Lexmark

Insider Threat—Securing the Human Layer of the OSI Stack

Insider Threat—Securing the Human Layer of the OSI Stack

> *"Regardless of the technology in place to protect data, people still represent the biggest threat."*[1]
>
> **Alex Ryskin**
> IT director for the laser laboratories at the University of Rochester, NY

In *Superman 3*, Richard Pryor's character (Gus Gorman) devises a scheme to skim money from accounts by "penny shaving" or "salami slicing." Gorman defies street wisdom regarding how to go undetected by not showing unusual behavior—like roaring into the employee parking lot in a shiny, new, bright-red sports car.

Often, behavior associated with insider threat is more subtle, although the aberrant behavioral changes of US spies Aldrich Ames and Robert Hanssen indicate the possibility of seemingly obvious misses. These obvious signs that pointed to Ames as a double-agent included $33,500 in credit card debt (motivation), physical security violations (attitude) and living beyond his $70,000 salary (cash purchase of his $540,000 home and a $50,000 Jaguar)—all clues of a secondary income. Hanssen also violated acceptable use policies, had infidelity and financial problems, did not follow CIA procedural guidelines, and was never subjected to a polygraph test. Ames' treasonous activities earned him $2.7 million over four years and Hanssen's earned him $1.4 million. Their activities also cost lives.

These examples illustrate that even the most trusted of insiders are capable of behavior that is contrary to policy set forth by their organizations, and that this often begins with small changes in normal behavior that begin a "slippery slope" into major violations which harm an organization, its reputation, and those associated with it. These examples also serve to demonstrate that the smallest to largest red flags often go unchecked or unnoticed by organizations until it is too late.

Both public and private sector organizations are subject to insider attacks. In fact, some have suggested that the OSI model, a widely accepted seven-layer representation of computing system services (physical, data, network, transport, session, presentation, application), be expanded to include a "user" layer. As computing practices have evolved, the end user influences how applications and data are used and accessed, effectively designing technology scenarios that programmers had not anticipated. In an effort to start modeling and understanding indicative or precursor behavior, Carnegie Mellon University's CERT division, supported by the United States Department of Defense, has researched and mapped insider threat activity since 2001. In their most recent edition of the *Common Sense Guide to Mitigating Insider Threat*, they found the following:

Insider threat landscape—Carnegie Mellon Findings[2]

- 23% of electronic crime events sampled were suspected or known to be caused by insiders.
- 45% of survey respondents felt that damage caused by an insider breach were more severe than similar attacks by an outsider.
- Of 1,000 sample insider threat cases, 734 were attributed to an intentional or malicious user.
- Insider threat events have become increasingly pervasive, originating from employees of all technical skill levels, age ranges, and income levels.
- As more companies gravitate toward a mobile workforce, incidents of insider data loss via remote connections or off-network machines will increase.
- Over half of insider sabotage cases stemmed from a privileged account holder.

These results validate the use of behavioral and event analysis to develop probability profiles for insiders. One of the challenges historically has been triaging high-probability insider threats: the employees who are at risk of contributing to the compromise of an organization's information. This challenge is exacerbated by the extraordinary amount of information that passes through enterprise servers, the proliferation of computing devices and fewer face-to-face encounters between security management and staff due, in part, to remote and flex-time work options.

Insider risks

The risk that insider threat poses to organizations is both direct and indirect. Fraud, embezzling, workplace violence and illicit release of company-proprietary or entrusted, confidential information result directly from inappropriate inside actions, whether performed through malice, ignorance or oversight. Indirectly, insiders pose a threat to an organization through organizational liability (due to data breach or non-compliance with prevailing laws or regulations), reputational loss, and damaged productivity.

Data Breach

In today's world, our access to data is no longer on an as-needed basis, having transformed to an always-on, always-connected atmosphere. Business factors such as ever-present smart devices, reliance on transient laptops rather than network-bound desktops, and the growing remote workforce have changed the way data breaches take place. Intel's 2016 "Grand Theft Data" report informs us that today close to half of data breach events are perpetrated by the insider rather than an external actor. Of these, internal data breaches are split equally between the malicious, or intentional, theft of data and the accidental breach, often occurring due to human error or a lack of knowledge of proper security practices. Most organizations find these attacks, while accounting for only a portion of data risk, to be more challenging as abnormal access and usage patterns from specific individuals can be difficult or impossible to track using traditional security tools.

Paper: A forgotten vulnerability

When it comes to protecting sensitive information from insider threats, many organizations think first about securing their digital systems and channels—their networks, servers and web-based sources. But leaving the hardcopy portion of your data out of your security strategy can be a costly mistake. In fact, 61 percent of large enterprises admitted suffering at least one data breach through insecure printing.*

*Quocirca 2017 Report, *Print security: An imperative of the IoT era*

Abuse of Privileged Information

As the obvious target for financial predators ("because that's where the money is"), the financial industry has set the standard for conscientious implementation of information security standards and ranks consistently high in budgeted investment in security. And yet, a secure perimeter does not assure security in the vault. Security practices internally may be lax. There may be bad actors within the organization's trusted community who have accumulated the privileges or knowledge required to subvert safeguards. In fact, 66% of IT security professionals themselves admit to deliberately seeking out or accessing company data unnecessary to their work.

Segregation of duties, for example, is a key mechanism for preventing privilege abuses, especially the escalation of privileges, by reducing opportunities for collusion or for conflict of interest among employees. On a policy level, segregation of duties guards against situations in which the right hand knows entirely too much about what the left hand is doing.

However, Jerome Kerviel's personal memory was not degaussed after changing work assignments. He became a trader at Societe Generale after working as a subject matter expert with its back office system for booking transactions (a system known as Eliot). His intimate knowledge of when Eliot scheduled the nightly reconciliation of the day's trades allowed him to hide his unauthorized transactions by deleting and re-entering them. He successfully posted trades that eventually grew to more than $70 billion in "problem investments" (AKA, losses) for Societe Generale. Although his system activity was inappropriate, no protective measures were in place to detect the precursor behavior. This is a situation that could have been prevented had Societe Generale deployed an intuitive system for aggregating an individual's system activities for analysis with respect to data in process.

Accidental Release of Entrusted, Third-Party PII

The weightier enforcement provisions of the 2009 HITECH Act have encouraged medical facilities to take HIPAA restraints more seriously. The US Department of Health and Human Services (HHS) oversight power includes fines for those facilities whose practices do not comply with the increasingly rigid standards for protecting confidential information. HHS levied a $4.3 million fine against Maryland-based Cignet Health in February 2011 (the first fine levied since HIPAA's 1996 passage),[3] $1.5 million against Blue Cross Blue Shield of Tennessee in March 2012 and $1.7 million against the Alaska Department of Health and Social Services in June 2012.[4] Other fines have also been levied, including fines against smaller medical practices and clinics. The advent of universal electronic health records makes it even more imperative that medical facilities protect the information under their custody—and know what and where that information is.

The Federal government could also benefit from a higher level of information situational awareness. A study released by Rapid7 in September 2012 estimated that the federal government unintentionally exposed approximately 94 million records containing citizen personally identifiable information (PII) between January 2009 and May 2012.[5] The estimate is based on breaches reported to the Privacy Clearinghouse. The majority of those records (76 million) were compromised when a hard drive containing VA medical information was not properly protected. Continuing years later,

MFPs and insider threat

In today's digital world, most security efforts are focused on preventing external threats. But what about the malicious and non-malicious breaches that are occurring internally? As information is shared and accessed across a growing number of sources, the potential for insider threat is growing in size, scope and complexity.

That risk is especially present when it comes to your hardcopy information—those documents that are accessed, shared or received from multifunction printers (MFPs).

even after weathering some of the most notorious of insider breaches by PFC Manning and Edward Snowden, the NSA has still failed to "fully implement technology to oversee privileged user activities; effectively reduce the number of privileged access users; and effectively reduce the number of authorized data transfer agents."[6]

Acts of Vengeance

In the physical world, attacks against one's employer may be called "going postal," a nickname that emerged from a series of twenty-some incidents between 1986 and 1997 in which various United States Postal Service individuals engaged in shooting sprees. More than 40 people were gunned down. The parallel in the cyber world is the kind of havoc wreaked by a disgruntled employee who decides to sabotage internal control systems. In addition to high-profile cases involving irregularities perpetuated by insiders in the financial industry (e.g., the aforementioned Societe Generale case), there are also well-publicized examples within numerous industries, large and small:

- A lone water treatment plant employee allegedly manually shut down operating systems at a wastewater utility in Mesa, Arizona in an attempt to cause a sewage backup to damage equipment and create a buildup of methane gas. Automatic safety features prevented the methane buildup and alerted authorities, who apprehended the employee without incident.
- A recently fired employee from a US natural gas company allegedly broke into a monitoring station of his ex-employer and manually closed a valve, disrupting gas service to nearly 3,000 customers for an hour.
- The Arkansas Department of Medicaid discovered a breach of 26,000 medical records including medical details and PII when an employee emailed the data to her personal account within minutes of a disciplinary discussion.
- A Premier America Credit Union Employee emailed an undisclosed number of customer records, including customer PII, social security numbers, passwords, and more, to his personal email address before departing the company.
- A contract software developer was terminated due to poor performance by an unnamed organization. Over a period of the next month, he was able to access 16 of his former co-worker's systems and a total of 24 user accounts, read secure emails, copy source code from his previous project, and deleted two modifications to the project.
- A US citizen who was arrested in Yemen in a March 2010 roundup of suspected al-Qaeda members worked for several contractors performing non-sensitive maintenance at five different US nuclear power plants from 2002 to 2008. This individual was able to pass federal background checks, as recently as 2008, before becoming a contracted employee.[7]

In each of these cases, a trusted staff member was directly or indirectly implicated in acts with negative consequences for his or her employer and for the communities dependent on that employer's utility services. Policies were ignored that would have checked such activity. A tool based on sophisticated behavior analysis and modeling could have alerted management to proactive measures.

Advanced hardcopy monitoring

Lexmark Secure Document Monitor (LSDM) lets you seamlessly monitor hardcopy data with the increased visibility that makes it possible to investigate, protect and prevent costly breaches.

You can install LSDM on your Lexmark MFPs to monitor hardcopy documents directly from their point of origination. LSDM technology automatically captures the content of every document that passes through a device, and routes it to a data loss prevention (DLP) provider for review.

LSDM can help you fill in the gap of hardcopy security with technology that's discreet, automated and connected to your existing systems.

Compliance and Audit Failures

Regulatory complexity continues to increase for many organizations. A look at the record for the payment card industry (PCI) illustrates the difficulty that organizations experience in meeting—and maintaining—regulatory compliance objectives. The 2016 Verizon Business Payment Card Industry (PCI) Compliance Report showed only about half (55.4%) of reported organizations passed PCI validation. However, many of these organizations struggle to maintain these compliance goals, most falling back out of compliance within a year. Aside from the obvious financial consequences of audit failures, the resulting data breaches resulting from unsecured financial and payment card data could cause monumental damages to organizations that fail to proactively track compliance initiatives.

Lost Productivity

When discussing employee theft, rarely is productivity or time management taken into account. Many managers don't like to point fingers, but taking one look at the balance sheet gives us shocking results. CareerBuilder's employee productivity study quickly gets to the root of the issue: personal devices and internet surfing.[8] According to their results, 24% of workers admit to spending an hour per day on personal calls, emails, and texts, while 21% estimate they spend at least an hour on non-work-related web viewing. Chances are, those results are highly conservative, especially as our smartphones increase in speed and functionality by the day. These statistics are echoed by findings from Gallup, Gartner and others that state disengaged staff spend at least an hour a day on non-work-related Internet activities. According to Gallup's State of the American Workforce report, put "bluntly, many employees feel indifferent

Insider threat protection from Lexmark and IID

Hardcopy data is only a portion of the information you need to collect and monitor in order to have full visibility and true insider threat protection. For maximum ease and efficiency, it's important to be able to connect that hardcopy information with the digital data you're monitoring.

Lexmark teamed up with Intelligent ID (IID) to create an end-to-end solution for complete insider threat protection. It provides all the capabilities you need to capture and view all user and document data—both paper and digital—from one place, for a more complete picture and increased protection.

Here's how LSDM with Endpoint ID puts everything you need to investigate potential threats at your fingertips:

1. **Capture** an image of every document
2. **Route** captured images to a single, unified monitoring dashboard
3. **Monitor** data usage and employee behavior for potential patterns, issues and threats
4. **Investigate** possible threats with pre-configured rules and searches, and build cases as evidence is collected
5. **Prevent** security breaches by uncovering potential threats and taking appropriate action

By leveraging the capabilities of Lexmark Secure Document Monitor (LSDM) and IID's Endpoint ID, you'll have greater visibility and in-depth insight to monitor threats and vulnerabilities.

about their jobs," with only 33% of employees feeling engaged at work and 51% actively watching for new jobs.[9] Stepping back to Careerbuilder's productivity statistics and doing some basic estimations, we can safely say that in a 1,000-person company with employees making an average of $15 per hour, $1,761,750 would be lost a year in employee "browsing" time. Suddenly it becomes apparent why rogue employees, bored workers, and detached contractors can easily rack up millions of dollars in theft of resources.

Information Ownership

As we investigate and analyze insider threat trends, we should also ask ourselves what happens when the perpetrator of insider theft does not realize that theft has taken place. Technology and portability of data evolves daily and, with it, so have the attitudes on information ownership by employees. While conventional wisdom states that materials created on behalf of an employer belong to that employer, many employees are no longer sharing that viewpoint. Today, over 31% of employees work from home 4-5 days a week and, therefore, are creating their data on a combination of employer-owned and personally-owned devices.[10] Once this data is created, there is typically no guarantees that the information resides solely on the employer's network and devices. In an eye-opening study by Symantec, it is revealed that 2 out of 5 employees regularly download work files to a personally owned tablet or smartphone and most employees regularly take company IP outside of the organization, but never clean it up. Most startlingly, half of employees who left or lost their jobs admitted to keeping confidential data and 40% intend on using this information in their new positions. Overall when surveyed, 56% of employees do not believe it is a crime to use a competitor's trade secrets.[11] It's easy to see how today's era of information mobility and data sharing has substantially blurred the lines of ownership in the minds of many employees.

Current approaches and limitations

Recommendations abound about how to address the challenges of containing and managing insider threat. Many are highly resource-intensive and so less likely to be implemented consistently and in a manner that is legally defensible.

Business Challenges

A large part of the challenge in securing vulnerable human factors is the frequent disconnect between the HR and IT or IT Security management teams. Tools used for monitoring network, file system and applications activities typically deliver too much data and too little analysis for HR professionals. These HR professionals need to understand what to look for when working with, training, and in disciplinary intervention with employees, including contextual information as well as contributing factors. Another challenge is when an insider or partner creates a hole or vulnerability, setting up a necessary precondition for exploitation by outsiders. This is especially important, perhaps, in data center situations where an organization is responsible for data repositories for multiple customers. You can give away trust but not risk and responsibility. And yet, organizations need to implement protective measures that will not be circumvented or ignored by staff and other trusted individuals—or processes.

Lexmark Secure Document Monitor with Endpoint ID Key Features

Automated document capture: Capture images of all documents printed, copied, scanned or accessed from the MFP for review and, if flagged based on rules you predefine, further investigation.

Next-level data loss prevention: Gain comprehensive insight into every stage of the data lifecycle.

Identity-based monitoring: Monitor user behavioral cues or patterns that could indicate threats or liability.

Activity statistics: Monitor web and application usage to identify productivity issues.

Infrastructure management: Receive endpoint updates regarding system performance and unauthorized processes.

Technology Challenge

Bridging the analytical gap between the information captured by tools aimed at the "first seven" layers of the OSI model and the information needed by people operating at "layer eight" and beyond is a challenge met by Intelligent ID's unique use of real-time data capture, system/application activity contextual awareness, and behavioral modeling to deliver targeted, all-user-friendly alerts and responses on suspect activity.

Summary

Current Intelligent ID customers across all industries and verticals value the straightforward implementation and learning process that are part of the Intelligent ID feature set, as well as the high degree of situational awareness provided by the real-time use of protected information. As one city government official described: "The flexibility of the rule sets and the ability to monitor all use of devices and any transfer of files to removable storage media were key reasons for selecting Intelligent ID . . . . The fact that we were able to create a clear audit trail of all user activity from any device and prevent any unauthorized use has helped us to immediately comply with our strict IT security policy."

Intelligent ID helps "secure the human" by monitoring user endpoints and informing administrators when it detects suspect activity, including abnormal user behavior and risky data handling procedures. This activity could include a deviation in "typical" behavior which often indicates a greater problem, as with US spies Ames and Hanssen; unauthorized transactions containing sensitive information, as in the case of Societe Generale trader Kerviel; or the potential exposure of confidential PII when copied to removable media or accessed from a sensitive location, as in the compromise of VA medical information (between 2009 and 2012). These, and countless other situations in which human behavior—whether malicious or accidental—puts organizations at grave risk, are diminished by Intelligent ID.

Through tracking risky or anomalous practices, correlating data about individual activities across multiple platforms and processes, and producing easily understood—and legally defensible—reports based on the client organization's business rules and compliance requirements, technical and non-technical managers alike gain the transparency and in-depth forensic evidence necessary to protect their organizations and take action when detrimental activity is suspected. To err may be human, but technology like Intelligent ID's can help deconstruct error and mitigate undesirable consequences.

A synthesis of security against insider threats

Lexmark Secure Document Monitor and Endpoint ID work together seamlessly to help you:

- **Collect data from all sources:** Collect information from every source—from paper to digital.
- **Investigate and build cases easier:** With a single, unified dashboard that allows you to monitor all users and information from one place, you'll be able to better understand how your data is being used, and build more robust case files and investigations.
- **Increase insight with tailored monitoring:** Endpoint ID allows you to set customized rules, keywords and alerts that are unique to your business, for a detection solution that provides you with insight that's tailored to your specific security needs.
- **Simplify compliance:** Automated compliance mapping provides real-time reports on the status of your pre-set initiatives, revealing gaps in compliance by individual endpoint, group, department or organization as a whole.

References

[1]Oak Ridge Laboratory. "Anatomy of an Insider Threat: Case Study in Human Vulnerabilities." Quote from Alex Ryskin (Scientist, Group Leader (Computer Support Group) University of Rochester Laboratory for Laser Energetics

[2]*Common Sense Guide to Mitigating Insider Threat, Fifth Edition* (2016)

[3]http://threatpost.com/en_us/blogs/hipaa-bares-its-teeth-43m-fine-privacy-violation-022311

[4]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/compliancereport2011-2012.pdf

[5]http://www.govtech.com/security/Report-Feds-Exposed-94-Million-Records-in-3-Years.html

[6]http://www.govexec.com/technology/2017/06/nsa-still-vulnerable-insider-threats-watchdog-found/138803/

[7]US Department of Homeland Security Office of Intelligence and Analysis—Note (19 July 2011). "Insider Threat to Utilities," pp. 4-5. http://info.publicintelligence.net/DHS-InsiderThreat.pdf.

[8]https://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?ed=12/31/2014&id=pr827&sd=6/12/2014

[9]http://news.gallup.com/businessjournal/203957/american-workplace-changing-dizzying-pace.aspx

[10]https://remote.co/10-stats-about-remote-work/

[11]Symantec, "What's Yours is Mine," 2014