Protecting Information Assets against Insider Threats

By T. Sean Kelly and Andrew Shaxted

This article will discuss the landscape of insider threats and steps organizations can take to protect their critical information assets against them. It will cover new data privacy considerations, tactical steps that can be implemented, and how corporate IT and security teams can work across departments to ensure a cohesive, executable program.

For many years, businesses have understood that personal data is an asset that holds (and creates) value. This belief is so commonplace that recently Gartner predicted that by 2021, companies would be valued on their information portfolios,[1] a trend also hinted at in certain recent M&A activity. Even without an information portfolio valuation, corporations are increasingly seeking to collect consumer and workforce personal data to generate insights and drive strategy. With corporate collection, use, and storage of personal data on the rise, managing personal data like any other prized asset on the books is critical.

A survey of cybersecurity professionals found that 42 percent believe insider attacks or breaches are the most damaging type of threat to the organization.[2] It makes sense then that prioritizing the insider threat in data protection initiatives can have the most meaningful direct and indirect results in mitigating data-related risk.

The insider threat landscape

While some paint the picture of the insider threat as a malicious actor seeking to intentionally destroy from within, this understanding reduces the issue. Is a poorly trained employee with access to the company's most critical personal data assets an insider threat? Yes. Is a well-meaning contractor that uses an unauthorized, unpatched device to access the corporate network an insider threat? Yes. The examples are endless, but the point is that the most impactful threats to corporate personal data can exist without intent.

Ultimately, the insider threat is a person with access to internal systems or information that intentionally or unintentionally uses that access to cause harm.

Unintentional actors and the threats they pose can include the following:

- **Untrained, poorly trained, or distracted employees:** Any person within the company who handles personal data contrary to standard operating procedures creates security control gaps. This can easily happen even among trained but distracted employees. A common scenario that falls into this category is an employee who accidentally sends an email containing personal data to an unintended recipient.
- **Unvetted or loosely managed contractors:** Where contractors are not included in the typical HR "hire-to-fire" business processes, it is impossible to ensure zero data leakage. Contractors are a common insider threat vector, who may often evade company device policies, system deprovisioning processes, and background check procedures.

Intentional actors and the threats they pose can include:

- **Disgruntled or departing employees:** Osterman Research[3] reported that "69 percent of organizations polled say that they have suffered significant data or knowledge loss resulting from employees who took information resourc-

[1] Gartner, "Gartner Says Within Five Years, Organizations Will Be Valued on Their Information Portfolios," Gartner (February 8, 2017) – https://www.gartner.com/en/newsroom/press-releases/2017-02-08-gartner-says-within-five-years-organizations-will-be-valued-on-their-information-portfolios.

[2] Cybersecurity Insiders, "Insider Threat 2018 Report," CA Technologies – https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf.

[3] Andy Patrizio, "Sensitive Data Often Follows Former Employees out the Door," CIO (APRIL 27, 2017) – https://www.cio.com/article/3192842/security/sensitive-data-often-follows-former-employees-out-the-door.html.

es with them when they left the business.” The failure to deprovision system access from a terminated employee in a timely manner presents countless opportunities for unauthorized access and possible breach.

- **Extorted employees:** Employee extortion, which may lead to compromised access, is on the rise as well. The FBI has been vocal about an increase in employee extortion.[4] While difficult to combat, it is important for information security and privacy teams to be aware of this trend, as the extortion of just one insider can leave holes in the organization’s security environment.

A recent Ponemon study cited the current average cost of an insider threat at $8.7 million.[5] The damage to customer trust, shareholder value, and business viability that can result from such an event can be equally destructive regardless of the insider’s intent.

Acknowledging vulnerability

In the 2018 Insider Threat Report[6] from Cybersecurity Insiders, nearly all organizations surveyed said they feel vulnerable to insider attacks, and 53 percent confirmed their organization had fallen victim to an insider attack in the last 12 months. Others said insider attacks have increased in frequency in recent years. Respondents in the study indicated several primary enabling risk factors, including “too many users with excessive access privileges, an increasing number of devices with access to sensitive data, and the increasing complexity of information technology.”

In parallel, new regulations like the General Data Protection Regulation (GDPR),[7] NY Department of Financial Services (NYDFS) Cybersecurity Regulation,[8] the California Consumer Protection Act of 2018 (CCPA),[9] and other state-based laws[10] are introducing heavy enforcement over companies handling of personal data.

Corporate stakeholders must determine how to implement proper information security controls that adequately protect personal data as well as enable business operations and innovation. Doing so requires a corporation to tackle information governance (IG) that encompasses clear, attainable, and robust programs and policies that protect data.

Endpoint data loss prevention (DLP) technology that automatically tracks, controls, detects, and/or blocks potentially harmful activity happening inside the network is one tool that can make a meaningful impact on operationalizing IG policies and keeping sensitive data inside the organization. Mobile device management tools are similarly useful and allow IT security teams to manage and control company-owned and employee-owned devices. They provide the ability to block access or wipe information if an insider risk associated with a device arises. Employee monitoring tools, while controversial from a privacy standpoint, are another category of technology that can be leveraged to detect and thwart suspicious insider activity. An increasing number of organizations are using various types of monitoring tools in

[4] “FBI Issues Warning after Extortion Schemes Surface Following Spate of Mega Breaches,” Trend Micro (June 03, 2016) – https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/fbi-warning-after-extortion-schemes-surface-following-mega-breaches.

[5] “2018 Cost of Insider Threats: Global,” Ponemon Institute LLC (April 2018) – https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2018/04/ObserveIT-Insider-Threat-Global-Report-FINAL.pdf.

[6] Cybersecurity Insiders, “Insider Threat 2018 Report,” CA Technologies.

[7] “The EU General Data Protection Regulation (GDPR) Is the Most Important Change in Data Privacy Regulation in 20 years,” EU GDPR.org – https://eugdpr.org/.

[8] “Cybersecurity Resource Center,” New York State Department of Financial Services – https://www.dfs.ny.gov/industry_guidance/cybersecurity.

[9] Rita Heimes, “Top 5 Operational Impacts of the CCPA: Part 1 — Determining If You’re a Business Collecting or Selling Consumers’ Personal Information,” International Association of Privacy Professionals (Jul 23, 2018) – https://iapp.org/news/a/top-five-operational-impacts-of-cacpa-part-1-determining-if-youre-a-business-collecting-or-selling-consumers-personal-information/.

[10] “Data Security Laws | Private Sector,” National Conference of State Legislatures (1/4/2019) – http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

the workplace, some of which can be extremely effective in protecting the loss of sensitive information.

Arming against insiders

Below, we will further discuss the ways organizations can prevent loss of sensitive data, and how holistic information governance can help. Education is the most powerful weapon in battling insider threats, with employees serving as a first line of defense. Staff should be trained on how to handle sensitive data and how to prevent inadvertent data leakage, and be incentivized to uphold company policy. When the entire workforce understands the many ways critical information can leak from the organization, and the extent of damages such a breach can cause, they are in a much stronger position to maintain and reinforce existing data protection programs. In addition to education, organizations can take additional tactical steps to protect themselves against insider threats.

Identify and protect sources and stores of sensitive data

As part of sound information governance, every organization should have a detailed map of its data universe, accounting for the entire scope of where sensitive information originates, flows, and is stored. This will inform which areas should be prioritized as new programs are rolled out, so they are applied to the most sensitive pools of data first and foremost.

With the data map as a guide, the team can also begin to audit and analyze where vulnerabilities exist, or where best practice protections such as encryption and access controls are lacking. Surprisingly, encryption, which is an effective and straightforward way to protect critical data, is still not used as broadly or formally as it should be within most enterprises. One study by Ponemon found that nearly 60 percent of enterprises do not have a consistent encryption strategy, and 37 percent turn over control of keys and encryption processes to cloud providers.[11] This is a stark reminder that most organizations today still have gaps in meeting baseline standards for information security and are leaving themselves open to unnecessary risk as a result.

Enhance identity access management integration with HR process

Cutting down on insider threats should start by limiting personal data access to the right people, at the right time, for the right reasons. The strongest identity access management (IAM) controls are coordinated with HR systems and processes. Information security systems (e.g., Active Directories and privileged access management systems) should integrate with the organization's human resource information system (HRIS) and track the worker's full hire-to-fire process (hire, promotion, role change, etc.). Automating and monitoring the process to the extent possible is critical.

Integrate contractors and third-party vendors into the control environment

Contractor onboarding should follow a similar onboarding process to that of employees, and in many cases should incorporate even more stringent access limitations. Similarly, organizations face challenges when attempting to integrate privacy and security controls into their vendor risk management programs. Ultimately, these programs should have the ability to assess, mitigate, monitor, and enhance vendor security control environments to the same extent it can its own.

Balance collaboration platform capabilities with data protection controls

Increased adoption of collaboration platforms such as Microsoft Teams, Slack, Skype, etc. adds complexity to centralized

[11] Jeff Goldman, "Just 41 Percent of Enterprises Have a Consistent Encryption Strategy," eSecurityPlanet (April 18, 2017) – https://www.esecurityplanet.com/network-security/41-percent-of-enterprises-have-a-consistent-encryption-strategy.html.

access management capabilities. Further, these communication apps serve as additional channels of data removal for any insider with access if not properly controlled. The intended functionality of the tools should be balanced against data privacy and protection requirements in an appropriate use policy. A first step is to provide a framework for how, when, and with whom employees can communicate. Then, the technical controls that limit use in accordance with the policy can be established.

Improved API development oversight

The advent of the open API environment has brought with it immense innovation, but also significant risk. Platforms, and the developers behind them, are more equipped than ever to transmit and ingest massive amounts of personal data. Without proper software development life cycle (SDLC) and oversight, developers may inadvertently or intentionally embed code that exposes personal data to third parties. IT security leaders must ensure that development teams have proper SDLC training to prevent accidental exposure. Further, data loss prevention principles should be incorporated into code review before new software is launched.

"Just in time" and periodic security assessments

Every organization should include insider threats in the broader inventory of risks it evaluates on both a periodic basis and on a "just in time" basis (where new information is discovered). Often, IT will deploy or provision access based on existing settings or user groups in other applications. While this may be the most direct and fastest option for launching a new application, it risks giving access to groups that don't need it, and therefore creating a potential threat where there doesn't need to be one. Instead, new network applications and systems should undergo a standardized and rigorous security assessment. As part of that assessment, IT must customize access for each new system individually, and keep that access updated on a regular basis to ensure proper limitations.

Conclusion

The intersection of data privacy risk and insider threat provides corporations with a prime opportunity to strengthen their data governance and security programs. Stakeholders can work hand-in-glove to protect against insider threats and reduce the risk of data loss while simultaneously improving data protection and streamlining processes. Doing so before the organization finds itself the subject of negative news headlines will help reduce costs and risks. This type of proactive approach helps lay a much stronger foundation for a long-term culture and reputation of trust.

About the Authors

T. Sean Kelly is a Senior Director at FTI Consulting and is based in Philadelphia. As a senior member of the information governance, privacy and security practice of FTI Technology, Mr. Kelly leverages more than a decade of experience to advise clients on all aspects of information life cycle management. He may be reached at sean.kelly@fticonsulting.com.

Andrew Shaxted is a Senior Director in FTI Technology's information governance, privacy and security practice, and is based in Chicago. He is a licensed attorney and global data privacy and infosec consultant with a background in technology and global risk management program implementation. He may be reached at andrew.shaxted@fticonsulting.com.