Insider Threat Risk Assessment and Telework

Karen A. Toriello-Fite

Center for the Development of Security Excellence

ED-520: Foundations of Insider Threat Management

Thomas Gentle

1 April 2021

Summary

The COVID-19 pandemic has accelerated the shift to permanent telework across the U.S. workforce, necessitating a new framework for how companies conduct risk management. While many workplaces are increasingly remote-friendly, most organizations still use tools and techniques designed for an office-only environment. Toriello-Fite argues that perimeter-based solutions that focus on defending from the outside are no longer enough; to succeed, Insider Threat Programs and professionals must add technical and non-technical solutions that look at individuals and their behavior to provide context and to protect against data loss, system misuse, unauthorized disclosure of classified information, or kinetic violence from insiders. She provides a set of recommendations and resources to better mitigate risk in a remote work environment through increased training and education, the use of virtual applications and desktops, strengthened coordination between communications, security, and human resources teams, and the use of User Behavior Analytics (UBA).

Insider Threat Risk Assessment and Telework

The outbreak of COVID-19 led many businesses and government agencies to migrate a large portion of their workforce to remote work. In mid-March 2021, the Ford Motor Company told about 30,000 of its global employees who have worked from home during the past year that they can continue to do so indefinitely, only commuting to work for group meetings and projects that need face-to-face interaction. “Ford's announcement sent one of the clearest signals to date that the pandemic has hastened a cultural shift in Americans’ work lives by erasing any stigma around remote work and encouraging the adoption of technology that enables it.” (Rugaber, 2021)

Jed Kolko, chief economist at the employment website Indeed, said, “If job postings are a guide, employers are increasingly open to remote work, even as some employees return to the

workplace." A report posted by Indeed in March 2021 states that postings for jobs that mention "remote work" or "work from home" have more than doubled since the pandemic began, reaching 7% in February 2021, up from just below 3% a year ago. In some industries, the increase has been even greater—jobs for paralegals and legal assistants went from under 5% in the second half of 2019 to 16% in the second half of 2020; jobs for actuaries and loan underwriters went from 4% to nearly 16%; and for mental health therapists, they went from 1% to nearly 7%. (Rugaber, 2021)

Timothy Golden, a professor of management at Rensselaer Polytechnic Institute, stated, "The pandemic has broken the social and cultural norms for how we work. Remote work has become much more accepted." (Rugaber, 2021)

Based on all this, it seems remote work is here to stay. Additionally, Britain's National Computing Centre states that "individuals find it difficult to have a true boundary between work and home life and that they spend time sharing personal and business information on social networking sites with a "trusting innocence" (Mohamed, 2009) (Colwill, 2009). Risk management for insider threat needs to evolve to gain control over this new way of doing business.

What is Risk Management?

Looking in a standard dictionary, you will see risk management defined in many ways, but all hit the same basic points—evaluating the chance of loss or harm and then taking steps to avoid or minimize the potential risk. The National Institute of Standards and Technology (NIST) developed and published the Risk Management Framework (RMF) in 2010—it is a set of criteria

designed for federal organizations to use to help standardize the risk management process. Initially meant for cybersecurity within the government and government contractors, the RMF can be used in any arena—finance, business, government, or insider threat.

NIST's Risk Management Framework consists of seven steps. They are:

Step 1: Prepare. Essential activities to **prepare** the organization to manage security and privacy risks**.** The expected outcomes of this step are:

- to identify the key risk management roles,
- establish an organizational risk management strategy and determine your risk tolerance,
- perform an organization-wide risk assessment,
- develop and implement an organization-wide strategy for continuous monitoring, and
- identify common controls.

Step 2: Categorize. Categorize the system and information processed, stored, and transmitted based on an impact analysis. The purpose of this step is to determine the adverse impact of the loss of different types of information with respect to the loss of confidentiality, integrity, and availability of systems and the information processed, stored, and transmitted by those systems. The expected outcomes of this step are:

- to document system characteristics,
- to complete security categorization of the system and information, and
- to have the categorization decision reviewed/approved by an authorizing official.

Step 3: Select. **Select,** tailor, and document the controls needed to protect the system and the organization based on risk. The expected outcomes of this step are:

- to select and tailor the control baselines,
- to designate the controls as system-specific, hybrid, or common,
- to allocate the controls to specific system components,
- to develop a system-level continuous monitoring strategy, and to
- have the security and privacy plans that reflect the control selection, designation, and allocation reviewed and approved.

Step 4: Implement. Implement the controls in the security and privacy plans for the system and organization. The expected outcomes for this step are:

- to implement the controls specified in security and privacy plans, and
- ensure the security and privacy plans are updated to reflect which controls are implemented.

Step 5: Assess. Determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization. The expected outcomes for this step are:

- to select the assessor/assessment team,
- to develop security and privacy assessment plans,
- to review and approve the assessment plans,
- to ensure assessments are conducted in accordance with the assessment plans,
- to develop security and privacy assessment reports,

- to take remediation actions to address deficiencies in controls,
- to update security and privacy plans to reflect changes based on assessments and remediations, and
- to develop a plan of action and milestones.

Step 6: Authorize. A senior official makes a risk-based decision to **authorize** the system (to operate). The purpose of this step is to provide accountability by requiring a senior official to determine if the security and privacy risk is acceptable. The expected outcomes of this step are:

- to generate an authorization package (executive summary, system security and privacy plan, assessment report(s), plan of action, and milestones),
- to render a risk determination,
- to provide risk responses, and
- to approve or deny authorization for the system or common controls.

Step 7: Monitor. Continuously **monitor** control implementation and risks to the system. The purpose of this step is to maintain ongoing situational awareness about the security and privacy posture of the system and organization to support risk management decisions. The expected outcomes of this step are:

- to monitor the system or organization in accordance with the planned continuous monitoring strategy,
- to conduct ongoing assessments of effectiveness in accordance with the planned continuous monitoring strategy,
- to analyze and respond to the output of continuous monitoring activities,

- to ensure a process is in place to report security and privacy posture to management, and
- to conduct ongoing authorizations using results of the planned continuous monitoring activities. (Computer Security Resource Center, 2016)

How Do We Assess the Risk?

There are several types of risk assessments that can help to protect organizations against insider threats. These assessments are essential both for local and remote workers, but they become even more important as you migrate to a long-term remote workforce.

Vulnerability assessment

Organizations need to perform an assessment, or call in a third party to perform an assessment, to find policy, technical, process, and behavioral vulnerabilities. According to the Computer Emergency Response Team (CERT), a Division of the Software Engineering Institute at Carnegie Mellon University, a vulnerability assessment should include document and plan reviews, interviews with key personnel in the organization, and the observation of security processes. Identify any changes since your last assessment and see how they might have changed your vulnerabilities. Try to acknowledge your assumptions and biases and question them.

Access-Based Assessment

Organizations need to identify key processes, information, and assets that might have value to their adversaries. The next step is to map departments and users to assets in order to

determine who has access to what. The resulting list of potential insiders should be scrubbed to ensure that those individuals truly need access to those key assets. If so, increased monitoring might be called for; if not, remove access. For a technical countermeasure, you can use an Access-Based Group Access Control Model, which is similar to Role-Based Access Control (all system administrators) but adds in additional variables such as work hours (all system administrators who work 2300-0700) to assist in determining if users are accessing the system at what would be considered odd hours for them. (Bishop, 2010)

Single points of failure

Organizations can implement policies and procedures that ensure least privilege, separation of duties, and two-person approval for improved security and integrity.

Psychological Indicator-Based Assessment

While a person's medical or legal records are likely not going to be used due to privacy laws, you can still make use of a manager's or supervisor's assessment of an individual's state of mind. Additionally, you can paint a picture of the employee over time using performance reviews. Do comments about attitude, tardiness, or productivity seem to be showing up more frequently? What about complaints filed against employees? (Bishop, 2010)

What Are the Threats?

There are several types of insider threats:

Malicious Insider—an employee or contractor who knowingly looks to steal information or disrupt operations. This might be an employee looking for ways to steal information that they

can profit from, or someone who is disgruntled looking for ways to hurt or embarrass their organization.

Negligent Insider—an employee who does not follow proper IT procedures. This could be a user who leaves their workstation without logging out, or a system administrator who fails to change a default password or apply a security patch.

Compromised Insider—a common example is an employee whose computer has been infected with malware. Compromised insider's computers can be used as a jumping off point for cybercriminals. From here they escalate privileges, infect other systems, and more. There are several ways an employee can become a compromised insider:

- **Phishing**—a cybercrime in which a targeted individual is contacted via email or text message by someone posing as a legitimate institution in order to lure the individual into providing sensitive data, such as personally identifiable information (PII), banking and credit card details, and passwords. Some phishing schemes may also try to entice a target to click on a link that triggers a malware download.
- **Malware infection**—a cybercrime when a machine is infected with malicious software—malware—infiltrates your computer. The goal of the malware in the case of a compromised insider is to steal sensitive information or user credentials. A malware infection can be initiated by clicking on a link, downloading a file, or plugging in an infected USB, among other ways.
- **Credential theft**—a cybercrime aimed at stealing the username and password—the credentials—of a targeted individual. Credential theft can be done in a variety of ways. Phishing and malware infection, mentioned above, are common. Some criminals may engage in social engineering, which is the use of deception to

manipulate individuals into divulging their credentials. A bogus call from the IT helpdesk, where the user is asked by the attacker to confirm their username and password, is a common technique.

- **Pass-the-hash**—a more advanced form of credential theft where the hashed—encrypted or digested—authentication credential is intercepted from one computer and used to gain access to other computers on the network. A pass-the-hash attack is very similar in concept to a password theft attack, but it relies on stealing and reusing password hash values rather than the actual plain text password. (exabeam, 2018)

How Do We Detect the Threats?

There are many non-technical insider threat indicators, and knowing how to recognize them in your employees and co-workers is a big part of insider threat prevention. Examples include:

- Poor performance reviews
- Policy disagreements
- Displeased/disgruntled employees
- Financial distress
- Suspicious financial gain
- Odd working hours
- Unusual international travel
- Leaving the company
- Overly enthusiastic employees

There are many indicators that are specific to online behavior, as well. Some of them are:

- Badging into work at unusual times

- Logging in at unusual times
- Logging in from an unusual location
- Accessing systems/applications for the first time
- Copying or printing large amounts of information
- Anomalous Privilege Escalation/Creating new privileged or administrative accounts
- Rapid data encryption—rapid scanning, encryption, and deletion of large amounts of files can indicate a ransomware attack.
- Downloading sensitive files during irregular hours
- Sharing account credentials
- Installing unauthorized software
- Leaving credentials unprotected on notepad files
- Logging on from unusual endpoints—neither the regular office worksite nor the approved alternate worksite as identified in the telework agreement

How Do We Mitigate Risk?

Every organization is mobile now: whether it is employees working from home, third party contractors, or members performing temporary duty. As we collaborate remotely, through Microsoft TEAMS, e-mail, or other platforms, the danger of employees making security mistakes as well as malicious insider behavior are both raised. Traditional perimeter-based technical intrusion detection systems, as currently configured, do not provide the security organizations need. There are still many things an organization can do to combat insider threats.

Training and Education

In a traditional office-based workplace, employees learn how to detect concerning behaviors exhibited by co-workers and report it to HR or security, as well as prevent common social engineering attacks such as phishing.

In a remote workplace—in addition to conducting regular anti-social engineering training, such as sending phishing emails to employees and focusing training on those users who do not recognize the email as a phishing attempt—training should pivot to emphasize:

- Rules for accessing company information—Taking into account risks like fake hotspots, shoulder surfing, and website and IP address spoofing
- Handling corporate information outside the office—Printing, storing, and transferring data
- Safety and security of devices—personal and government-owned
- File sharing and transfer protocols—certificates, encryption, etc.

You must provide a readily available hotline for reporting suspicious activity. In addition, you can set up a monitoring framework for identifying the unusual or concerning behavior of individuals who access sites remotely. While you must grant privileges to employees so they can do their jobs, granting too many can backfire when users or system administrators abuse their privileges, either accidentally or on purpose. Therefore, it is necessary to find a happy medium. Baracoldo and Joshi, in their paper *An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats* propose "a framework that extends the role-based access control (RBAC) model by incorporating a risk assessment process and the trust the system has on its users. Their framework adapts to suspicious changes in users' behavior by removing privileges when users' trust falls below a certain threshold." (Baracaldo, 2013)

Insider threat programs require buy-in from employees. As part of the training and education program, employees also need to be made aware of the benefit an insider threat program provides for them, personally, not just for the organization. For example, data breaches can negatively affect your organization, but can also impact the employee through identity theft. Internalizing insider threat mitigation strategies because it helps *them* will bleed over to better security hygiene in the workplace. Let them know that they are trusted with the organization's valuable assets but that there is a need for controls because of the security risks. Being transparent allows you to inform employees clearly about:

- What behavior is monitored,
- What constitutes a security violation,
- What the result of a violation will be, and
- What an employee's privacy rights are and how they are respected.

This approach allows employees to make the right decisions and take responsible action with respect to their own behavior and the behavior of their colleagues. (Colwill, 2009)

Asset Holders

In the traditional workplace, the organization is the "asset holder" because they are in possession of equipment, infrastructure, and facilities.

In a remote workplace, insiders are the "asset holders." They possess personal and organizational devices, storage devices, cloud storage accounts, etc. Employees can work remotely and use multiple mechanisms for handling and storing assets. The risk model should include threats and vulnerabilities related to operations conducted with these assets outside the office environment.

Visibility

In traditional workplaces, visibility is often limited to organization-owned devices and actions that occur on organizational networks and physical facilities.

In remote workplaces, the organization must gain visibility over the movement, transmission, and storage of data. Virtual applications and desktops (VDIs) are growing in usage among organizations with remote workers. They were not, however, built with insider threats in mind. "The visibility provided by, for example, Citrix and VMWare VDIs doesn't help to detect data exfiltration and system misuse in real-time by insiders with legitimate access. Security teams must painstakingly piece together the user's identity and their actions with data activity and any application(s) in question from hard to understand VDI logs" (observeIT, 2021)**.**

Additionally, steps should be taken to identify concerning behaviors. Consider using open sources such as social media to gain insights into stressors or triggers that might result in an insider threat. Fortunately for us, we have the Insider Threat Hub that provides continuous evaluation of all workers (remote and traditional) as potential insider threats.

Protection

In traditional workplaces**,** the main priority is to protect and control equipment and people within the confines of the installation or facility. There are technical and non-technical means of providing perimeter security.

In a remote workplace, the traditional perimeter is gone; therefore, special pains must be taken to ensure the encryption of data in transit to prevent malicious insiders from accessing data that was not explicitly intended for them.

Coordinate Communications Security and Human Resources

This is applicable to both office and remote settings. Coordination between the communications and personnel departments can help ensure that employees who might be experiencing a stressor—such as receiving a poor evaluation or being fired—can have computer accesses curtailed, monitored, or removed and a preventive measure.

Employ User Behavioral Analytics

User Behavior Analytics (UBA), also called User and Entity Behavior Analytics (UEBA), is "the tracking, collecting, and analyzing of user and machine data to detect threats within an organization. Using various analytical techniques, UEBA determines anomalous from normal behaviors" (observeIT, 2021). In a nutshell, data is collected over a period of time to create a baseline of what "normal" user behavior looks like. The system then flags behavior that does not fit the pattern.

Summary

Most every workplace is remote friendly now, but we still use tools and techniques designed for an office-only environment. Perimeter-based solutions that focus on defending from the outside are no longer enough; we must add technical and non-technical solutions that look at individuals

and their behavior to provide context and to protect against data loss, system misuse, unauthorized disclosure of classified information, or kinetic violence from insiders.

References

Baracaldo, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security*, 237-254. Retrieved February 22, 2021, from https://www.sciencedirect.com/science/article/pii/S0167404813001119

Bishop, E. F. (2010). A Risk Management Approach to the "Insider Threat". *Insider Threats in Cyber Security*, 115-137. Retrieved February 22, 2021, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.224.7268&rep=rep1&type=pdf

Chinchani, I. N. (2005). Towards a Theory of Insider Threat Management. *International Conference on Dependable Systems and Networks.* Yokohama, Japan: IEEE. Retrieved February 22, 2021, from https://cse.buffalo.edu/caeiae/documents/pdf/dsn2005.pdf

Colwill, C. (2009). Human Factors in Information Security: The Insider Threat -- Who Can You Thrust These Days? *Information Security Technical Report*, 186-189. Retrieved Fefbruary 22, 2021, from https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/previous%20articles/ch11internalthreatsusers.pdf

Computer Security Resource Center. (2016, November 30). NIST Risk Management Framework. Gaithersburg, MD, USA. Retrieved March 16, 2021, from https://csrc.nist.gov/projects/risk-management/about-rmf

exabeam. (2018, May 7). *Security Operations Center.* Retrieved from exabeam: https://www.exabeam.com/security-operations-center/how-to-find-malicious-insiders-tackling-insider-threats-using-behavioral-indicators/

Hashim, A. Z. (2018). Risk Assessment Method for Insider Threats in Cyber Security: A Review. *International Jornal of Advanced Computer Science and Applications, 9*(11), 126-130. Retrieved February 22, 2021, from https://thesai.org/Downloads/Volume9No11/Paper_19-Risk_Assessment_Method_for_Insider_Threats.pdf

Kandias, S. B. (2013). Proactive Insider Threat Detection Through Social Media: The YouTube Case. *Proceedings of the 12th Association for Computing Machinery Workshop on Privacy in the Electronic Society.* Berlin, Germany: ACM. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.701.5768&rep=rep1&type=pdf

Kont, P. W. (2018). *Insider Threat Detection Study.* Tallinn, Estonia: NATO Cooeperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Maayan, G. (2020, November 30). *The State of Security.* Retrieved February 22, 2021, from tripwire.com: https://www.tripwire.com/state-of-security/featured/insider-threats-risk-assessment-considerations-for-remote-work/

Nostro, c. b. (2014). Insider Threat Assessment: a Model-Based Methodology. *Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing.* Braga, Prtugal: ACM. Retrieved from file:///C:/Users/101310~1/AppData/Local/Temp/Insider_Threat_Assessment_a_Model_Based-1.pdf

observeIT. (2021, March 16). *Securing the Remote Worker*. Retrieved from observeIT: https://www.observeit.com/solutions/securing-the-remote-worker-use-case/

Rugaber, T. a. (2021, 03 17). Will work from home outlast virus? Ford's move suggests yes. *Stars and Stripes*. Retrieved from https://www.stripes.com/will-work-from-home-outlast-virus-ford-s-move-suggests-yes-1.666113

Silowash, C. M. (2012). *Common Sense Guide to Mitigating Insider Threats 4th Edition.* Carnegie Mellon University. Pittsburgh: Software Engineering Institure. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA585500.pdf

The Ponemon Institute. (2019). *2019 State of Password and Authentication Security Behaviors.* Traverse City: The Ponemon Institute. Retrieved from https://pages.yubico.com/2019-password-and-authentication-report

The Ponemon Institute. (2020). *2020 Cost of Insider Threats: Global Report.* Traverse City: The Ponemon Institue. Retrieved from https://www.observeit.com/ponemon-report-2020-cost-of-insider-threats-global-cyberwire/

The Ponemon Institute. (2020). *2020 Global PKI and IoT Trends Study.* Traverse City: The Ponemon Intitute. Retrieved from https://info.entrust.com/rs/104-QOX-775/images/2020-Global-PKI-and-IoT-Trends-Study.pdf