contexts throughout an organization. In order to best comprehend risk management, it is worth identifying how it is defined and how it intersects with insider threats. Risk is commonly defined as the probability of loss or damage. As illustrated in the Department of Defense Risk Model in Figure 1, 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 of Figure 1).

Therefore, the strategy for mitigating insider threat must:

- Take into account each of the factors in the risk model segment and their interaction therein as illustrated in Figure 1.
- Consider the content of and relationships among the risk model segments illustrated in Figure 1.
- 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.


Figure 1 – Department of Defense Risk Model.

Part of risk management must also be a 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.

## UNDERSTANDING THE INVESTIGATIVE CHALLENGE OF INSIDER THREATS

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 for 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. 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 its 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 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 in order to avoid prompting or exacerbating additional harmful insider activity.

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 MITIGATION

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 below and represented in the associated graphic 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 how well the insider threat team can incorporate the policy and human components of the insider threat program into the technical model.

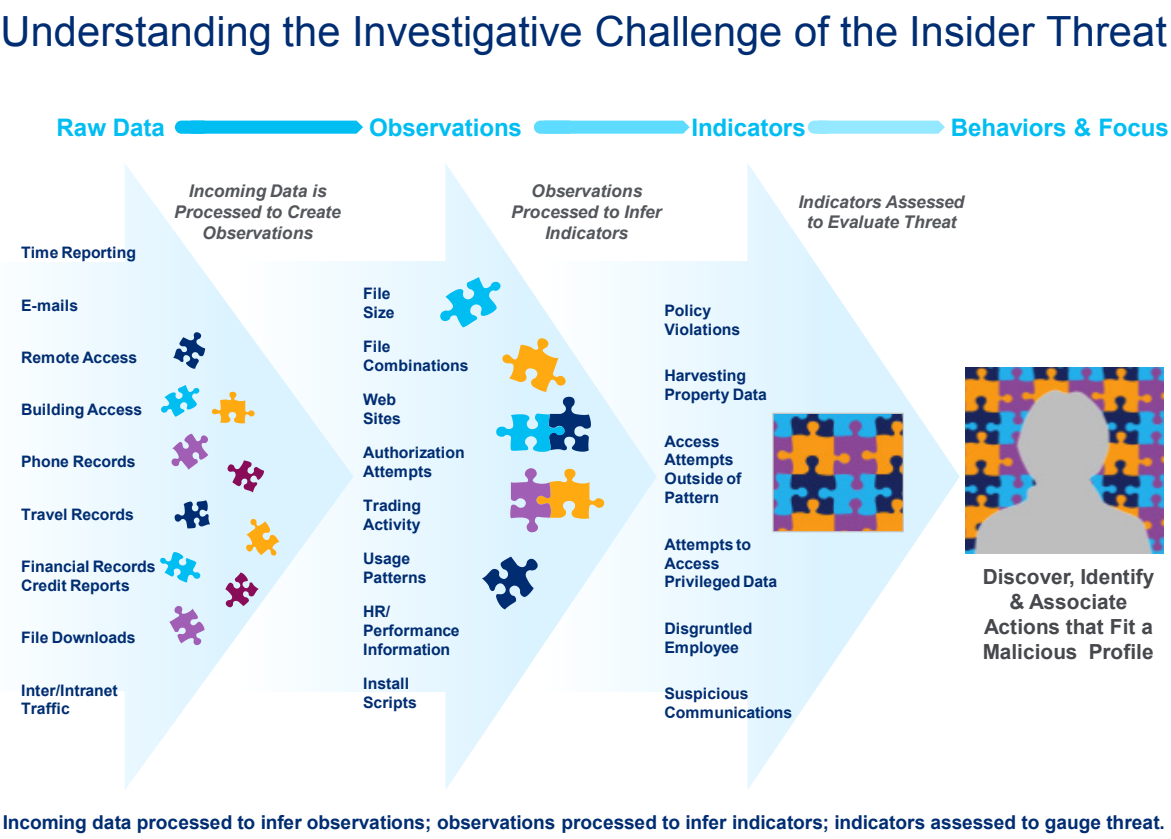


Figure 2 – Model-Based Predictive Classification Concept

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 in Figure 2.

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 introduce 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 some data (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 different 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 help 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 counsel and compliance groups 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.

As an example, The Federal Financial Institutions Examination Council's ("FFIEC") Cybersecurity Assessment Tool ("CAT"), sets forth explicit regulatory expectations with respect to insider threat programs at different levels of maturity. 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 to 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, and at the "advanced" level, a firm should have automated tools to proactively identify high-risk insider behavior or data mining by insider threats.

In its February 2015 report on Cybersecurity Practices, the Financial Industry Regulatory Authority ("FINRA") also issued guidance for firms on managing intentional and unintentional insider threat risks, noting that insiders often gain inappropriate access to firm systems or information as a consequence of being granted inappropriate access upon hiring, being allowed to accumulate privileges as they change positions, or being allowed to expand their access without a compelling business need. Additional problems can arise when credentials are stolen or misused, or when user-facing applications have excessive permissions or access to back-end systems and databases. As a consequence, both malicious and unintentional insider threats can result from the same weaknesses in access controls.

## STRUCTURING AN INSIDER THREAT MITIGATION PROGRAM

While it may be virtually impossible to completely eliminate insider attacks, an insider threat mitigation 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, 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 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. That being said, it is 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 mitigation 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. 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 mitigation 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 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.

## IMPLEMENTING AN INSIDER THREAT MITIGATION 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 mitigation program. 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 mitigation program. The key tasks for each component are described in more detail in section IV.

Firms should also identify key metrics that can be used to assess their insider threat program. These metrics can be developed and assessed under the NIST Framework. For example, according to the SIFMA Benchmarking Survey, over half of responding firms reported that they align their insider threat programs with either the NIST Framework or Carnegie Mellon University's CERT Best Practices. Within the framework 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. The key metrics may include the following:

## KEY MANAGEMENT METRICS

- Annual budget for insider threat program.
- Return on investment ("ROI") for insider threat program expenditures.
- Frequency of reports to board or directors and/or executive management and qualitative assessment of the detail and value of such reports.
- Number of insider threat incidents reported or investigated.
- Number of complaints or reports regarding suspicious financial transactions on firm or client accounts.
- Specific action items and identified risk areas from internal audit reports, regulatory examinations or risk assessments provided by external or independent third parties, including maturity scores and un-remediated follow-up items from prior assessments.
- Financial losses or costs associated with insider threat incidents at the firm.
  Number of regulatory notifications submitted.

## KEY OPERATIONAL METRICS

| DATA SOURCE | KEY METRIC |
|---|---|
| **Emails/E-communications** | Monthly statistics on the volume of anomalous email traffic. |
| **File downloads** | Daily reports on file downloads to detect high-volume or anomalous exfiltration of confidential data. |
| **Internet/Intranet traffic** | Weekly reports on suspicious internet use or traffic from firm networks. |
| **Anomalous activity logs** | Weekly metrics from logs of anomalous activity in proprietary business applications or platforms. |
| **Data loss prevention logs** | Daily review of logs from the firm's data loss prevention tool. |
| **Disciplinary action reports** | Reports of disciplinary actions and/or policy violations. |
| **Remote access records** | Weekly assessment of anomalous patterns in remote access to firm networks. |
| **Employee performance evaluations** | Individual employee performance reports stating abnormally subpar performance or behavioral problems. |
| **Background check data** | Red flags in pre-employment screening data. |
| **External storage device exceptions** | Current number of exceptions granted to employees for use of external storage devices. |
| **Time sheets, phone records, and travel records** | Monthly review of employee travel records and time sheets for discrepancies or unusual reimbursement requests. |
| **Building access records** | Unusual patterns of building access by employees or contractors. |
| **Printing/Scanning activity** | Anomalous spikes in volume of printing and scanning by individual employees or contractors. |

Although many of the metrics recommended above will be useful for most financial firms, some key metrics may vary among firms. According to the SIFMA Benchmarking Survey, nearly 70% of firms rated their cross-functional division and assignment of responsibilities, or "RACI participation level" as being "responsible" for developing a formalized insider threat program and for establishing a baseline of normal behavior for both networks and employees. Similarly, about 60% of firms rated their RACI level as being "responsible" for deploying solutions for monitoring employee actions and correlating information from multiple data sources. Email surveillance was also generally identified as one of the most useful sources of data. Nevertheless, some of the best practices with respect to key metrics are dependent on the specific activities, purposes, and organizational structure, size, and location of the firm. In some circumstances, the type of risks can inform the metrics used to assess the strength of a firm's program. Firms responding to the SIFMA Benchmarking Survey reported that their insider threat programs

covered a variety of risks, including espionage, employee conduct, employee fraud, data theft, physical theft, workplace safety, privilege misuse, sabotage, reputational damage, and dangerous combinations of access.

Insider threat risks often converge around the point of employee onboarding or 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 former 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 third-party service providers into their insider threat programs. Third parties can be a source of significant cybersecurity vulnerabilities and additional insider threats. Consequently, supply chain risks and third-party service provider supervision have received increasing attention from federal financial 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.[1] 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.[2] The OCC requires banks to conduct independent reviews of vendors so that the bank's management can effectively manage cybersecurity risks,[3] and the Federal Reserve Board recommends the establishment of a risk management program that addresses ongoing monitoring of service providers.[4] 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 mitigation 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 V details some of these legal requirements and risks.

Section VI 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 mitigation 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.

1 See FINRA Report on Cybersecurity Practices, February 2015.

2 See SEC OCIE 2015 Cybersecurity Examination Initiative.

3 See OCC Bulletin 2013-29.

4 See Federal Reserve Board "Guidance on Managing Outsourcing Risk."

Section VII is a bibliography containing the sources cited in this guide, as well as other helpful resources. Please note that citations in this guide contain some short titles, whose full citations can be found in the bibliography.

We suggest firms follow an approach similar to what is described in the NIST Cybersecurity Framework when putting the core elements of this document into practice.[5] 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 putting the core elements of this document into practice, modified slightly to call out key items specific to insider risk.

[5] See NIST Cybersecurity Framework, Sec. 3.2.

## SEVEN CORE STEPS TOWARDS IMPLEMENTING AN INSIDER THREAT MITIGATION PROGRAM

SIFMA suggests firms follow an approach similar to what is described in 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 mitigation program. Outside experts can provide more tailored, detailed assistance and feedback. In addition to private consultants, there are a number of non-profit and government resources that can provide assistance. The CERT Insider Threat Division of the Software Engineering Institute at Carnegie Mellon University, a federally funded research and development center, hosts workshops on evolving insider threats, works with organizations on program development, and provides training and certification courses to insider threat program managers and assessors. More information can be found at http://www.cert.org/insider-threat/products-services/index.cfm. 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.

[6] See NIST Cybersecurity Framework, Sec. 3.2.

## IV. CORE COMPONENTS

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 defines 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 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<br>Common Sense Guide, 5th Ed., Best Practice #1<br>NIST Cybersecurity Framework (ID.AM-1, 2, 4)<br>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:<br>• Systems (software, hardware, devices)<br>• Data & Intellectual Property<br>• Personnel<br>• Third party Providers<br>• Partnerships | NIST Cybersecurity Framework (ID.AM-5)<br>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<br>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.<br>**Structure**: Determine the location of the insider threat team within the organization<br>**Staff**: Hire new personnel with counterintelligence experience to staff the insider threat team, or train existing employees in relevant skills<br>**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.<br>**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<br>Common Sense Guide, 5th Ed., Best Practices #2 and #3<br>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<br>International Implementation of Best Practices<br>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.<br>**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<br>DoD Insider Threat Mitigation, Appendix A, Rec. 3.1<br>AFCEA Insider Threat: Protecting U.S. Business Secrets, pp. 6-8<br>FFIEC CAT, Domain 1, Training and Culture<br>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.<br>**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.<br>**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.<br>**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<br>DoD Insider Threat Mitigation, Section 2.6, Risk Management, pages 7-8<br>Common Sense Guide, 5th Ed., Best Practice #6<br>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.<br>**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<br>Spotlight On Insider Threat: Trusted Business Partners, pp. 12-14<br>National Risk Estimate<br>Common Sense Guide, 5th Ed., Best Practice #16<br>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.<br>Establish a list of indicators that could tip investigators to suspicious behaviors.<br>**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<br>Symantec White Paper<br>Behavioral Risk Indicators<br>Common Sense Guide, 4th Ed., Best Practice #16<br>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.<br>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.<br>**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.<br>**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<br>FBI: Detecting and Deterring an Insider Spy<br>Understanding the Insider Threat, pp. 90-91<br>DoD Insider Threat Mitigation, Appendix A, Rec. 6.8<br>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.<br>**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<br>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.<br>Manage remote access from both internal and external parties.<br>Implement controls to prevent unauthorized escalation of user privileges and lateral movement among network resources.<br>Require contractors who use information systems by contract to meet minimum standards for technical safeguards, and ensure compliance with such standards by routine audits.<br>**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 roles.<br>**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<br>NIST Cybersecurity Framework (PR.AC-3; PR.MA-2)<br>SEC Cybersecurity Risk Alert, p. 3<br>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.<br>Establish personnel security vetting procedures commensurate with an individual's level of information system access.<br>**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<br>NIST Cybersecurity Framework (PR.AC 1-5)<br>DoD Insider Threat Mitigation, Appendix A, Recs. 5.3, 2.3<br>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:<br>• Termination of physical and electronic access rights<br>• Changing passwords to all systems and data that the employee had access to, including shared accounts, files and folders<br>• Collect all equipment given to employee<br>• Deleting remote access tools from employees' personal devices (e.g., RSA tokens) | Common Sense Guide, 4th Ed., Best Practice #14<br>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.<br>**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<br>Information Risk in Financial Institutions<br>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**:<br>Ensure that employees, contractors, and other personnel receive regular training and updates on topics relevant to mitigating insider threats, including:<br>• Protocols for handling sensitive information, including IP and customer information<br>• Responsibilities and processes for alerting management of suspicious activities<br>• Handling of critical assets and physical and electronic access controls.<br>Establish mandatory minimum standards for security education, awareness and training programs related to the insider threat.<br>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<br>NERC CIP-004<br>DoD Insider Threat Mitigation, Appendix A, Rec. 3.3<br>SEC Cybersecurity Risk Alert, p. 3<br>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.<br>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<br>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:<br>• Reporting suspected insider activity to insider threat team<br>• 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<br>• Indicators of insider threat behavior<br>• How to safely use social media | Minimum Standards for Executive Branch Insider Threat Programs, Section I.1.a-c<br>How to Protect Insiders from Social Engineering Threats<br>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<br>**Backup data**: Ensure data backups are available and recovery processes account for the actions of malicious insiders.<br>**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<br>Common Sense Guide, 4th Ed., Best Practice #17<br>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.<br>**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<br>Common Sense Guide, 4th Ed., Best Practice #19<br>NIST Cybersecurity Framework (PR.DS-5)<br>Common Sense Guide, 5th Ed., Best Practice #19<br>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"rin 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.<br>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<br>SEC Cybersecurity Risk Alert, p. 5<br>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.<br>**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<br>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:<br>• Full-packet sensors to investigate actions or inform response activities<br>• Web content sensors to track risky internet use<br>• Updated virus/malware scanners<br>• Log correlation engines or system information event management (SIEM systems to log, monitor, and audit employee actions)<br>• 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<br>NIST Cybersecurity Framework (DE.CM-1-7)<br>Human Behavior, Insider Threat and Awareness<br>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.<br>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:<br>• Conducting personnel investigations<br>• Restricting details of inquiries to relevant staff<br>• Determining when it is appropriate to involve outside experts and law enforcement in investigations<br>• Conducting a forensics analysis of an incident | Minimum Standards for Executive Branch Insider Threat Program (Point F)<br>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<br>NIST Cybersecurity Framework (DE.CM-3)<br>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<br>Common Sense Guide, 4th Ed., Best Practice #5<br>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<br>Capitalize on information sharing programs run by DOD, DHS and FBI<br>Consider participation in information depositories when/if they are developed by Congress<br>Build relationships with local and state law enforcement and monitor local data sources as consolidated reporting is limited currently<br>**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 so as to help reduce impact on workplace privacy. | DOJ/FTC Antitrust Policy Statement<br>Suitability and Security Clearance Report<br>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.<br>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.<br>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:<br>• Reviewing affected systems and re-creating the incident<br>• Interviewing suspects and witnesses<br>• Documenting evidence and findings in a centralized system<br>• Delegating investigative responsibilities among relevant personnel<br>• Sharing information related to the investigation only on a need-to-know basis | NIST Cybersecurity Framework, RS.CO-1 - RS.CO-2<br>Electronic Crime Scene Investigation<br>Prosecuting Computer Crimes |
| | **Decision Tree**: Create a decision tree that outlines how to respond to investigation findings. The tree should address:<br>• Intervening vs. continuing to monitor concerning behavior<br>• When to involve non-insider threat team personnel in the investigation<br>• When to escalate incidents up the management chain within the organization<br>• Circumstances warranting consultation with third-party experts and/or legal counsel<br>• Situations warranting notification to law enforcement | NIST Cybersecurity Framework RS.CO-3 to RS.CO-5<br>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.<br>• Implement tools for a rapid and effective audit of a host computer system to detect any anomalies in its programs and files.<br>• 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<br>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.<br>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.<br>**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 of 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<br>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.<br>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.<br>**Implement secure backup and recovery processes**: Store backup media off-site. Ensure that 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<br>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.<br>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 |

## V. LEGAL RISKS

Although insider threat mitigation programs can protect firms from potentially crippling theft and system damage, they may also expose firms to some legal risk. In the United States, firms' monitoring practices are subject to the Electronic Communications Privacy Act (ECPA) at the federal level, as well as various state privacy and tort laws. While these laws generally contain exceptions that may permit workplace monitoring, such exceptions are often predicated on providing sufficient notice of monitoring practices. The Fair Credit Reporting Act (FCRA) also restricts the allowable scope of background checks on prospective employees. Other countries, particularly those in the European Union, more stringently regulate workplace monitoring and background checks. This section details the primary laws that may be applicable to an insider threat program in the United States, and also provides an overview of some of the relevant laws in the UK, Germany, Hong Kong, and India. There may be other applicable laws and/or applicable regulations depending on the relevant facts and circumstances.

This section is not intended to provide and should not be construed as providing legal advice. Prior to instituting any insider threat mitigation program, companies should engage in a thorough legal analysis and with their own legal counsel.

### A. ELECTRONIC COMMUNICATIONS MONITORING

#### 1. FEDERAL LAW

The primary federal law governing electronic communications privacy in the U.S. is the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 et seq. Title I of the 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 Title I apply to real-time monitoring programs, such as web traffic monitors and keystroke loggers. See, e.g., United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003).

Real-time monitoring can be potentially lawful under two exceptions to Title I of ECPA. Under § 2511(2)(a)(i), known as the "service 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." While few courts have closely interpreted this exception, it is generally understood that it permits 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.

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. § 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 provided for monitoring). Firms can therefore help protect themselves against potential liability under Title I of ECPA 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. Firms that provide their own email services to employees, however, 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)). 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 Title I, 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).

Employers should be aware of additional restrictions on employee surveillance imposed by the National Labor Relations Act. Section 7 of the National Labor Relations Act 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 Advice Memorandum (July 28, 2011), regarding Buel, Inc., Case 11-CA-22936. 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 addition 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, including 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 record 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). 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 to 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.

In light of 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.

### 2. 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 work place, 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.

Only a few 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 and Delaware, by contrast, require private employers to inform employees of any monitoring. Conn. Gen. Stat. Ann. § 31-48d; Del. Code Ann. tit. 19, § 7-705. While providing employees notice of monitoring is always a best practice, as noted above, firms that operate in Connecticut and Delaware should be especially careful to fully disclose their monitoring policies. State law requirements may, in some circumstances, require some form of systems monitoring for cybersecurity purposes. The New York Department of Financial Services recently finalized a cybersecurity regulation that 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). 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.

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—including 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. A court in Washington, for instance, noted 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." State v. Townsend, 20 P.3d 1027, 1031 (2001). A Massachusetts court also dismissed a 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." Restuccia v. Burk Tech., No. 95-2125, 1996 Mass. Super. LEXIS 367 (Mass. Super. Ct. Nov. 4, 1996). 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, which generally impose 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 have "an objectively reasonable expectation" of privacy in the place of intrusion. Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 490 (1998). Courts have also almost uniformly 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) ("The Court finds no support for the conclusion that [the plaintiff] had a reasonable expectation of privacy in an open office."); People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd., 895 P.2d 1269, 1282 (Nev. 1995) (stating in dicta that "there is, generally speaking, a reduced objective expectation of privacy in the workplace"). 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.[7] 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, which prohibits employers from inquiring about a prospective employee's salary history during all stages of the interview process. If the employer already knows the applicants 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, Oregon, and the city of Philadelphia.

## B. 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. 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.

### 1. THE FAIR CREDIT REPORTING ACT (FCRA)

A candidate's financial history may be indicative of not just his or her character, but also his or her 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. In the United States, the procurement of such 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[8]—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. 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

[7] N.Y. Lab. Law § 201-d.

[8] See, e.g., Investigative Consumer Reporting Act (ICRAA- CA Civil Code §1786. In some instances, the California law is broader than FCRA. Firms operating in California should consult local counsel to develop a background check policy.

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. § 1681a(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. § 1681a(y)(2).

### 2. RESTRICTIONS ON EMPLOYER CREDIT CHECKS

An increasing number of cities and states are passing laws specifically restricting the ability of employers to conduct credit checks on job applicants and current employees. For example, New York City passed the Stop Credit Discrimination in Employment Act in 2015, which 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—and the list of states considering such laws is growing. 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

### 3. EEOC GUIDANCE ON THE CONSIDERATION OF CRIMINAL HISTORY

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. 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 [hereinafter "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.

Recently, the EEOC brought enforcement actions against employers for failing to provide robust, individualized assessments for those excluded by criminal history screening policies. In 2015, BMW paid $1.6 million to settle a lawsuit in which the EEOC alleged that BMW's logistics contractor excluded African-American workers at a disproportionate rate when it applied BMW's criminal conviction records guidelines to incumbent employees. See EEOC, "BMW to Pay $1.6 Million and Offer Jobs to Settle Federal Race Discrimination Lawsuit" (Sept. 8, 2015), available at https://www.eeoc.gov/eeoc/newsroom/release/9-8-15.cfm. 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.

#### 4. 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 user name 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. 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). Accordingly, firms should instruct human resources and other personnel responsible for hiring to use only publicly visible online information to screen job candidates and check up on current employees, and ensure that information obtained about an employee's outside activities is not used to discriminate against employees or applicants in a way that violates state law. Furthermore, firms should consult with legal counsel to determine the applicability of FCRA disclosure and consumer authorization requirements to any firm efforts to assemble an employment report, even when such reports are based on public record data obtained from social media accounts.

The majority of 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 SRO 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.

### C. FOREIGN PRIVACY AND EMPLOYMENT LAW CONSTRAINTS

Foreign countries' privacy and employment regulations and protections often differ significantly from those of the United States. 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, the United Kingdom (UK), India, and Hong Kong. We also include a brief overview of the European Union's General Data Protection Regulation. The information regarding laws in Germany and India are drawn from Lori Flynn et. al, International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany, Software Engineering Institute, April 2014, available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2014_005_001_88427.pdf.

#### 1. NOTABLE CYBERCRIME, PRIVACY, AND EMPLOYMENT LAWS

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

| Category of Law | India | Germany | UK | Hong Kong |
|---|---|---|---|---|
| **Cybercrime** | IT Act of 2001<br>Indian Penal Code, 1860 | Implementation of the Budapest Convention on Cybercrime (note: this is international not just Germany) | Regulation of Investigatory Powers Act 2000 | Computer Crimes Ordinance (No. 23 of 1993) |
| **Privacy** | IT Rules (2011) | German Data Protection Amendment Act; Federal Personal Data Protection Act of 2001; Act on Employee Data Protection; Federal Data Protection Act<br><br>EU General Data Protection Regulation (applicable to all firms operating in the EU or offering goods or services to EU customers) | UK Data Protection Act 1998; Regulation of Investigatory Powers Act 2000<br><br>EU General Data Protection Regulation (applicable to all firms operating in the EU or offering goods or services to EU customers) | Personal Data (Privacy) Ordinance (Cap. 486); Code of Practice on Human Resource Management; Privacy Guidelines: Monitoring and Personal Data Privacy at Work |
| **Human Resources** | The Indian Contract Act; the Indian Penal Code; Persons with Disabilities Act; Industrial Law; Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal Act), Equal Remuneration Act, 1976 | Federal Gender Equal Treatment Act | Human Rights Act 1998; UK Equality Act 2010 | Employment Ordinance (Cap. 57) |

### 2. OVERVIEW OF RELEVANT PROVISIONS

**EU GDPR:** The European Union General Data Protection Regulation ("GDPR") applies to organizations operating within the EU and organizations outside the EU that offer goods or services to individuals in the EU, effective May 25, 2018. The GDPR imposes responsibilities on "controllers" and "processors" of information, but data controllers bear the ultimate responsibility for ensuring that their contracts with processors comply with the GDPR. The GDPR covers a broad definition of "personal data" that includes identifiers such as IP addresses and even pseudonymized data, if the data is still attributable to the individual. Furthermore, the GDPR's fundamental data protection principles apply irrespective of technology. Accordingly, financial firms that operate in the EU or offer goods and services to EU customers must take the provisions of the GDPR into consideration when developing and designing an insider threat program and strike a balance between their legitimate interests as employers and the reasonable privacy expectations of their employees.

Under the GDPR, an individual's consent to process his or her data must be freely given, specific, informed, and unambiguous. However, consent is unlikely to provide a legal basis for data processing at work unless employees can refuse without adverse consequences. Performance of contract or legitimate interest of the employer may apply; but under such circumstances, the employees must be provided effective information about monitoring,

and the monitoring must comply with principles of proportionality, data minimization and subsidiarity.[9] In general, data subjects have the right to object to processing unless the controller demonstrates compelling legitimate grounds for processing. Non-consent-based processing is allowed for national security, general public interests, protection of individual rights and freedoms, or prevention/investigation/detection/prosecution of criminal offenses, within specific guardrails established by the GDPR. However, data subjects have a right of erasure without undue delay where data is no longer necessary for purposes collected, or where the data subject withdraws consent or objects to processing.

The GDPR also imposes restrictions on cross-border transfers of information. If a firm relies on consent to transfer data outside the EU, the firm should closely examine whether data subjects have been sufficiently informed of the risks of transfer. Both controllers and processors must designate a data protection officer, and controllers are obligated to notify supervisory authorities of a data breach no later than 72 hours after becoming aware of the breach. Violations of controller and processor obligations under the GDPR are subject to fines of up to 10 million euros or 2% of annual turnover (whichever is higher), and violations regarding processing, data subject rights, or transfers of personal data are subject to fines of up to 20 million euros or 4% of annual turnover (whichever is higher).

Although the GDPR does not directly prohibit or require the establishment of an insider threat program, the restrictions on data processing, data transfers, and individual consent may affect the implementation of a financial firm's insider threat program. Accordingly, as firms undertake efforts to comply with the GDPR through privacy by design, the insider threat team should work with legal counsel to ensure that the firm's insider threat program does not violate any of the restrictions or requirements of the GDPR.

**Germany:** On July 6, 2017, Germany implemented the EU GDPR by passing the German Data Protection Amendment Act (GDPAA), which will replace the Federal Personal Data Protection Act of 2001 as the primary privacy law in Germany when it becomes effective on May 25, 2018. Under Section 26(1) of the GDPAA, data collection and processing for the establishment, performance, or termination of employment is permitted as "necessary for purposes of the employment relationship." Employers should strike a practical balance between their interests and the employee's privacy rights in determining what data processing is "necessary." However, companies are required to implement suitable measures to ensure that all processing of employee data is done in compliance with the principles of Article 5 of the GDPR, including (a) purpose limitation, (b) transparency, (c) lawfulness of processing, (d) data minimization, (e) accuracy, (f) storage limitation, (g) confidentiality, and (h) integrity and security. These principles should form a mandatory part of any company policy regarding the processing of employee data. It is permissible to process employee data pursuant to consent by the employee, but it should be noted that German Data Protection Authorities view employee consents with skepticism, and the GDPAA provides guidance on when consents may be deemed "voluntary." Unlike the legal framework in the United States, where employees have a limited expectation of privacy in their use of company IT assets and systems, the GDPAA (and the current Federal Personal Data Protection Act) require that any collection and use of employees' personal data during investigations be supported by documented suspicion, that the collection is necessary, and that the employee does not have an overriding interest in prohibiting collection. Further, the Federal Commissioner for Data Protection and Freedom of Information has also stated that constant monitoring of employees' e mail or browsing patterns is impermissible because it constitutes "permanent surveillance" of the employee, which she described as a "severe intrusion." In July 2017, the German Federal Labor Court also ruled that data obtained through key-logger surveillance software that monitored employee computer use violated the Federal Personal Data Protection Act.

[9] See Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, available at ec.europa.eu/newsroom/document.cfm?doc_id=45631.

Germany's Gender Equal Treatment Act, which prohibits employment discrimination based on ethnic origin, gender, disability, religion, belief, age, and sexual orientation, may limit the scope of background checks. Although not yet required under the law, the Federal Anti-Discrimination Agency (FADA) has piloted an anonymous employment application process that initially excludes an employer from viewing an applicant's name, age, gender, and family status.

**United Kingdom:** The Data Protection Act 1998 (the "Act") governs data protection in the UK and has implemented the EU Data Protection Directive 95/46/EC. The Act is enforced by the Information Commissioner's Office ("ICO") and imposes a number of obligations on data controllers (i.e., the person who determines the purposes and means of the processing of personal data; in this case, an employer), who must comply with the eight data protection principles set out in the Act. The UK Parliament is considering a new Data Protection Bill to comply with the European Union General Data Protection Regulation (GDPR), and employers should monitor the development of the new legal framework in order to prepare for future compliance.

The ICO has published detailed guidance for employers in the form of the Employment Practices Code and its supplementary guidance (the "Code"). The Code does not impose any legal obligations, but instead sets forth best practices for compliance with the Act. Under Article 13 of the Act, any individual who suffers actual damages because of a violation of the Act is entitled to compensation from the data controller for that damage.

The ICO makes it clear in the Code that the Act does not prevent workplace monitoring. However, the Code notes that it will usually be intrusive to monitor employees, and recognizes that workers are also entitled to a degree of privacy in their work environment. The ICO recommends that employers conduct a privacy impact assessment prior to monitoring employees. The assessment should involve: (i) the clear identification of the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver; (ii) the identification of any likely adverse impact of the monitoring arrangement; (iii) considering alternatives to monitoring or different ways in which it might be carried out; (iv) taking into account the obligations that arise from monitoring; and (v) judging whether monitoring is justified. The ICO also recommends that employers clearly communicate to employees the circumstances in which they may be monitored, as well as any restrictions on private use of company computers. The Code recommends that employers avoid monitoring personal emails, and only open them where the reason (e.g. suspected criminal activity) is sufficient to justify the degree of intrusion involved.

The Code also recommends that a prospective employer should only vet job applicants where there are, significant risks to the employer or customers that must be mitigated and there is no less intrusive alternative. Vetting should be narrowly tailored to address the risk, should be based on reliable sources, and should occur as late in the employment stage as possible. It should be noted that financial services firms are eligible to request an applicant's conviction record from the Disclosure and Barring Service ("DBS") for candidates seeking "approved person status" under the Financial Services and Markets Act 2000 (i.e., those in customer functions such as traders, directors, money laundering reporters, or system and control specialists).

The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a framework for lawful interception of communications, access to communication data, and surveillance. Under Chapter 1 Section 1 of RIPA, it is illegal for a person to intentionally and without lawful authority intercept any communication within the UK in the course of its transmission by means of a public or private telecommunication system. The exceptions to RIPA mirror the exceptions to the American Wiretap Act, discussed above, except that both the sender and recipient of a communication must consent to an interception for it to be permissible under the consent exception. The Code, along with promulgated regulations, also take a restrictive view of the "provider exception," allowing an employer email provider to monitor communications only to supervise transactions or other business matters, detect or prevent crime, or ensure regulatory or self-regulatory compliance.

In relation to monitoring employees to protect against inside threats, employers should be mindful of general UK employment law and the UK Equality Act 2010 (the "Equality Act"). With respect to pre employment background checks, 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.

The extent and nature of information sought must be 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. The applicant should also be informed that vetting is to be carried out early in the application process. Comprehensive vetting should only be conducted on successful applicants.

The Equality Act will also apply with respect to the recruitment process. The employer should ensure that it does not breach any discrimination laws in its recruitment process, including, but not limited to, conducting background checks.

In order for a dismissal of an employee to be fair in the UK, the employer must have had a potentially fair reason for dismissing the employee and it must have acted reasonably in the circumstances. An employer cannot dismiss someone simply on the basis of "concerning behaviors" that it has not investigated properly. Where an employee is dismissed unfairly, their principle employment claim would be for unfair dismissal. A dismissed employee may also have a claim for wrongful dismissal in breach of any notice provisions in their contract of employment. If an employer wishes to dismiss an employee because he or she is perceived as an insider threat risk, the employer should ensure that satisfies the following requirements:

## VALID REASON

Potentially fair reasons for dismissal are (i) capability or qualifications; (ii) conduct; (iii) redundancy; (iv) breach of a statutory duty or restriction; and (v) "some other substantial reason." It is likely that behavior discovered by online monitoring will fall within the conduct reason (for example, where the conduct is identified as prohibited in a disciplinary policy) or "some other substantial reason."

In considering whether the dismissal is reasonable in the circumstances, it is necessary to look at whether the dismissal is substantively fair and whether it is procedurally fair. In order for the dismissal to be substantively fair, 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.

## PROCEDURE

To mitigate against a claim for unfair dismissal, an employer must also follow a fair procedure when investigating allegations of misconduct and considering dismissing employees. Before dismissing an employee, an employer should:

(a) Investigate the issues/ allegations. This may include speaking to witnesses and producing a report;
(b) Inform the employee of the issues in writing;
(c) Ensure the employee is made aware of their right to be accompanied;
(d) Conduct a disciplinary hearing or meeting with the employee;
(e) Inform the employee of the decision in writing; and
(f) Give the employee a chance to appeal.

The Advisory, Conciliation and Arbitration Service ("ACAS") has issued a Code of Practice on Disciplinary and Grievance Procedures which applies to misconduct dismissals. Employers should consider this code when taking a decision to dismiss an employee.

## PENALTIES

It may be that another less severe disciplinary measure is appropriate (for example a first written warning or a final written warning) but this will always depend on the specific conduct of the employee and the circumstances of the case. The outcome of any investigation should not be pre-determined.

## NOTICE

An employer should ensure it considers the terms of an employee's contract of employment in relation to notice. Where the employee's conduct is sufficiently serious as to amount to gross misconduct, the employer should be able to terminate the employee's employment summarily without notice. Where the conduct does not warrant summary dismissal, an employer must give the employee notice of the termination of their employment as identified in their contract of employment (or where permitted by the contract of employment, make a payment in lieu of notice).

**India:** India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules legislation ("IT Rules") regulates the collection, processing, and use of personal information by organizations. Adopting a definition similar to that used in the EU's Directive 95/46/EC, 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." These rules provide additional regulations for sensitive personal information, such as passwords, and financial and medical information.

In late November 2017, a committee of experts constituted by the Government of India and led by Supreme Court Justice Shri B. N. Srikrishna issued a white paper soliciting public comments on a detailed proposal for a new data protection framework for India. The white paper was prompted by a decision of the Supreme Court of India declaring privacy to be a fundamental right and calling for the development of a data protection regime. The issuance of the white paper signals the intent to introduce significant changes to India's data protection regime through legislation, and firms that conduct business in India or work with business partners in India should seek legal advice on how new data protection requirements, once issued, may affect the design and implementation of their insider threat program.

Indian employment law is another area relevant to insider threats. India does not have a law directly governing employee screening. But under the IT Rules, an individual's 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 the individual's informed 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."

Although background checks are generally permitted under Indian law, the lack of centralized and updated information can make conducting them difficult. To alleviate some concerns about 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.

**Hong Kong:** The key privacy law in Hong Kong applicable to monitoring employees is The Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"). In particular, the PDPO sets out the 6 Data Protection Principles ("DPPs") which are the basic requirements which data users must comply in the handling of personal data, including employees' personal data collected during monitoring activities. Although a contravention of the DPPs does not constitute an offence, the Privacy Commissioner may serve an enforcement notice on data users for contravention of the DPPs and a data user who contravenes an enforcement notice commits an offence.

The Privacy Commissioner has issued a "Code of Practice on Human Resource Management" ("Code") which 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. 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 Privacy Commissioner.

The Privacy Commissioner has also issued the "Privacy Guidelines: Monitoring and Personal Data Privacy at Work" ("Privacy Guidelines on Monitoring") (Attachment 2). Although the Privacy Guidelines on Monitoring is only best practice and data users are not obliged to follow the guidelines, in deciding whether data users are in breach of the DPPs, the Privacy Commissioner would take into account whether the data users have complied with the guidelines published by the Privacy Commissioner, in addition to other factors.

Employers must ensure that they do not contravene the DPPs of the PDPO 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 (DPP1 (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 (DPP1 (1)(c) & (2) (b)); (iii) a written privacy policy on employee monitoring has been implemented and practicable steps have been taken to communicate that policy to employees (DPP1(3) & DPP5). It should be noted that in any investigation by the Commissioner, employers may be called upon to explain and prove, among other things, that they have complied with the above requirements.

The Privacy Guidelines on Monitoring recommend employers to undertake a systematic assessment before determining whether employee monitoring is the best option given the risks and activities that the employer seeks to manage. In the event that the employer does decide to monitor, the Privacy Guidelines on Monitoring 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). Further details on the information to be included in the Employee Monitoring Policy can be found in Section 3.2 of the Privacy Guidelines on Monitoring.

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 Privacy Commissioner 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 DPP1(2). The Privacy Commissioner 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 DPP5 and ABB 14 of 2006. Further, numerous complaints are made every year to the Enforcement & Complaints Section of the Privacy Commissioner for Personal Data (PCPD), some of which result in corrective action by the PCPD.

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 (DPP1(c); (2)). Moreover, paragraph 2.7.2 of the Code (non-mandatory provisions) provides that "As 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."

As a general rule, 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 with regard

to a fair process prior to dismissal and it is not mandatory for employers to implement grievance and disciplinary procedures although this is recommended in the "Guide to Good People Management Practices" published by the Hong Kong Labor Department. 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).

## VI. 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 the challenges firms face in this area and help bring the risks alive with real-world incidents.

### CASE #1

#### UNAUTHORIZED EMAIL ACCESS

**Summary:** A former employee repeatedly accessed his previous supervisor's email account after leaving the financial company, allowing him to email himself company proprietary information and materials.

**Cause of the Incident:** The insider was an employee of a financial services company. After departing the company, the former employee repeatedly accessed his former supervisor's email account (using credentials provided to him by the former supervisor) on about 100 occasions without authorization. The former employee sent emails from the former supervisor's email account to his personal email account and to his email account at his new employer company. One of those emails included an attachment that contained proprietary information, including internal performance metrics. Another email attached a password-protected spreadsheet with compensation and performance evaluation information for various employees.

**Action Taken:** The company investigated after the supervisor received a bounce-back message to his email account on an email he had not personally sent. The supervisor notified the IT Department, and the company notified legal authorities. The company implemented remedial measures, including hiring a computer forensics firm to conduct a review of its systems.

**Result:** The ex-employee pleaded guilty in federal court to a misdemeanor charge of unauthorized computer intrusion.

**Take-away:** Enforce policies prohibiting employees from sharing passwords/credentials. Establish and enforce password strength requirements. Monitor suspicious email activity through data loss prevention tools and anomalistic monitoring.

### CASE #2

#### CODE THEFT

**Summary:** A software engineer attempted to steal proprietary computer code for a trading platform from his employer, a financial services firm that trades securities and other financial products.

**Cause of the Incident:** The insider was employed as a software engineer at a global trading firm. A substantial portion of the trading done by the firm's employees is facilitated by a proprietary computer trading platform, which the firm was in the process of updating and improving. After learning that his supervisor had resigned and being notified of a meeting with another supervisor about his future at the firm, the insider began to steal the source code for the updated trading platform. The insider researched and ultimately used the technique of steganography to hide the code within other PDF files (personal tax and immigration documents) on his work computer. Before attending the meeting with the new supervisor, the insider attached zip files containing the source code to two saved draft emails addressed to a personal account, but he did not send the emails.

**Action Taken:** During the course of the meeting with the new supervisor, the insider was fired and immediately escorted out of the building, despite multiple requests to return to his desk to retrieve files on his computer. On multiple occasions following his termination, the insider contacted individuals employed by the firm seeking the return of computer files on his firm desktop computer, which he claimed were personal documents.

**Result:** The insider made numerous requests to retrieve the files from a former co-worker, who was working at the direction of law enforcement. The insider was arrested after he reported to the lobby and retrieved a disk he believed contained those files from a law enforcement agent posing as an employee. The insider was charged with one count of attempted theft of trade secrets, which carries a maximum sentence of 10 years in prison and a maximum fine of $250,000 or twice the gross gain or loss from the offense.

**Take-away:** Termination decisions should be managed confidentially, and access privileges should be immediately revoked following termination to prevent the exfiltration of confidential information by disgruntled former employees. Privileged users should be monitored closely to ensure that they do not abuse their access privileges. Network monitoring software should be configured to detect and prevent the download and exfiltration of sensitive information.

## 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 pled 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 by 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.

## VII. BIBLIOGRAPHY


Admin. of Barack Obama, Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), available at http://www.fas.org/sgp/obama/insider.pdf. ["Minimum Standards for Executive Branch Insider Threat Programs"].

Armed Forces Commc'n & Elecs. Ass'n Cyber Comm., Insider Threat: Protecting U.S. Business Secrets and Sensitive Information (2013). ["AFCEA Insider Threat: Protecting U.S. Business Secrets"].

Richard C. Brackney and Robert H. Anderson, RAND Nat'l Sec. Research Div, Understanding the Insider Threat: Proceedings of a March 2004 Workshop (2004), https://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF196.pdf. ["Understanding the Insider Threat"].

Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (2012). ["The CERT Guide to Insider Threats"].

Dawn Cappelli et. al, Common Sense Guide to Prevention and Detection of Insider Threats 3rd Ed. – Version 3.1, Carnegie Mellon, Software Engineering Institute (2009), p. 62, available at https://www.cylab.cmu.edu/files/pdfs/CERT/CSG-V3.pdf. ["Common Sense Guide, 3rd Ed."]

Deanna D. Caputo et al., Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior, MITRE Corp., Institute for Information Infrastructure and Protection (2009). ["Human Behavior, Insider Threat, and Awareness"].

CERT Insider Threat Ctr., Unintentional Insider Threats: Social Engineering (2014), available at http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=77455.

CERT Insider Threat Ctr., Common Sense Guide to Mitigating Insider Threats, Fifth Ed. (2016), available at http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484738.

Matthew L. Collins et. al, Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations, Carnegie Mellon, Software Engineering Institute (2013), available at http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_48680.pdf. ["Collins, Spotlight On Insider Theft of IP"].

Cyber Council: Insider Threat Task Force, Intelligence and Nat'l Sec. Alliance, A Preliminary Examination of Insider Threat Programs in the U.S. Private Sector, (2013).

Adam Cummings et al., Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (2012), available at http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=27971. ["Insider Threat Study: Fraud in the Financial Services Sector"].

David L. Charney, True Psychology of the Insider Spy, 18 Intelligencer: J. of U.S. Intelligence Studies, no. 1, 2010. ["True Psychology of the Insider Spy"].

Defense Intelligence Agency, Your Role in Combating the Insider Threat, http://www.hsdl.org/?view&did=441866. ["Your Role in Combating the Insider Threat"].

Dep't of Defense, DoD Insider Threat Mitigation, available at www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380. ["DoD Insider Threat Mitigation"].

Dep't of Homeland Security, National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat Report (2013). ["National Risk Estimate"].

Dep't of Justice, Prosecuting Computer Crimes, Office of legal Education, Executive Office for United States Attorneys (2007), available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. ["Prosecuting Computer Crimes"].

Dep't of Justice and Federal Trade Comm'n, Antitrust Policy Statement on Sharing of Cybersecurity Information, available at http://www.justice.gov/atr/public/guidelines/305027.pdf. ["DOJ/FTC Antitrust Policy Statement"].

Ernst & Young, Identity and Access Management: Beyond Compliance (May 2013), available at http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf. ["Identity and Access Management"].

FBI, U.S. Department of Justice, The Insider Threat: An Introduction to Detecting and Deterring An Insider Spy, https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view. ["FBI: Detecting and Deterring an Insider Spy"].

FBI and DHS, Public Service Announcement: "Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information" (Sept. 23, 2014), available at https://www.ic3.gov/media/2014/140923.aspx.

FFIEC, Cybersecurity Assessment Tool (May 2017), available at https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

IBM, 2015 Cyber Security Intelligence Index, available at https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf.

Intel Security, White Paper: Tackling Insider Threats (November 2016), available at http://resources.idgenterprise.com/original/AST-0178225_Tackling_Insider_Threats_WP.pdf.

Lori Flynn et al., Best Practices Against Insider Threats in All Nations, Carnegie Mellon, Software Engineering Institute (2013), available at https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084.pdf. ["Best Practices Against Insider Threats in All Nations"].

Lori Flynn et al., International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany, Carnegie Mellon, Software Engineering Institute (2014), available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2014_005_001_88427.pdf. ["International Implementation of Best Practices"].

Frank L. Greitzer et al., Pac. Nw. Nat'l Lab., Predictive Modeling for Insider Threat Mitigation, Dep't of Energy (2009), http://www.pnl.gov/coginformatics/media/pdf/tr-pacman-65204.pdf. ["Predictive Modeling for Insider Threat Mitigation"].

Stephen J. Hadley, Assistant to the President for Nat'l Sec. Affairs, Memorandum on Adjudicative Guidelines from to William Leonard, Director, Info. Sec. Oversight Office (Dec. 29, 2005), https://fas.org/sgp/isoo/guidelines.html.

Carly L. Huth and Robin Ruefle, Components and Considerations in Building an Insider Threat Program (Nov. 7, 2013), https://www.sei.cmu.edu/webinars/view_webinar.cfm?webinarid=69076.

Insider Threat Team, CERT, Unintentional Insider Threats: A Foundational Study (2013), available at http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744.

Todd Lewellen et al., Spotlight On: Insider Threat from Trusted Business Partners Version 2: Updated and Revised (2012) available at https://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_53417.pdf. ["Spotlight On Insider Threat: Trusted Business Partners"]

Michelle Keeney, J.D., Ph.D. et al., Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors (2005), available at https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf. ["Insider Threat Study: Computer System Sabotage"].

Microsoft, How to Protect Insiders from Social Engineering Threats (August 18, 2006), http://technet.microsoft.com/en-us/library/cc875841.aspx.

National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (2014), available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. ["NIST Cybersecurity Framework"].

National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders, U.S. Dep't of Justice, 2nd Ed. (2008), available at https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. ["Electronic Crime Scene Investigation"].

Ponemon Institute, 2016 Cost of Insider Threats: Benchmark Study of Organizations in the United States (September 2016), available at https://dtexsystems.com/cost-of-insider-threat/.

PwC, US Cybercrime: Rising Risks, Reduced Readiness (June 2014), available at http://isacala.org/doc/ISACA-LA_June10-2014-Cybercrime_Rising_Risks_and_Reduced_Readiness.pdf.

Fahmida Y. Rashid, Insider Threat: Limit Privileged Access, BankInfoSecurity (Aug. 23, 2013), https://www.bankinfosecurity.com/new-tips-for-fighting-insider-threat-a-6014.

Raytheon, Best Practices for Mitigating and Investigating Insider Threats (2009), available at https://www.raytheon.com/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf. ["Raytheon Whitepaper"].

Raytheon, Privileged Users White Paper (2015), available at https://www.raytheon.com/capabilities/rtnwcm/groups/cyber/documents/content/rtn_244837.pdf.

Andree Rose et al., Developing a Cybervetting Strategy for Law Enforcement (2010), http://www.iacpsocialmedia.org/wp-content/uploads/2017/02/CybervettingReport-2.pdf. ["Developing a Cybervetting Strategy"].

Robert N. Rose, The Future of Insider Threats, Forbes (August 30, 2016), available at https://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#483d69da7dcb.

Securities and Exchange Commission, Office of Compliance Inspections and Examinations, "National Exam Program Risk Alert, Cybersecurity Examinations" (April 15, 2014), https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf. ["SEC Cybersecurity Risk Alert"].

Eric D. Shaw and Harley V. Stock, Symantec, Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall (2011), available at https://www4.symantec.com/mktginfo/whitepaper/21220067 GA WP Malicious Insider 12 11 dai81510 cta56681.pdf. ["Behavioral Risk Indicators"].

George Silowash et al., Common Sense Guide to Mitigating Insider Threats 4th Edition (2012), available at http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017. ["Common Sense Guide, 4th Ed."]

Sara Sinclair et al., Information Risk in Financial Institutions: Field Study and Research Roadmap, FinanceCom 2007, available at http://www.cs.dartmouth.edu/~sws/pubs/sstjp07.pdf. ["Information Risk in Financial Institutions"].

Suitability and Sec. Clearance Performance Accountability Council, Report to the President (2014), https://obamawhitehouse.archives.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf. ["Suitability and Security Clearance Report"].

Thales, 2017 Data Threat Report, available at https://dtr.thalesesecurity.com/.
Verizon, 2016 Data Breach Investigations Report, available at
http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.
Verizon, 2017 Data Breach Investigations Report (10th Ed.), available at
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.
Vormetric, 2015 Insider Threat Report, available at https://dtr.thalesesecurity.com/insiderthreat/2015/.

WWW.SIFMA.ORG