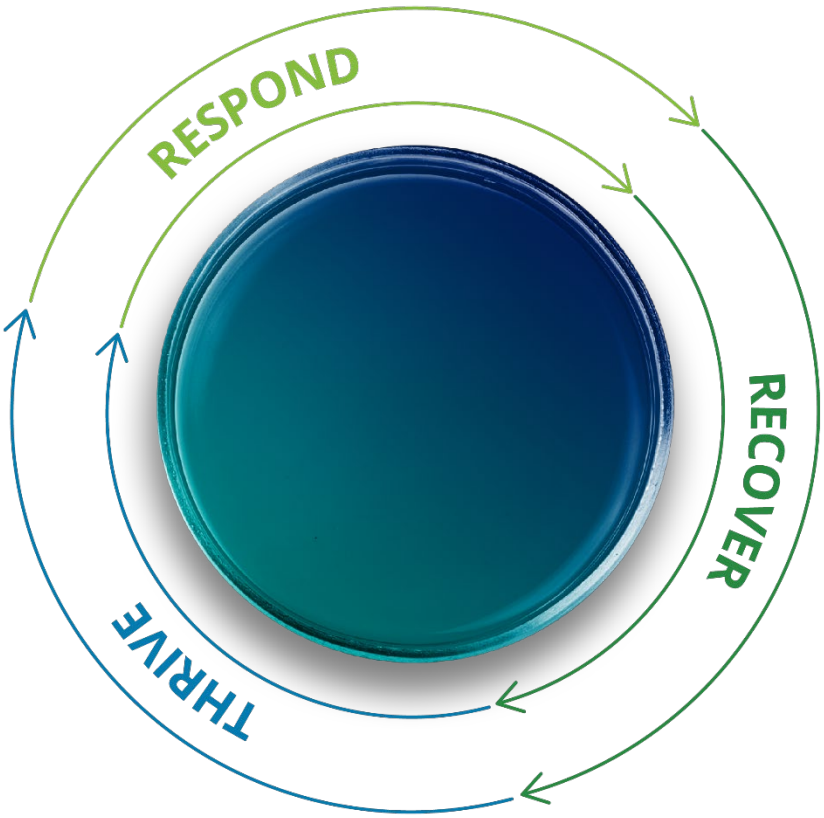
Deloitte.



New World, New Risks

Managing Potential Insider Threat During COVID-19

April 2020

Introduction

The COVID-19 pandemic has given organizations an entirely new and unfamiliar set of risks to manage. As those organizations balance protecting their workforce with keeping business running, they also cannot lose sight of protecting against familiar risks as well. Specifically, the pandemic may increase the risk negligent or malicious insiders may pose to critical assets and data. Compounded by immense economic uncertainty, the loss of critical assets, to include research and development, proprietary information, and critical materials can hinder an organization's recovery. Given this "new normal", there is value in proactively refining current approaches to better protect critical assets given emerging threats.

Fundamentals of Insider

People are any organization's most important asset, but people are also human. We all have emotions, stresses, and make mistakes. An insider threat occurs when those factors cause an employee, contractor, or vendor to either intentionally or unintentionally compromise valuable information, material, people or facilities.

While motives can vary from case to case, insider threats typically follow a discernible pattern of behavior that typically moves along a continuum of idea to action. As a result, behavioral factors that impact the idea of a threat or technical and organizational factors that impact the action can all increase the risk of an insider attack (See Figure 1).

As the world shifts from one of bricks and mortar to one of bits and bytes, organizations have become more proactive in preventing, detecting, and responding to potential insider threats. These mitigation measures are intended to disrupt the forward motion of asset exploitation, ranging from data exfiltration or system compromise to sabotage or even workplace violence. Now, as the world shifts once again, organizations must re-visit these controls and ensure that they are a good fit for how work is done today.

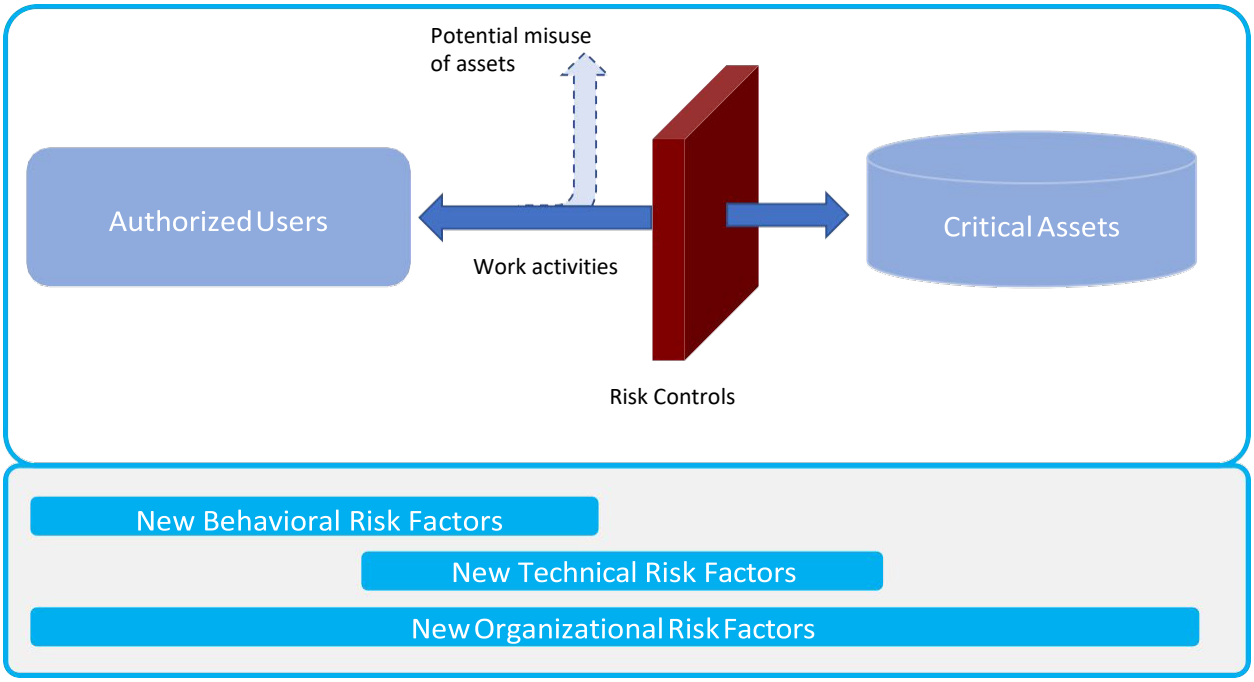


Figure 1: As the context of work shifts, new behavioral, technical, and organizational factors can increase the risk of insider threat

New Behavioral Risks

Unusual times can provoke unusual responses in people. So far organizations and workers have borne the challenges, but as the COVID-19 crisis stretches into weeks – if not months – employees' resiliency will be tested.[1] Prolonged stress may increase anxiety, impulsivity, impair judgment and lead people to become negative and distort/catastrophize their experiences. In any time of crisis, individuals can begin to feel desperate, resulting in behavior that departs from the norm, potential increasing risk of insider events.

For example, even in more conventional times, separations can often be a trigger for insider activity. Whether leaving voluntarily or involuntarily, employees who feel undervalued may seek to use sensitive data or assets for their own personal gain. As the financial impacts of the current crisis grow and more workers are laid off or furloughed, this area of risk only increases. Similarly, as the crisis constrains individual's finances either via lost income or through drop in economic markets impacting savings, retirement, and 401K accounts, compounding anxiety about financial security and sense of safety and stability for their families. For those hurting financially, normally unthinkable acts like fraud could begin to seem like viable lifeline.[2]

Potential Risks

- Resiliency for both employees, leaders, and organizations is challenged in periods of crisis, compromising optimism and future outlooks.
- Anxiety and stress may cause workers to pay less attention to security policy and practices. Working from home has different distractions than the office and may further exacerbate lapses in attention, leading to more unintentional incidents.
- During a crisis people tend to catastrophize their thinking into negative perspectives, resulting in a lost sense of optimism, lost balance to their emotions and potentially leading to more impulsive actions. In some cases, this may lead to intentional and malicious acts out of desperation for safety and security.
- A growing sense of panic amongst the workforce when realignment and furloughs occur. This panic can be fueled by rumors when there is limited information flow, leading to employees feeling disconnected.
- A higher volume of separations can cause lagging access (physical and virtual) leaving the organization exposed after the employee separates.

Potential Mitigation

- Develop new routines, help employees balance work with breaks to mitigate stress.
- Develop employee outreach programs that demonstrate understanding of concerns about job security, promotion impacts, and pay cuts.
- Coordinate with Human Resources to establish clear and consistent responses to employee fears, facilitate employee feedback on crisis response, and monitor concerning or malicious behavior.
- Disseminate informational updates integrated with Human Resources communications to mitigate the spread of misleading rumors about workforce reductions and other negative impacts.
- Share enhanced reminders and incentives about protection of proprietary information and increased monitoring of the virtual workforce.
- Be proactive in quickly removing access or company property from furloughed and/or terminated employees.

[1] Resilience is built by attitudes, behaviors and the use of social support. It is an inner strength that is helps people rebound in the face of adversity and see past the problem. It is enhanced through optimism, remaining balanced, managing strong emotions, and sustaining a sense of safety and social support.

[2] Eric Shaw and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." Center for the Study of Intelligence. Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015).

New Technical Risks

The onset of the COVID-19 virus has resulted in significant changes to the context or more specifically the way in which work is conducted. With States directing entire communities of non-essential workers to stay home, businesses have had to rapidly shift to a virtual work environment. While pre-existing insider threat programs designed to monitor employees remain a safeguard to critical assets, an entirely remote workforce presents entirely new risks.

Organizations have typically managed these risks by having a specific number of employees working virtually; however, in the wake of COVID-19 entire workforces have gone remote in a matter of days. The speed with which this occurred gave some organizations limited time to prepare and adapt current controls. Additionally, some of the technical controls that organizations typically have in place may have to be eased to allow for virtual work.

Potential Risks

- Employees trying to be as productive as possible might become lax in following security guidelines. Employees unfamiliar with remote work may be more likely to connect via an unsecure network, create work arounds to important controls, or click on phishing emails thereby introducing vulnerabilities to the system.
- Organizations' equipment is now in the home and not the office, allowing for potential use by others and lacking appropriate destruction mechanisms (e.g., shredders, burn bags).
- Employees may hoard information out of an unrealistic fear that the system will crash or use that as an excuse to collect information for future employment or actions against the organization.
- As employees shift to working remotely, many may be using personal devices versus company-issued equipment to access organizational networks and systems. The addition of new devices to an organization's environment increases the attack surface, providing cyber adversaries extended access to target and penetrate critical assets
- Remote work means a rise in the number of devices employees are using for their jobs, and an increase in the use of online conferencing tools. Without security controls in place, adversaries may be able to join meetings.
- There may be an increased likelihood of cybercriminals seeking stolen PII to make fraudulent claims, particularly related to stimulus funding, as the CARES Act.

Potential Mitigation

- Ensure employees are up to speed on basic security hygiene, including strong passwords and multifactor authentication (e.g., routine guidance on how to operate virtually, increase awareness of risk posed by COVID-19-themed phishing campaigns).
- Provide employees with guidance necessary to operate safely and be vigilant of potential mistakes that could lead to asset loss.
- Consider new technology tools to both increase authentication of users (e.g. multi-factor authentication) as well as detect and respond to malicious activity on the network.
- Be sure to assess security of collaboration tools as such tools become increasingly important to working with colleagues and customers alike.
- Develop and implement corporate security policies and guidelines for Bring Your Own Device (BYOD) to help ensure corporate security software is installed (e.g., VPNs are patched and up-to-date) on personal devices.
- Increase awareness among employees about the likelihood and dangers of COVID-19 phishing schemes. Organizations may consider an all-hands approach to incentive adherence to common cyber security protocols (e.g., communications to emphasize that the business will never ask for your password).
- Coordinate a cyber review to update data loss prevention (DLP), webfilters, proxy systems – new modules, rules and alerting. Consider increased or greater restrictions on privilege accounts and detection mechanisms to identify whether employees are using cloud applications to share/store sensitive information

New Organizational Risks

Every organization has its own risk tolerance, that is how it decides to balance security with the execution of business operations. Too much security can impede business, while too little can put critical assets in jeopardy.

The COVID-19 pandemic has caused many organizations to shift their risk tolerance almost overnight as they adapted to new ways in which work is conducted. However, it is critical that organizations do not let temporary measure become permanent defaults. Organizations should review their current level of risk tolerance regularly as the crisis evolves.

Potential Risks

- In a rush to be operational, organizations may be inclined to downgrade sensitivity levels (e.g., business confidential) and ease security controls to facilitate continuity of business.
- All industries may be at increased risk of fraudulent activity. Pre-crisis risk tolerance decisions likely do not fit the new normal. This isn't business as usual and the status quo will likely leave the organization with unmitigated risk.
- Organizations may relax their risk tolerance for third party vendors in order to bring vendors online quickly and minimize supply chain disruptions.
- Particular attention should be given to risk tolerance around cyber security controls. An account compromise may manifest as aninsider risk.

Potential Mitigation

- Revisit and refresh lists of critical assets and crown jewels given the new normal.
- Evaluate business processes based on the changes in work delivery. For example, organizations may need to evaluate policies to ensure employees can transfer and download necessary files.
- Continuously reevaluate the current circumstances of work to inform risk decision as the fluid situation of the pandemic response evolves.

Managing Risk, Staying Resilient

The COVID pandemic is causing the ground to shift under the feet of nearly every organization. In such difficult circumstances, the resilience of workers is shining through as organizations continue to operate as best they can. However, we are all human, and as the crisis drags on, uncertainty, new technologies, and changing circumstances can introduce risk even to the best prepared organizations. Timely steps to address those risks can help save significant disruption and loss of critical assets tomorrow, all while supporting the resilience of the workforce today.

For more information, please contact the Deloitte Insider Threat Team:

Mike Gelles
Managing Director
Deloitte Consulting LLP
mgelles@deloitte.com
+1 202 251 9615

Linda Walsh
Managing Director
Deloitte &Touche, LLP
lwalsh@deloitte.com
+1 973 255 9295

John Adams
Managing Director
Deloitte Consulting LLP
johnadams2@deloitte.com
+1 571 867 8344

Ken Croke
Specialist Leader
Deloitte Consulting LLP
kcroke@deloitte.com
+1 617 593 7479

Ben Sprague
Senior Manager
Deloitte Consulting LLP
benrsprague@deloitte.com
+1 571 814 6818

Elizabeth Burns
Manager
Deloitte Consulting LLP
eliburns@deloitte.com
+1 571 733 8967

Mark Freedman
Senior Consultant
Deloitte Consulting LLP
mfreedman@deloitte.com
+1 202 207 6097

Deloitte.