sifma

CYBERSECURITY

INSIDER THREAT BEST PRACTICES GUIDE

JULY 2014

I. DISCLAIMER

This report was prepared as an account of work within the private and public sector. Neither SIFMA or any of this members, or any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process 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. 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. A systemized, targeted program is therefore necessary to combat insider threat risks.

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, each component in an insider threat mitigation program has a distinctly human element. While external cybersecurity threats can usually only be prevented or detected through technical tools, insider threats commonly exhibit human behaviors that foreshadow the attacker's intent. An appropriately trained insider threat mitigation team can leverage technical tools, such as network monitoring software, and counterintelligence skills to detect and investigate suspicious insider behavior. 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 in ensuring the effectiveness of an insider threat mitigation program, they are not without legal risk. Although privacy and employment laws in the United States are generally permissive of employers' efforts to protect their assets, 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 certain insider threat precautions. Firms should therefore use the framework within this document as a starting point, but must also consult with local counsel throughout the development and implementation of an insider threat program.

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. The recent Edward Snowden incident demonstrates that even the most secure organizations can face devastating losses caused

by a knowledgeable and motivated system administrator who is not contained by adequate internal safeguards or sufficiently rigorous administrative standards and expectations. In response, the National Security Agency (NSA) cut back the number of system administrators by 90%, imposed a "buddy" system for certain access, and disciplined NSA personnel who shared their passwords with Snowden.

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. 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.

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 and good management oversight are necessary to identify the potential warning signs of insider activity and the appropriate method to intervene before an attack occurs and 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 and mitigate the risk through administrative, investigative, technical or disciplinary safeguards and responses.

WHO ARE THE INSIDERS?

An insider is any individual with the ability to access an organization's internal systems and resources. However, individuals who have intentionally carried out insider attacks tend to have similar motivations. Financial gain has always been a popular motivator, made all the more appealing by digitized systems that lend themselves to stealing vast quantities of customer data or intellectual property ("IP") assets to aid larger fraud schemes. Other insiders, motivated by malice against employers or a desire to seek revenge, seek to disrupt, undermine or destroy 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 also noted that perpetrators of insider attacks share common characteristics. For instance, one study found that 80% of insiders who stole confidential or proprietary information were male and over half held technical positions. Other studies have attempted to identify the psychological traits prevalent in insider spies. However, other surveys of insider threat case studies have suggested that insiders do not fit any particular demographic or occupational profile. This lack of an agreed set of characteristics makes it difficult to uniformly apply a set of rules for insider threat discovery. Moreover, using such traits to profile insiders carries some degree of legal risk, particularly in EU member states that restrict automated decision-making based on such profiles. 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 and cohesiveness. The bottom line is that an employee can become an insider threat from almost any background or starting point.

RISK MANAGEMENT

Risk is the probability of loss or damage. Risk management is a function of three variables: criticality, vulnerability and threat. The first element is criticality; how important is this asset to the mission? The second element is vulnerability; in what ways can the asset be compromised, exploited, damaged or destroyed? The third element is threat; who intends to exploit a vulnerability, against what, and what capabilities do they possess to do so? Risk occurs at the intersection of criticality, vulnerability and threat. However, prudent management will focus on segments 4, 5 and 6 of figure 1.

Therefore, the strategy for mitigating the insider threat must:

- Consider the content and relationships among the risk model segments illustrated in figure 1.
- Reduce the overlap area common to criticality, vulnerability and threat
- Require as a matter of prudence that some attention be given to reducing the number of vulnerabilities absolutely, and particularly those vulnerabilities that are known to be exploitable particularly should they become employed as part of a critical asset.
- Note that the threat, criticality, and vulnerability are dynamic and not static. They must be reevaluated often, especially during operations or crisis situations.

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, as is the "cost" to personnel and organizations. Cost/benefit analysis of information security, as part of an overall risk management strategy, is an important topic that should be the focus of further research and attention.

Figure 1 – Department of Defense Risk Model.

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 (disputes with co-workers or superiors, threats, chronic absenteeism). To monitor for both types of behaviors, firms should utilize network monitoring software and implement reporting mechanisms for employees and supervisors to report suspicious activity.

Network monitoring software is a critical tool for detecting internal and external cyber threats, but it is useful only to the extent that key staff can properly interpret the data it generates. To decide what kinds of 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 the 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, and 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 uncovered, the team member should consult with the full insider threat team to discuss whether further monitoring or an expansion of the investigation is warranted.

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 an Insider Risk Mitigation Policy and corresponding training and awareness programs for all personnel. The Policy should explain how personnel can avoid 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. The Policy 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 insider threat risks. Such training should stress the importance of reporting any suspicious behavior, policy violations, personnel conflicts or any other signal of an insider threat risk, and describe the confidential and, in jurisdictions where it is permitted, anonymous mechanisms for reporting, such as whistleblower hotlines. Information from the Policy should be incorporated into training for new employees, and the firm should send periodic reminders of employees' duty to safeguard against and report threats.

Putting the policy and human component together with network and system monitoring 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 is one possible way of structuring a predictive model that combines psychosocial and tradition cyber data to raise red early flags for further analysis. The confidence level that a firm puts in the predictive accuracy of the model will vary depending on the indicators captured, the ability of managers to correctly assess their employees and how well malicious insiders are able to hide their true actions. In addition, prioritization is a key concept within the model as not all possible data can be collected continuously, and some (e.g., HR records) may not be available in real time, hence firms need to adopt an incremental approach to data collection, analysis, and decision making in which different data are collected and analyzed for different individuals depending upon their position and insider threat risk determined by the model.[1]

[1] See Predictive Modeling for Insider Threat Mitigation, pp. 5-7.

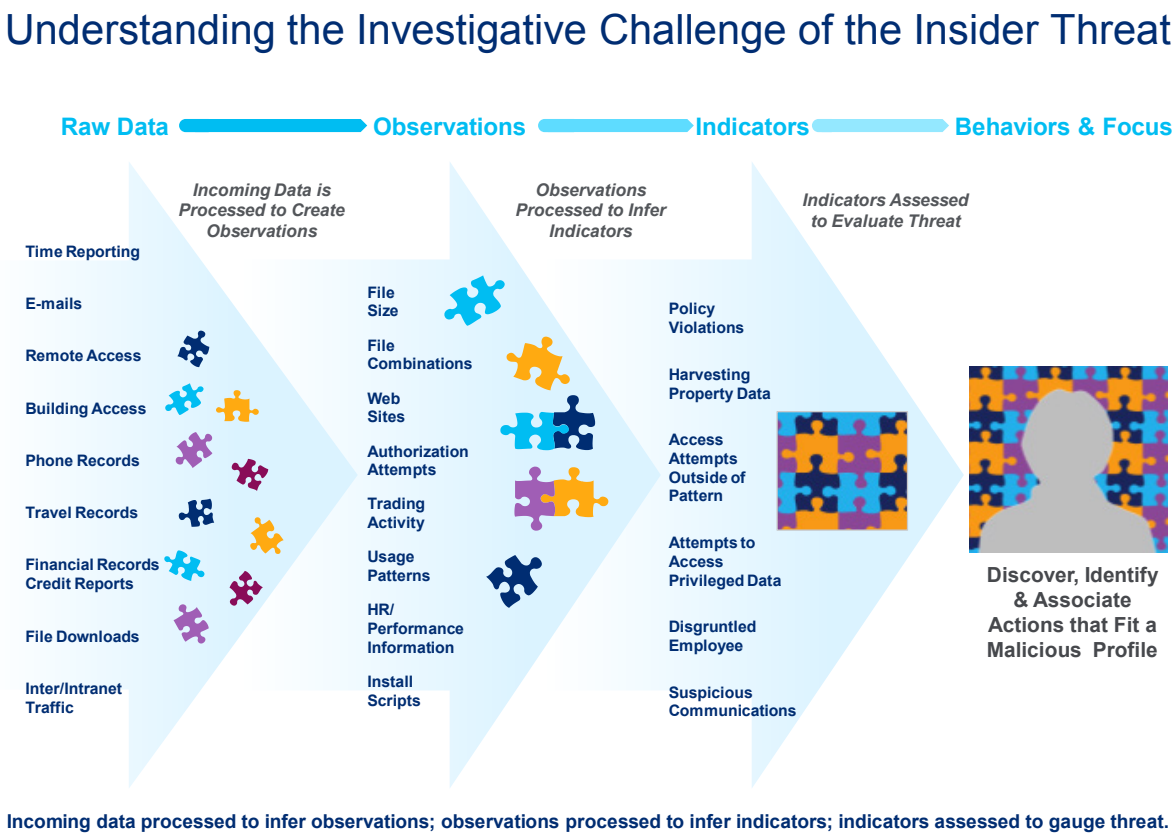

Figure 2 – Model-Based Predictive Classification Concept[2]

At the highest level, the model comprises a knowledge base of indicators and heuristic models of insider behavior. Indicators are essentially the semantics of insider behavior and characteristics interpretations of intentions and actions based on observations. This knowledge base informs all of the components of the insider threat model, and is in turn updated or modified by outputs from components that perform functions such as data collection, data fusion, and analysis. The process can be thought of as a set of multi-layered analysis/inference processes that progress from data to observations to indicators to behaviors, as depicted in Figure 2.

In the end, behaviors are sequences of activities for achieving some specific purpose, whether malicious or benign; the objective is to warn analysts about inferred behaviors consistent with established patterns of insider exploits. The conceptual model employs a hybrid approach based on pattern recognition and model based reasoning. While identifying deviations from "normal" behavior—anomalies—is part of the threat analysis, so too is reasoning about conformance with prototypical behaviors that reflect possible malicious exploits. The challenge is to conduct model based reasoning on the recognized patterns at a semantic level rather than applying template recognition.

[2] Graphic derived from Predictive Modeling for Insider Threat Mitigation.

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, policy, physical security, 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 solely 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 it is allocated sufficient personnel, technology, and financial resources; therefore, visibility of the program to, and support from, top-level management is also essential.

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. While structures can vary, it is the unit's separate identity that 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 the critical point that the organization 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.

The insider threat team should also 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 comprehensive monitoring by IT, security, and other relevant departments has been implemented. 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. The firm should 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/civil liberties protections. The results of these reviews should be reported by internal audit staff to senior management and/or the Board to ensure they are involved, aware, and that issues are resolved in a timely 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 and can also serve as a consistent set of terms for communication and integration into a firm's enterprise risk management program. The principles of taking a risk based approach, which is threat informed, based on the resources available and supportive of the overall business model of the firm hold true whether creating or improving a cybersecurity program or an insider threat mitigation program. The key tasks for each component are described in more details in section IV.

An insider threat program cannot be developed by the firm in a vacuum, however. Because insider threat prevention and detection necessarily require some degree of intrusion into insiders' background and work habits, firms must take into account privacy and employment laws when developing program policies and procedures. Workplace risks stemming from insider programs may be even more pronounced in jurisdictions with more prescriptive privacy protection laws, 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 insider threat mitigation programs to senior management, as well as showing potential areas of weakness in programs. They can be a helpful aid in bringing the risks "alive" to the employees of a firm and "personalizing" the threat, since most people can put themselves into these scenarios.

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 are to short titles, whose full citations can be found in the bibliography.

Regarding implementation steps firms can take to put the core elements of this document into practice, we suggest firms follow an approach similar to what is described in the NIST Cybersecurity Framework.[3] The steps outlined for prioritization, 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 repeat and overlap with other risk practices. Below are the seven steps, modified slightly to call out key items specific to insider risk, that firms should follow in putting the core elements of this document into practice.

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

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 future state to determine gaps. Next 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 in regards to the gaps identified in the previous step. It then monitors its current practices against the target state.

This guide is only meant 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 developing 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.

IV. CORE COMPONENTS

Identitiy (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	**Inventory**: Identify and inventory all assets within the firm. Require contractors who use information systems to at least meet the same requirements, contractually as employees regarding accountability, random computer audits, timely access changes, and password policy. In many cases it may make sense to have enhanced oversight and requirements.	Common Sense Guide,[1] Best Practice #6 NIST Cybersecurity Framework (ID.AM-1, 2, 4) DoD Insider Threat Mitigation, Appendix A, Rec. 2.10
	Criticality: Determine what assets are most critical to the proper execution of the organization's business goals. Items to be considered are: • Systems (software, hardware, devices) • Data & Intellectual Property • Personnel • Third party Providers • Partnerships	NIST Cybersecurity Framework (ID.AM-5) DoD Insider Threat Mitigation, Appendix A, Rec. 1.10
	Security agreements: Define explicit security agreements with all third parties, including access restrictions and monitoring capabilities.	Common Sense Guide, Best Practice #9 NIST Cybersecurity Framework (ID.AM-6; PR.AT-3)
Governance (ID. GV): Structure an insider threat team and develop corresponding policies and procedures for monitoring and management	**Structure**: Determine the location of the insider threat team within the organization **Staff**: Hire new personnel with counterintelligence experience to staff the insider threat team, or train existing employees in relevant skills **Policies and Procedures**: Assign monitoring and investigation roles and responsibilities within team; establish policies and procedures for conducting investigations. Ensure oversight on the program is established at the board level.	AFCEA Insider Threat: Protecting U.S. Business Secrets, pp. 2-4, 6
	Designation of Corporate Sponsor: Firms should establish a senior official who will be principally responsible for establishing and operating an insider threat program that will link into other areas and functions within the organization (e.g. Human Resources, Information Technology, etc.)	Minimum Standards for Executive Branch Insider Threat Program, Section D
	Global governance: Ensure that the legal and regulatory requirements of each region and country in which the firm operates are understood and managed, including laws relating to privacy and civil liberties. Adjust policies, procedures and practices to account for cultural differences across regions.	Best Practices Against Insider Threats in All Nations International Implementation of Best Practices
	Communication to personnel: After an insider threat program is established, communicate its existence and associated policies and procedures to employees.	Common Sense Guide, Best Practice #16 DoD Insider Threat Mitigation, Appendix A, Rec. 3.1 AFCEA Insider Threat: Protecting U.S. Business Secrets, pp. 6-8

Identitiy (ID) continued		
Category	Subcategories	Informative References
Risk Assessment (ID.RA): Understand the risk that insiders pose to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Vulnerabilities**: Identify the vulnerabilities within critical assets that could make them susceptible to an insider attack. **Threats**: Identify external threats that could be the source of an attack delivered by an insider in addition to the conditions that could lead to an organization employee or resource becoming a threat. **Impacts**: Apply threats (both internally driven and externally driven but internally supported) to critical systems and vulnerabilities in order to assess the risk to the organization and the possible impacts to the execution of the business and achievement of its goals.	National Risk Estimate DoD Insider Threat Mitigation, Section 2.6, Risk Management, pages 7-8
	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.	Common Sense Guide, Best Practice #1 Spotlight On Insider Threat: Trusted Business Partners, pp. 12-14 National Risk Estimate
Risk Management Strategy (ID. RM): Establish policies and procedures to identify kinds of behaviors that indicate insider activity	**Suspicious network and application activity**: Identify behaviors that could indicate suspicious insider activity if they occur more frequently than network baseline. Establish a list of indicators that could tip investigators to suspicious behaviors.	Human Behavior, Insider Threat and Awareness Symantec White Paper Behavioral Risk Indicators Common Sense Guide, Best Practice #16
	Concerning behaviors: Create profile of behaviors and characteristics that may indicate that an individual is an insider threat. Develop models showing appropriate access to assets and behavior with respect to such assets for each type of employee. Create a comprehensive list of system and user behavior attributes that can be monitored to establish normal and abnormal patterns to enable anomaly and misuse detection.	Predictive Modeling for Insider Threat Mitigation, at 9 FBI: Detecting and Deterring an Insider Spy Understanding the Insider Threat, pp. 90-91 DoD Insider Threat Mitigation, Appendix A, Rec. 6.8
	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.	DoD Insider Threat Mitigation, Appendix A, Recs. 1.3, 2.7
	Legal risk analysis: Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.	National Risk Estimate, Recommendation #5, page iii

Protect (PR)		
Category	Subcategories	Informative References
Access Control (PR.AC): Implement appropriate technical and administrative safeguards to ensure that access to assets and systems are limited to authorized users.	**Technical safeguards**: Strengthen cybersecurity standards in accordance with NIST Cybersecurity Framework. Manage remote access from both internal and external parties. Implement controls to prevent unauthorized escalation of user privileges and lateral movement among network resources.	Common Sense Guide, Best Practice # 13 NIST Cybersecurity Framework (PR.AC-3; PR.MA-2) SEC Cybersecurity Risk Alert, p. 3
	Administrative safeguards: Implement processes and policies to limit access rights/credentials of all users, but especially privileged users, to ensure that only the minimum amount necessary is provided. Establish personnel security vetting procedures commensurate with an individual's level of information system access.	Common Sense Guide, Best Practices # 7, 8, 10 NIST Cybersecurity Framework (PR.AC-1-5) DoD Insider Threat Mitigation, Appendix A, Recs. 5.3, 2.3
	Off-boarding procedures: Implement standardized, comprehensive off-boarding procedures to ensure all access to company information is terminated upon employees' departure, including: • Termination of physical and electronic access rights • Change passwords to all systems and data that the employee had access to, including shared accounts, files and folders • Collect all equipment given to employee • Delete remote access tools from employees' personal devices (e.g., RSA tokens)	Common Sense Guide, Best Practice #14 NIST Cybersecurity Framework (PR.AC-1-3)
	Toxic Combinations of Entitlements: Seek out and remove conflicts of system access permissions that allows a user to break the law, violate rules of ethics, damage customers' trust, or even create the appearance of impropriety and ensure that segregation of duties analysis is performed to prevent its occurrence in the future.	Identity and Access Management Information Risk in Financial Institutions
Awareness and Training (PR. AT): Implement programs to alert personnel to insider threat risks and consequences	**Education and training topics**: Ensure that employees, contractors, and other personnel receive regular training and updates on topics relevant to mitigating insider threats, including: • Protocol for handling sensitive information, including IP and customer information • Responsibilities and processes for alerting management of suspicious activities • Handling of critical assets and physical and electronic access controls. Establish mandatory minimum standards for security education, awareness and training programs related to the insider threat. Ensure training is delivered on a regular basis to existing employees and is a part of all new hire training packages. Document attendance and compliance similar to other mandatory training.	Common Sense Guide, Best Practice #3 NERC CIP-004 DoD Insider Threat Mitigation, Appendix A, Rec. 3.3 SEC Cybersecurity Risk Alert, p. 3

Protect (PR) continued		
Category	Subcategories	Informative References
	Notice and consent for computer use policy: Upon hiring, and annually thereafter, require personnel to read and acknowledge their agreement to a computer use policy. The policy should indicate that any activity on any firm computer, electronic device (including company-owned mobile devices) or firm owned network (i.e. employees under BYOD program connecting to the firm's network or systems) is subject to monitoring and could be used against them in a criminal, security, or administrative proceeding. Computer use policies should state explicitly that users do not have any expectation of privacy on work computers and devices. Mandate use of "warning banners" or other on-line messages that serve to raise the awareness to the need for secure and appropriate system usage, and that highlight recent observed misuse and its consequences.	Minimum Standards for Executive Branch Insider Threat Programs, Section H.3 DoD Insider Threat Mitigation, Appendix A, Recommendation 4.2
	Awareness programs: Highlight importance of preventing and detecting insider threats through periodic emails, memos, and/or announcements. Potential awareness topics include: • Reporting suspected insider activity to insider threat team • Methodologies of adversaries to recruit trusted insiders and collect sensitive information ("social engineering"), and steps that employees can take to protect themselves against such threats • Indicators of insider threat behavior • How to safely use social media	Minimum Standards for Executive Branch Insider Threat Programs, Section I.1.a-c How to Protect Insiders from Social Engineering Threats Common Sense Guide, Best Practice 18
Information Protection Processes and Procedures (PR.IP): Maintain policies, processes and procedures to protect systems and assets from insider threats	**Policy maintenance and enforcement**: Clearly document and consistently enforce policies and controls **Backup data**: Ensure data backups are available and recovery processes account for the actions of malicious insiders.	Common Sense Guide, Best Practice #2 Common Sense Guide, Best Practice #17
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.	Best Practices and Controls for Mitigating Insider Threats, Slide 17 Common Sense Guide, Best Practice #19 NIST Cybersecurity Framework (PR.DS-5)

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	**Network and Application Baseline**: Monitor networks over a designated period to determine a "normal"obaseline of network activity. Baseline should be periodically evaluated to account for changes in technology use among personnel (e.g., influx of millennial employees may results in greater mobile device and social network use).	Common Sense Guide, Best Practice #17 SEC Cybersecurity Risk Alert, p. 5
	Monitor audit logs: Develop tools for effective scanning and analysis of system and network audit logs to detect anomalous system and insider activity.	DoD Insider Threat Mitigation, Appendix A, Recommendation 6.2
	Technical infrastructure: Where possible, implement monitoring software on the application layer in order to distinguish user behavior from automated machine behavior (e.g., routine browser cookie deletion). Useful tools include: • Full-packet sensors to investigate actions or inform response activities • Web content sensors to track risky internet use • Updated virus/malware scanners • Log correlation engines or system information event management (SIEM systems to log, monitor, and audit employee actions • Systems to log, monitor, and audit employee actions and response activities on the application layer in order to distinguish user behavior from automated machine	Common Sense Guide, Best Practice #12 NIST Cybersecurity Framework (DE.CM-1-7) Human Behavior, Insider Threat and Awareness
Security Continuous Monitoring (DE. CM): Designate appropriate personnel for insider threat mitigation team and implement continuous intelligence monitoring	**Insider threat mitigation personnel**: Larger firms will benefit from a separate unit staffed by specially trained counterintelligence personnel. Individuals with experience in government counterintelligence are particularly valuable. Smaller firms for which a separate counterintelligence unit is not practical should still have employees designated for insider threat monitoring and investigations. Such employees should ideally have experience or training in: • Personnel investigations • Restricting details of inquiries to relevant staff • Determining when it is appropriate to involve outside experts and law enforcement in investigations • Conduct a forensics analysis of a incident	Minimum Standards for Executive Branch Insider Threat Program (Point F) AFCEA Insider Threat: Protecting U.S. Business Secrets, p. 6
	Resource allocation: Institute more stringent monitoring policies on privileged users and high risk personnel.	Common Sense Guide, Best Practice #10 NIST Cybersecurity Framework (DE.CM-3)
	Continuous evaluation program: Instead of re-evaluating employees at pre-set duration as one-time events based on their access and critically, establish a program where employees are constantly monitored and data is collected at regular intervals in small segments to look for changes over a longer period of time. Use surveys of employees and data collection in order to catalog life events and changes as they occur.	Suitability and Security Clearance Report Common Sense Guide, Best Practice #5 DoD Insider Threat Mitigation, Appendix A, Recommendation 2.7

Detect (DE) continued		
Category	**Subcategories**	**Informative References**
	Increase awareness of potential threats: Gain new intelligence about possible threats through information sharing with government agencies and other private organizations Report instances of insider threats at your organization to DHS, FBI, and Secret Service Capitalize on information sharing programs run by DOD, DHS and FBI Consider participation in information depositories when/if they are developed by Congress Build relationships with local and state law enforcement and monitor local data sources as consolidated reporting is limited currently.	DOJ/FTC Antitrust Policy Statement Suitability and Security Clearance Report
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 exhaust" on the internet. 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 –nsuspicious behaviors that may indicate insider activities, or security flaws that are vulnerable to exploitation by insiders. Such systems may include a whistleblower hotline, online reporting portals, or an employee designated to receiving tips. Establish mechanisms through which customers may report fraudulent transactions or other suspicious activity on their accounts (e.g., unauthorized access attempts). Ensure existing programs are linked to the insider threat analysis activities. Make use of existing data collection platforms and repurpose collected information for analysis.	Your Role in Combating the Insider Threat

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

Respond (RS) continued		
Category	**Subcategories**	**Informative References**
Analysis (RS.AN): Classify incident to determine appropriate investigative procedure	**Type of insider**: Determine whether the insider incident was a result of unintentional or intentional activity. An attack that was unintentionally enabled by an insider – e.g., through the use of their access credentials – should be further investigated to determine whether a malicious insider facilitated the attack. Implement tools for a rapid and effective audit of a host computer system to detect any anomalies in its programs and files. Develop capabilities to do forensic analysis 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, the 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
	Personnel action: Remove access from the person suspected to remove the risk of continued or new malicious activity. Determine what disciplinary or legal action should be taken against the person(s) responsible for the incident. Where appropriate, consider legal action to recover or enjoin the use of stolen information. Ensure that management invokes minor sanctions for low level infractions of the stated security policy, in order to demonstrate the organization's commitment to the policy and vigilance in the enforcement of its principles.	DoD Insider Threat Mitigation, Appendix A, Recommendation 4.3

Recover (RC)		
Category	**Subcategories**	**Informative References**
Recovery Planning (RC.RP): Execute recovery processes and procedures to control the scope of the incident and restore affected data	**Isolate and restore**: Isolate any system compromised by the attack to prevent damage to other systems. In accordance with the firm's system recovery plan, restore damaged or destroyed data by retrieving backup tapes and, when necessary, engaging IT or outside forensic professionals to recover backup files on servers and hard drives.	NIST Cybersecurity Framework RC.RP-1
Improvements (RC.IM): Evaluate incident and incorporate lessons learned into future activities	**Incident evaluation**: Meet with senior management and other appropriate personnel to discuss potential improvements to prevent similar incidents in the future. Consider engaging independent auditors to evaluate security and monitoring systems to identify weaknesses and suggest improvements.	NIST Cybersecurity Framework RC.IM-1, RC.IM-2

Recover (RC) continued		
Category	Subcategories	Informative References
Communications (RC.CO): Communicate with internal and external parties to ensure coordinated response to incident	**Public relations**: Work with internal and external PR personnel to develop company's public response to incident. Designate individuals authorized to speak on behalf of the organization in regards to the incident, and inform others of policy on speaking to outsiders regarding the incident.	NIST Cybersecurity Framework RC.CO-1, RC.CO-2
	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 US 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 ECPA." See Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009), Appendix A, p. 209, available at http://www.justice.gov/criminal/cybercrime/docs/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 such efforts violate the SCA. See, e.g., Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 920 (W.D. Wis. 2002).

2. STATE LAW

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.

Nearly every state has enacted a law analogous to the federal Wiretap Act. While most state wiretap statutes mirror the federal law's requirements and exceptions, a dozen states – California, Connecticut, Florida, Illinois Maryland, Massachusetts, Michigan, 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). Accordingly, while firms may wish to protect themselves against claims under all-party consent wiretap statutes by including a monitoring warning in all emails sent from company email addresses, such statutes may not pose significant legal risk in this context.

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); People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd., 895 P.2d 1269, 1282 (Nev. 1995) (stating 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.

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). Although FCRA only applies to consumer reports obtained

from consumer reporting agencies (CRAs), some states – most notably California[4] – impose similar restrictions for investigations conducted in-house as well. Employers will therefore minimize their risk exposure by complying with FCRA standards for all types of financial background investigations and screening.

FCRA does not generally restrict what information may be obtained in background checks, but rather how it is obtained. The law applies to any information obtained in a consumer report, which is broadly defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. . . ." 15 U.S.C. § 1681a(d)(1). An employer must provide a clear, conspicuous, written notice to an applicant or current employee, and obtain his or her consent, to get 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 Bureau of Consumer Protection Business Center, 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 (05-11-98).

Investigative consumer reports, though more onerous to obtain, may reveal even more information about a job candidate or employee. 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: notice must be provided within three days after a report is requested, § 1681d(a)(1)(A), and 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 Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act") 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 excep 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).

[4] 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.

2. EEOC GUIDANCE ON THE CONSIDERATION OF CRIMINAL HISTORY

While no law forbids the consideration of an individual's criminal history in making employment decisions, the Equal Employment Opportunity Commission (EEOC) has issued guidance stating that such consideration may violate Title VII of the Civil Rights Act of 1964, 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), http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm#VIII [hereinafter "Guidance"]. The Guidance provides that a policy of excluding applicants based on their criminal histories violates Title VII unless such 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 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."

Recently, the EEOC has brought enforcement actions against two large employers for failing to provide robust, individualized assessments for those excluded by criminal history screening policies. See EEOC v. BMW Manufacturing Co. LLC, No. 7:13-cv-01583 (D.S.C. July 26, 2013); EEOC v. DolGenCorp LLC, No. 1:13-cv-04307 (N.D. Ill. June 12, 2013). Although the outcome of these cases has yet to be determined, and some states and entities are challenging the agency's policy of requiring individualized assessments, for the time being firms must weigh the benefit of criminal screening for the job in question with the potential risks of violating Title VII. Firms may want to strike this balance by 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.

3. SOCIAL MEDIA

While examining publicly-available social media profiles can be an informative part of applicant screening, firms should be mindful that nineteen states have enacted laws prohibiting employers from forcing applicants or employees to reveal their personal, private profiles. Such legislation prohibits 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-5-34:6B-10 (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.

All but three of these laws, however, contain language clarifying that the laws do not prohibit employers from complying with federal, state, or self-regulatory organization (SRO) obligations to screen employees. The three states that do not contain this limitation – California , Colorado, and Maryland – each 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,

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. 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 http://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 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 2011	Implementation of the Budapest Convention on Cybercrime	Regulation of Investigatory Powers Act 2000	Computer Crimes Ordinance (No. 23 of 1993)
Privacy	IT Rules	Federal Personal Data Protection Act of 2001; Act on Employee Data Protection; Federal Data Protection Act	UK Data Protection Act 1998	Personal Data (Privacy) Ordinance (Cap. 486)
Human Resources	Persons with Disabilities Act; Industrial Law; Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal Act)	Federal General Equal Treatment Act	Human Rights Act 1998	Employment Ordinance (Cap. 57)

2. OVERVIEW OF RELEVANT PROVISIONS

Germany: Germany's primary privacy law is the Federal Personal Data Protection Act of 2001, which implements the EU Data Protection Directive. Section 32 of the Federal Personal Data Protection Act of 2001 permits data collection and processing for employment purposes "where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract." It also requires that any collection and use of employees' personal data during investigations be supported by documented suspicion, and that the collection is necessary and the employee does not have an overriding interest in prohibiting collection. 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." However, employers are entitled to carry out random, contemporary monitoring of log data, so long as the process is fully transparent.

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 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 particular, 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, therefore, ensure 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.

Indian employment law is another area relevant to insider threats. Unlike the United States, India has no law requiring notification to consumers that a credit check has been requested about them. In addition, 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. However, Indian Constitution Article 15 prohibits state discrimination based on "religion, race, caste, sex or place of birth." Women in the private workforce are also protected by the Industrial Law and the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act.

Although background checks are 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 various factors, including whether the data users have complied with the guidelines published by the Privacy Commissioner.

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 monitoring, 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 paragraph 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.

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, several groups, including industry non-profits and government agencies, have compiled summaries of reported insider incidents that have occurred over the years. Below is a representative sample of summaries of incidents involving cyberattacks that resulted in firm-wide losses. These 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 personal accounts.

SOFTWARE MANIPULATION/ABUSE OF ACCESS PRIVILEGES

CASE #1

Summary: Software developer manipulated software to link a personal card to corporate accounts, allowing him to gain millions of rewards points redeemable for items of value.
Source: Insider Threat Study: Fraud in the Financial Services Sector, p. 19

The insider was employed as a lead software developer at a prominent credit card company, which offered a rewards program where customers could earn points based on the volume and frequency of their credit card usage. These points could later be redeemed for gift cards, services, and other items of monetary value. Because a corporate account could hypothetically accumulate an immense number of rewards points, the program was configured in such a way that the back-end software would not allow corporate accounts to earn points. An insider devised a scheme by which he could earn fraudulent rewards points by bypassing the back-end checks in the software and linking his personal accounts to corporate business credit card accounts of third-party companies. After compromising a co-worker's domain account by guessing the password, he was able to implement a backdoor that allowed him to successfully link his personal accounts to several corporate accounts. The insider cashed in the rewards points for items of value, such as gift cards to popular chain stores, and sold them in online auctions for cash. In all, the insider was able to accumulate approximately 46 million rewards points, $300,000 of which he was able to convert into cash before being caught by internal fraud investigators. The insider admitted to the scheme and bargained with investigators for a reduced sentence if he agreed to provide information on his technical backdoor and offer insight as to how organizations might prevent a similar occurrence from happening in the future.

Take-away: Establish and enforce password strength requirements for user accounts and monitor software for unauthorized code changes.

CASE #2

Summary: Bank loan processor used privileged access to fraudulently increase personal loans.
Source: Insider Threat Study: Fraud in the Financial Services Sector, p. 22

The insider worked as the loan processor for a banking institution. As part of her job responsibilities, she had full privileges to read and modify loan information within the organization. She took out two legitimate loans totaling

$39,000 from her employer organization for her own personal expenses, which in itself was not a violation of company policy. However, to help pay for additional personal expenses, she used her privileged access several times to fraudulently increase her personal loan amounts. She then withdrew the resulting difference, thereby committing embezzlement. She was discovered when a routine audit revealed that essential loan documentation was missing from her loan account, which the insider had removed to cover up the fraud. By the end of her scheme, she had stolen approximately $112,000. She was sentenced to 18 months in prison and 5 years' probation and was ordered to pay full restitution.

Take-away: Privileged users, including supervisors, should be monitored closely to ensure that they do not abuse their access privileges. Transactions involving employees who also have accounts with the institution should be overseen by someone other than the employee account holder.

CASE #3

Summary: Software developer implemented obscure function allowing him to conceal illegal trades that totaled $691 million.
Source: Common Sense Guide, 3rd ed., p. 56

A currency trader (who also happened to have a college minor in computer science) developed much of the software used by his organization to record, manage, confirm, and audit trades. He implemented obscure functionality in the software that enabled him to conceal illegal trades totaling $691 million over a period of five years. In this case, it was nearly impossible for auditors to detect his activities. The insider's supervisor managed both the insider and the auditing department responsible for ensuring his trades were legal or compliant. When auditing department personnel raised concern about the insider's activities, they were doing so to the insider's supervisor (who happened to be their supervisor as well). The supervisor directed auditing department personnel not to worry about the insider's activities and to cease raising concern, for fear the insider would become frustrated and quit.

Take-away: Auditing personnel, including managers, should be wholly independent from other firm functions to ensure the integrity of their audits and investigations.

CASE #4

Summary: Application developer modified code so that no alert was sent when data was illegally modified, enabling him to steal large sums of money without detection.
Source: Common Sense Guide, 3rd ed., p. 68

An organization built automated monitoring into its software that sent automatic notification to the security officer any time a highly restricted screen was used to modify information stored in the database. Role-based access control restricted access to this screen to a few privileged users; the automated notification provided a second layer of defense against illegal data modification using that function. However, a developer of the application who happened to have access to that function modified the code so that the automated notification was no longer sent. He then proceeded to use the function to steal a large sum of money from his employer. The organization had a configuration management system in place for software changes; when a program was compiled, a report was produced listing which files were compiled, by which computer account, and when. It also listed modules added, modified, or deleted. Unfortunately, this report was not monitored, and therefore the application changes were not detected during the year and a half over which the fraud was committed.

Take-away: Simply running network monitoring software on firm systems is not enough to detect suspicious insider activity. Results from automated programs must be monitored by individuals trained in interpreting activity to recognize potential threats.

DATA THEFT

CASE #5

Summary: Call center employees printed screen captures of customer records and used information to issue fraudulent credit cards and make purchases.
Source: Insider Threat Study: Fraud in the Financial Services Sector, p. 31

The insider and his accomplices were customer service employees at a financial institution's call center. These employees had access to customer information, which included personally identifiable information (PII). While accessing customer accounts during the normal course of business, the insider and his accomplices printed screen captures of customer records and gave them to an outsider to make fraudulent purchases. Sometimes the insiders modified customer records to have a credit card sent to an address to which they had access, and they would use these newly issued cards to make fraudulent purchases. One insider even purchased a wedding dress with a fraudulent card. The organization's total losses exceeded $2.2 million.

Take-away: If technically feasible, printing and screen captures should be disabled within customer information databases if there is no business necessity for them. Printing activity and changes to customer information databases should be closely monitored for unusual patterns.

CASE #6

Summary: Upon resigning, a firm executive made a backup copy of his work computer hard drive, which contained proprietary information from the firm.
Source: Common Sense Guide, 3rd ed., p. 41

Four executives left their firm to form a competing company. A few days before they left, one of them ordered a backup copy of the hard drive on his work computer, which contained customer lists and other sensitive information, from the external company that backed up the data. The company also alleged that its consulting services agreement and price list were sent by email from the insider's work computer to an external email account registered under his name. The insiders, two of whom had signed confidentiality agreements with the original employer, disagreed that the information they took was proprietary, saying that it had been published previously.

Take-away: Employers should explicitly set forth in policies what information is considered proprietary, and files containing such information should be marked as such to avoid later disputes. Requests for copies of large amounts of data, including hard drives, should require approval and be justified by a legitimate business purpose.

CASE #7

Summary: Disgruntled engineer who was terminated from his position deleted file containing major project valued at $2.6 million.
Source: Common Sense Guide, 4th ed., pp. 36-37

An e-commerce company employed an insider as a chief project engineer. The organization took the insider off of a major project and subsequently terminated his employment. Afterward, the insider's accomplice, an employee of the victim organization, allegedly gave the insider the password to the server storing the project he had worked on. According to some sources, the insider wanted to delete the project file for revenge. Other sources claim that the insider wanted to hide the file during a presentation so that his accomplice could recover the file, appear to be a hero, and avoid being fired. The insider did delete the file, but the organization was able to recover the lost data. The project was valued at $2.6 million. The insider and his accomplice were arrested.

Take-away: Remote access to sensitive materials should be restricted to pre-approved individuals who have a business necessity for such access. Data should be routinely backed up and stored in a location separate from the business's primary servers.

CASE #8

Summary: Upon quitting job, disgruntled former Vice President for engineering copied a file containing a developing product to removable media, deleting the file from the server and backup tapes. He held the file hostage, offering to restore it for $50,000.
Source: Common Sense Guide, 3rd ed., pp. 44-45

A vice president for engineering who was responsible for oversight of all software development in the company was engaged in a long-running dispute with higher management. This dispute was characterized by verbal attacks by the insider and statements to colleagues about the degree of upset he had caused to management. The insider engaged in personal attacks once or twice a week and on one occasion, in a restaurant, screamed personal attacks at the CEO of the company. A final explosive disagreement prompted the insider to quit. When no severance package was offered, he copied a portion of a product under development to removable media, deleted it from the company's server, and removed the recent backup tapes. He then offered to restore the software in exchange for $50,000. He was charged and convicted of extortion, misappropriation of trade secrets, and grand theft. However, the most recent version of the software was never recovered.

Take-away: The insider threat team and human resources should be alerted to any recurring personnel disputes and intervene to take appropriate action. Users' access credentials should be immediately deactivated after an employee resigns or is terminated.

CASE #9

Summary: Product engineer downloaded trade secrets and design specifications valued at $20 million and took it with him to work at a competing foreign company.
Source: Spotlight on Insider Theft of IP, p. 9

The insider was a product engineer at the victim organization, an automobile manufacturer. Due to the nature of the insider's work, the insider had access to trade secrets and design specifications from the company. Nearly two years prior to leaving the organization, the insider downloaded design specifications and used them to aid in finding employment at competing organizations. A year and a half after stealing the design specifications, the insider accepted a job offer from a company that manufactured automotive electronics in a foreign country. The insider continued to work at the victim organization for two months after accepting this job offer. The night

before permanently leaving the victim organization, the insider downloaded thousands of documents unrelated to the insider's job onto an external hard drive. These documents included company designs for various automotive systems and were valued at more than $20 million. One year after leaving the victim organization, the insider was hired by a direct competitor of the victim organization located in the same foreign country as the first beneficiary organization. The insider was arrested upon returning to the United States. Forensic examiners examined the insider's laptop and found thousands of confidential and proprietary documents from the victim organization. The insider was arrested, convicted, and sentenced to over five years in prison.

Take-away: Access to sensitive files should be restricted to those who have a business necessity for such access. While all use of removable media should be highly controlled, external transfer of sensitive files should be disabled for all users below a designated level of management.

SYSTEM SABOTAGE

CASE #10

Summary: Disgruntled lead developer erased the hard drive of his company-provided laptop, which contained the only copy of an application's source code.
Source: Common Sense Guide, 3rd ed., pp. 40-41

The lead developer of a critical production application had extensive control over the application source code. The only copy of the source code was on his company-provided laptop; there were no backups performed, and very little documentation existed, even though management had repeatedly requested it. The insider told coworkers he had no intention of documenting the source code and any documentation he did write would be obscure. A month after learning of a pending demotion, he erased the hard drive of his laptop, deleting the only copy of the source code the organization possessed, and quit his job. It took more than two months to recover the source code after it was located by law enforcement in an encrypted form at the insider's home. Another four months elapsed before the insider provided the password to decrypt the source code. During this time the organization had to rely on the executable version of the application, with no ability to make any modifications.

Take-away: Project supervisors should ensure that all data relating to the project is stored on the firm's centralized database and automatically backed up. Network activity of demoted employees should be closely monitored for unusual activity.

CASE #11

Summary: Programmer at a telecommunications company inserted logic bomb into the code of a premier product, causing disruption to company's services to customers.
Source: Common Sense Guide, 3rd ed., p. 62

A programmer at a telecommunications company was angry when it was announced that there would be no bonuses. He used the computer of the project leader, who sat in a cubicle and often left his computer logged in and unattended, to modify his company's premier product, an inter-network communication interface. His modification, consisting of two lines of code, inserted the character "i" at random places in the supported transmission stream and during protocol initialization. The malicious code was inserted as a logic bomb, recorded in the

company's configuration management system, and attributed to the project leader. Six months later, the insider left the company to take another job. Six months after that, the logic bomb finally detonated, causing immense confusion and disruption to the company's services to their customers.

Take-away: Computers should automatically log-out after a given period of inactivity, and users should be required to enter additional credentials to change file codes.

CASE #12

Summary: Underground leader of hacking group was hired as a security guard at a hospital. Using various malicious hacks, he caused the hospital's HVAC system to shut down and was almost able to usurp the computer systems to conduct a DDoS attack.
Source: Common Sense Guide, 4th ed., p. 33

A hospital facility employed the insider, a contractor, as a security guard. The insider wasextensively involved with the internet underground and was the leader of a hacking group. Theinsider worked for the victim organization only at night and was unsupervised. The majority ofthe insider's unauthorized activities involved a heating, ventilation, and air conditioning (HVAC)computer. This HVAC computer was located in a locked room, but the insider used his securitykey to obtain physical access to the computer. The insider remotely accessed the HVAC computer five times over a two-day period. In addition, the insider accessed a nurses' station computer, which was connected to all of the victim organization's computers and also stored medical records and patient billing information. The insider used various methods to attack the organization, including password-cracking programs and a botnet. The insider's malicious activities caused the HVAC system to become unstable, which eventually led to a one-hour outage. The insider and elements of the internet underground were planning to use theorganization's computer systems to conduct a distributed-denial-of-service (DDoS) attack against an unknown target. A security researcher discovered the insider's online activities. The insider was convicted, ordered to pay $31,000 restitution, and sentenced to nine years and two months of imprisonment followed by three years of supervised release.

Take-away: Firms should conduct background checks on all personnel who may have access to firm systems. Any access to computers should require a user to enter credentials, and the system should generate alerts when a computer is accessed off-hours.

CASE #13

Summary: Disgruntled systems administrator consolidated critical software, deleted it, and stole the backup tapes for it, causing $10 million in damage.
Source: Insider Threat Study: Computer System Sabotage, p. 3.

A system administrator, angered by his diminished role in a thriving defense manufacturing firm whose computer network he alone had developed and managed, centralized the software that supported the company's manufacturing processes on a single server, and then intimidated a coworker into giving him the only backup tapes for that software. Following the system administrator's termination for inappropriate and abusive treatment of his coworkers, a logic bomb previously planted by the insider detonated, deleting the only remaining copy of the

critical software from the company's server. The company estimated the cost of damage in excess of $10 million, which led to the layoff of some 80 employees.

Take-away: Network monitoring software should be configured to alert monitoring personnel to high-volume data transfers. Firms should regularly inform their employees of confidential reporting mechanisms for suspicious behavior, and stress the importance of reporting during routine training.

CASE #14

Summary: Laid-off application developer gained remote access to company network, hacked its website, reset network passwords, and changed pricing records.
Source: Insider Threat Study: Computer System Sabotage, p. 3.

An application developer, who lost his IT sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's web pages, changing text and inserting pornographic images. He also sent each of the company's customers an email message advising that the website had been hacked. Each email message also contained that customer's usernames and passwords for the website. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords and changed 4,000 pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay $48,600 restitution to his former employer.

Take-away: Following a hacking incident, passwords to accounts on all potentially compromised systems should be reset. Former employees – particularly those identified as being upset or angry with the firm – should be considered as suspects in such incidents.

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), http://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

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"].

Dept'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, http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat. ["FBI: Detecting and Deterring an Insider Spy"].

Lori Flynn et al., Best Practices Against Insider Threats in All Nations, Carnegie Mellon, Software Engineering Institute (2013), available at http://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 http://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 Adjundicative Guidelines from to William Leonard, Director, Info. Sec. Oversight Office (Dec. 29, 2005), http://www.fas.org/sgp/isoo/guidelines.pdf.

Carly L. Huth and Robin Ruefle, Components and Considerations in Building an Insider Threat Program (Nov. 7, 2013), http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=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 http://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 http://resources.sei.cmu.edu/asset_files/CERTResearchReport/2005_013_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"].

Fahmida Y. Rashid, Insider Threat: Limit Privileged Access, BankInfoSecurity (Aug. 23, 2013), http://www.bankinfosecurity.com/insider-threat-limit-privileged-access-a-6014.

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

Andree Rose et al., Developing a Cybervetting Strategy for Law Enforcement (2010), http://www.iacpsocialmedia.org/Portals/1/documents/CybervettingReport.pdf. ["Developing a Cybervetting Strategy"].

Securities and Exchange Commission, Office of Compliance Inspections and Examinations, "National Exam Program Risk Alert, Cybersecurity Examinations" (April 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+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), http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf. ["Suitability and Security Clearance Report"].

(Footnotes)

1 All references to the "Common Sense Guide" in this section refer to the 4th edition of the publication.