protiviti®
Face the Future with Confidence

Protecting your organization from insider threats in a changing world

Cybersecurity threats are growing exponentially as companies introduce an increasing number of Internet of Things (IoT) devices into operations and collect and store an ever-escalating amount of data. This technology and data sprawl is providing bad actors with more entry points into networks and systems. Too often, organizations have failed to make commensurate investments in data protection, even as mandates require companies to better safeguard sensitive data from ransomware, phishing campaigns and other cybercrimes. To be fair, rapid digital innovations in cloud computing, mobile devices, machine learning and other applications make it difficult for companies to keep pace with adequate security measures. As a result of these trends, annual global cybercrime damages are expected to reach $6 trillion in 2021.[1]

While most of the public reporting focuses on external breaches, insider threats pose as much of a security risk — if not more. An inside threat actor is someone who has privileged access to information technology systems and commits theft, fraud or sabotage, or who is careless in maintaining policies or practices aimed at preventing outsider access.[2] A well-known class of malevolent inside actors has long focused on disrupting software development to disable systems, embezzle funds and/or embarrass organizations. But in an operating environment dramatically altered by Covid-19, the insider threat has become even more acute. In particular, the transition to remote working, or "work from home" (WFH), has expanded the number of likely scenarios in which individuals may gain uncontrolled access to sensitive data.

Workers with authorized access to certain materials and assets commit the lion's share of insider damage, including the inappropriate use of data — whether

[1] Cybercrime Magazine, *Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021*, October 26, 2020.

[2] Cyber Infrastructure Security Agency, Insider Threat.

calculated or negligent — and the intentional theft of data and proprietary information. But former employees, vendors, business partners, contractors and others can pose as insiders, often by obtaining employee credentials, passwords or other privileged information. In fact, a 2018 Protiviti survey of 1,300 firms revealed that more than half viewed data sharing with partners and vendors as the primary source of their IT vulnerability.[3] Furloughs and jobs losses resulting from the pandemic, along with economic lockdowns, are only increasing insider threat concerns.

In an operating environment dramatically altered by Covid-19, the insider threat has become even more acute. In particular, the transition to remote working, or "work from home" (WFH), has expanded the number of likely scenarios in which individuals may gain uncontrolled access to sensitive data.

Threat impact

Regardless of an inside threat actor's status or motivation, the damage they inflict on companies can spill over into communities in the form of lost jobs and opportunities.[4] The threat can even affect entire industries and research efforts that lose an edge against overseas competitors.[5] To diminish the likelihood of these consequences, organizations need to manage a variety of insider threat impacts, including the following:

- **Fraud** — introducing bogus information into sensitive customer accounts or embezzling money
- **Data Exfiltration** — sharing proprietary or sensitive information with competitors or others outside of the organization
- **Privileged Misuse** — accessing and using information in violation of compliance, including sharing it with outsiders or non-authorized personnel
- **Denial of Service and Sabotage** — using technical methods to disable or disrupt normal business operations, including rendering a computer network unresponsive by flooding it with superfluous requests
- **Loss of Intellectual Property** — theft of proprietary information such as formulas, algorithms, blueprints, source code, and mergers and acquisition information

Addressing insider risk in the current climate

The growing sophistication of internal threats requires organizations to maintain constant vigilance on current insider threat dangers and those on the horizon, especially considering the disruptive operating environment introduced by the pandemic. Conducting thorough background checks during the hiring process, confirming that IT security protocols and access controls are addressed during the onboarding and offboarding processes, performing regular IT security awareness and training programs, ensuring the effectiveness of a third-party risk management platform, and continually assessing the risk environment are all critical controls that help thwart insider threats.

Still, those traditional controls by themselves fail to fully combat insider threats. Organizations need to adopt additional measures in the areas of data inventory and classification, data loss prevention across all platforms (phones, cloud, etc.), and remote working. Protecting an organization's "crown jewels" of information, for example, first requires collaboration between information security and business leaders to agree on what assets are most valuable relative to others to establish risk tolerance. Organizations must also determine where the assets are located, by what means and systems they are accessed, and who has access to them.

[3] ESI ThoughtLab, *The Cybersecurity Imperative*, October 16, 2018.

[4] National Insider Threat Task Force, *Protect Your Organization from the Inside Out: Government Best Practices*, 2016.

[5] Ibid.

The ability to control negligent and malicious behaviors presented a challenge prior to the wholesale shift to a WFH environment, and it has only become more formidable since. Internal threat assessment findings released in 2018 found that a vast number of employees were transferring data to unencrypted devices, expanding the potential for phishing attacks by accessing personal emails on company machines, opening up data to the public through the improper use of cloud applications, and using a VPN to conceal visits to inappropriate and risky gaming, gambling and pornography websites.[6]

Threat mitigation

To further buttress traditional controls in an effort to mitigate insider risk, organizations should consider implementing a two-pronged strategic approach focusing on technology and the organization. Here are some key takeaways that can help companies formulate and execute the strategy.

Protecting an organization's "crown jewels" of information first requires collaboration between information security and business leaders to agree on what assets are most valuable relative to others to establish risk tolerance. Organizations must also determine where the assets are located, by what means and systems they are accessed, and who has access to them.

Technology strategy

- **Identity and Access Management** — A failure to verify identities and control access renders virtually all other security measures useless. Organizations should consider multi-factor authentication (MFA) techniques, which can block 99.9 percent of attacks intended to compromise account security.
- **Data Loss Prevention** — Several tools can help address insider threats, including a security information and event management platform (SIEM), which collects and aggregates log data from other systems, and endpoint loss systems (DLP), which control access to certain files and file sharing.[7]
- **Enterprise Cloud Security** — Organizations are utilizing the cloud for a growing share of their computing needs, including software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) applications. But IT teams must have visibility over data and the ability to implement identity and control policies.[8,9]
- **Investigation and Response** — A decision tree or matrix can help companies decide when to intervene and halt an insider threat versus when to simply monitor the situation to learn more about the activity and identify other participants. But companies also need to determine whether the complexity or magnitude of the crime makes it appropriate to engage external investigators. Organizations can model how the incident progresses through the chain of management and predetermine their response to an individual's activity.
- **Monitoring** — In many cases, tools to detect abnormalities are already embedded in networks. Some SIEM vendors are incorporating user and entity behavior analytics (UEBA), which help to establish baseline behaviors and identify high-risk profiles, as well as activity, access and events associated with insider threats.[10] As discussed in a recent Protiviti blog, however, the WFH environment requires an adjustment of these baselines.

[6] Infosecurity, *Orgs Failing to Identify Insider Threat Blind Spots*, May 15, 2020.

[7] Cybersecurity Insiders, *2019 Insider Threat Solutions Guide*.

[8] McAfee, *What Is Cloud Security?*

[9] CSO, *Top cloud security controls you should be using*, October 21, 2019.

[10] Sirius Edge.

Organizational strategy

- **Threat Modeling** — Organizations should conduct threat modeling activities to identify, classify and prioritize threats and ensure effective documentation and reporting. These activities also can help the organization gain an understanding of how a technology interacts with external users and determine the threats, countermeasures and mitigations, and then rank those threats.[11] Organizations also need to leverage a structured asset management process to identify critical assets essential to maintaining operations and achieving the organization's mission. These can range from information about employees, contractors and vendors to buildings, vehicles and machinery.[12] Additionally, the model needs to consider separation of duties and least-privilege concepts to ensure, where feasible, users and system services are granted the minimum access rights necessary to complete assigned tasks.
- **Awareness** — People are the best mechanisms to sound an alert about insider threats, and linking security awareness training to employee monitoring can help build transparency and trust.[13] An untrained staff is the single largest cybersecurity threat because they are easy marks for phishing and other targeted attacks.
- **Stakeholder Communication** — Validating threat models and potential insider threats with stakeholders can ensure IT risk mitigation efforts continue to evolve to meet new challenges.
- **Multi-Disciplinary Approach** — A comprehensive approach to thwart insider threats should go beyond an organization's IT security apparatus and include other business functions, including governance personnel and committees, and the internal audit, compliance and risk management departments, to name a few.

Next steps

Organizations interested in refining or strengthening their insider threat programs should first review the appropriateness and effectiveness of what is in place today and determine how well the program aligns with standards for an insider threat program. How effectively does the program detect, deter and respond to malicious insiders versus those that are simply negligent or mistake prone? Is the current program the right fit for the company's budget, size, culture and industry? How appropriate are the current insider threat mitigation strategies for remote working or cloud-first infrastructure environments? How would efforts to close identified gaps affect culture or other intangibles? A good source of information on standards is the Common Sense Guide to Mitigating Insider Threats, a treatise on the subject published by Carnegie Mellon University's CERT Insider Threat Center. Once areas that need improvement have been determined, organizations should update and refine their insider threat programs to close any identified gaps in a manner consistent with the organization's risk tolerance and culture.

How Protiviti can help

Protiviti works with organizations to focus on foundational information security questions:

- Do we know what we need to protect (e.g., the data and information systems assets that are most important — the "crown jewels"), and where those assets are located? Are we properly caring for them? How do we know? Who are we protecting them from, and are our defenses working as intended? Whom should we permit access, and how can we tell the difference between authorized users and inside threat actors? How will we know if things are not working as we planned?
- Are we able to recognize a new insider threat to our environment and detect likely attack techniques on a timely basis? Are we able to align our protection measures to meet the threat?
- If or when incidents occur, are we ready to respond appropriately? Can we manage those incidents and keep them from happening again?

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation, and management services to help organizations

[11] CSO, *Threat modeling explained: A process for anticipating cyber attacks*, April 15, 2020.

[12] Cyber Infrastructure Security Agency, *Protect The Organization's Critical Assets*.

[13] Sirius Edge.

identify and address security and privacy exposures (e.g., misappropriate use of data by authorized users, theft or loss of critical data, threats from external attackers, loss of revenue or reputation impairment) before they become problems. Working with companies in all industries, we evaluate the maturity of their insider threat security programs and the efficacy of their controls — and help them design and build improvements when needed. We have a demonstrated track record of helping companies react to security incidents, establish proactive security programs, deal with identity and access management, and handle industry-specific data security and privacy issues. Our experience and dedication to developing world-class incident responses have resulted in deep expertise in security strategies, response execution, forensic analysis and response plan development.

Contacts

Joel Hammer
+1.206.262.2935
joel.hammer@protiviti.com

John Stevenson
+1.469.374.2410
john.stevenson@protiviti.com

Thomas Moon
+1.206.262.2929
thomas.moon@protiviti.com