Tackling Insider Threat with Data Loss Protection

FEATURING RESEARCH FROM FORRESTER

Best Practices: Mitigating Insider Threats

A FRESH PERSPECTIVE ON DATA SECURITY TO ANSWER UNSOLVED PROBLEMS WITH INSIDER THREATS

Data loss due to insider threats is on the rise. With employee churn at an all time high, everyday scenarios such as departing employees are contributing to the problem. And in spite of our best efforts, there will never be enough security people, policies or products to prevent data loss from happening.

The brutal truth is...
60% of departing employees **admit to taking** company data.
70% of IP theft happens in the **30 days before** an employee announces their resignation
90% of insider threats **go undetected**
(Source: Forensic investigations company Precision Discovery 2018)

The most troubling reality is that insider threats continue rising even as more and more organizations invest in DLP (data loss prevention) solutions in an attempt to stem rampant data loss. But traditional DLP simply wasn't designed to manage insider threats. Its original objective was to prevent the exfiltration of regulated data to meet compliance requirements. Traditional DLP just doesn't deliver a comprehensive solution to prevent data loss from insider threats. Moreover, legacy DLP ends up overwhelming security teams with endless policy management — and frustrating end users with rigid policies that stifle productivity and collaboration.

Code42 is challenging the DLP status quo by focusing on protecting the data itself. This new paradigm — next-generation data loss protection — centers on comprehensive visibility into your data and your users' file activity. This visibility delivers the insights required for faster insider threat detection and response. The Code42 Next-Gen Data Loss Protection solution provides purpose-built tools and workflows targeted at your biggest insider threats.

See how Code42 enables a smarter approach to mitigating insider threats. Learn more here.

IN THIS DOCUMENT

Best Practices: Mitigating Insider Threats

Defend Your Organization Against The Threats Insiders Pose

by Joseph Blankenship and Claire O'Malley

May 31, 2019

Why Read This Report

Whether accidental or malicious, insider incidents can result in financial fraud, privacy abuses, intellectual property theft, or damage to infrastructure. It's difficult for security pros to detect this suspicious activity because insiders need to have privileged access to data to do their jobs. Since insiders are people and, therefore, entitled to privacy and due process, security pros must handle these incidents with greater care than external threats. This report describes how to build an insider threat program.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

Insiders Are Responsible For More Than Half Of Your Data Breaches

With trusted access to your most sensitive data, insiders represent a real threat to your business. More than half of our survey respondents told us their firm had experienced an insider incident — either the inadvertent or the malicious misuse of data.

Insider Threats Are Not A Technology Problem

Insiders are people, not computers. Treating insiders as a technology problem ignores the human aspects of motivation and behavior. Detecting insiders requires a defined process and a focused team in addition to detection technologies.

Best Practices: Mitigating Insider Threats

Defend Your Organization Against The Threats Insiders Pose

by Joseph Blankenship and Claire O'Malley
with Stephanie Balaouras, Merritt Maxim, Heidi Shey, Salvatore Schiano, Madeline Cyr, and Peggy Dostie

May 31, 2019

Table Of Contents

Related Research Documents

How Insiders Use The Dark Web To Sell Your Data

Recruiting And Retaining Insider Threat Analysts

Top Cybersecurity Threats In 2019

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

All Data Theft Is An Inside Job — And It Will Cost Your Business

Data theft requires access to the data. That access is either obtained by actors who, using compromised credentials, masquerade as insiders, or it's granted to an insider as part of his or her job.[1] Insiders can be any employee, contractor, partner, or vendor who has access to your firm's data and systems. Today, most security teams focus their security controls on external threats and fail to treat the insider threat as a major threat vector. More than half of global network security decision makers whose firms had suffered a data breach in the past 12 months told us they had experienced at least one insider incident.[2] The damage comes in many forms:

- **Fraud.** Insiders can use their privileged access to modify records, take sensitive data, or steal/transfer money for financial gain. For example, a deputy manager at Punjab National Bank had unauthorized access to a level 5 password which he used to authorize $1.8 billion in fraudulent transactions.[3]
- **Intellectual property theft.** Insiders steal intellectual property such as secret formulas, source code, blueprints, or M&A documentation to sell or use outside the company. In January 2019, Apple filed a criminal complaint against a former employee accused of selling trade secrets.[4] Inside jobs aren't just limited to company employees, however. For example, a third-party contractor, Reality Winner, faces criminal charges of sharing classified information after she allegedly printed and distributed secret NSA documents to the press.[5]
- **Sabotage and destruction.** Insiders perform acts of sabotage such as corrupting data, breaking equipment, or damaging infrastructure maliciously.[6] A former IT admin in the UK was recently sentenced to two years in jail after he used stolen credentials to delete the AWS servers of the company that fired him.[7] A former Georgia-Pacific system administrator was sentenced to 34 months in prison after authorities convicted him of remotely accessing systems at a company paper mill and causing damage to the plant's operations.[8]
- **Snooping, leaking, and doxing.** Insiders can abuse their access to invade the privacy of others or access secrets to which they shouldn't be privy. Often, these insiders leak this information to the media or disclose sensitive information online. A US House of Representatives intern was fired and arrested for doxing senators Lindsey Graham, Mike Lee, and Orrin Hatch.[9] In one especially complicated incident, the head of the National Public Health Unit in Singapore gave his husband access to a list of HIV-positive citizens and visiting foreigners; his husband later sent the list to multiple news agencies and government departments.

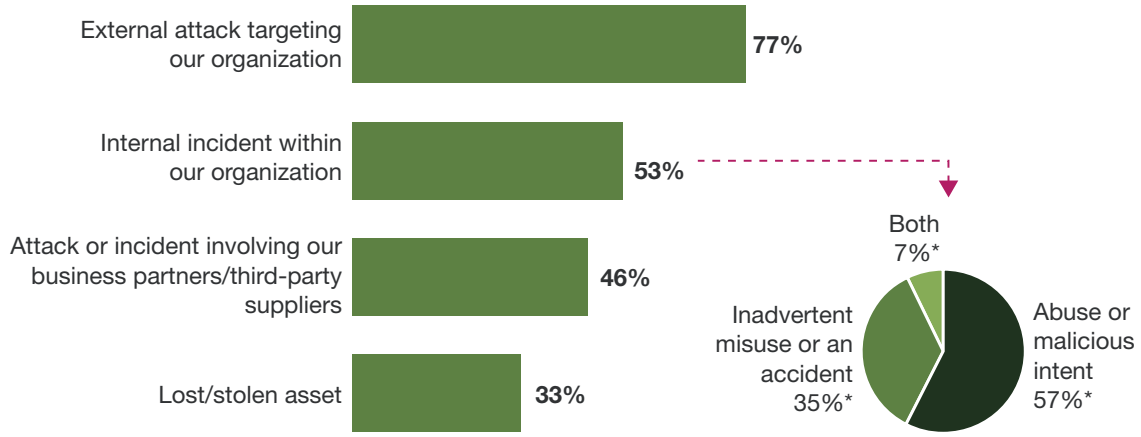
SECURITY PROS MUST ACCEPT THAT THEIR OWN USERS ARE A THREAT . . .

Most of the time, trust in our employees and peers is well placed and allows us to conduct business. However, users intentionally or unintentionally contribute to data breaches. There are three types of insider threats: unintentional misuse, compromised account, and malicious insider. Security pros must realize that:

- **Everyone makes mistakes.** Inadvertent misuses of data make up 35% of the data breaches that our survey respondents attributed to insiders (see Figure 1). For example, an employee could accidentally violate security policy by sending unencrypted documents by email. It's also common for healthcare workers to download sensitive data to a thumb drive and bring the information home to finish their work on an unsecured PC.
- **Cybercriminals disguise themselves as your employees.** Malicious actors from the outside compromise the credentials of privileged users to gain access to financial data. The illicit forums on the dark web connect buyers and sellers of sensitive data, making it easy for them to find each other, negotiate the terms, and conduct the transaction.[10] When this happens, it's difficult to tell that it's not a trusted administrator who has accessed cardholder accounts but a cybercriminal stealing data for their own financial gain.
- **Malicious insiders are on the rise.** Your cubemate may have ulterior motives. For a variety of reasons, trusted insiders are turning rogue to steal data, commit fraud, or sabotage company assets.[11] In 2015, these malicious insiders accounted for 26% of our respondents' internal data breaches. In 2018, that number rose to 57% (see Figure 2).

FIGURE 1 Internal Incidents Were The Second Most Common Cause Of Breaches In 2018

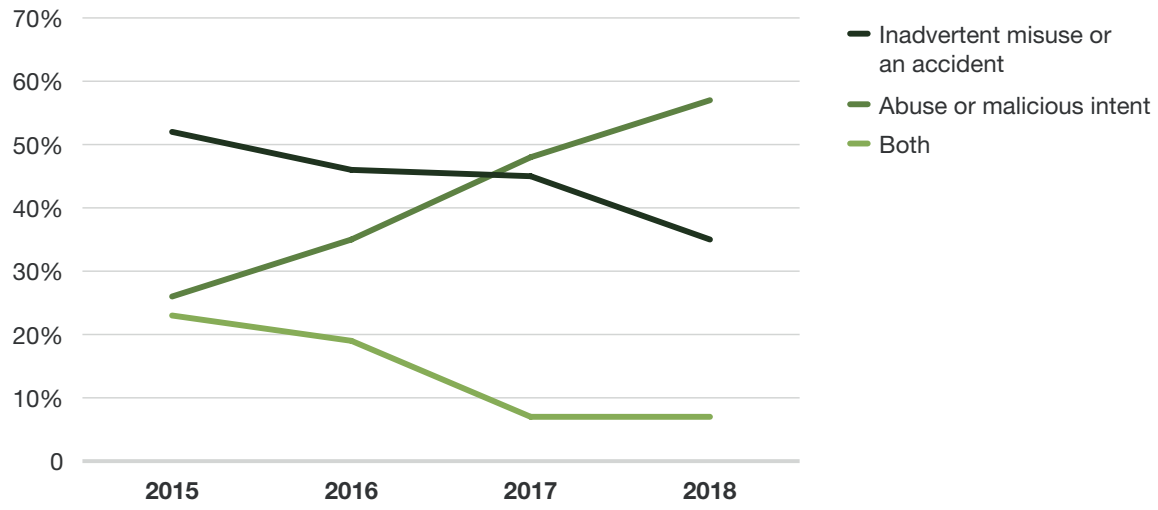
Percentage of respondents who experienced at least one of the following types of attack in the past 12 months
(Multiple responses accepted)



While 35% of external attacks were carried out via a software exploit, 33% involved some type of user interaction (e.g., a watering hole attack, phishing, or social engineering).†

Base: 332 network path security decision makers who have experienced a breach in the past 12 months
*Base: 176 network path security decision makers who experienced an internal attack when their company was breached
†Base: 257 network path security decision makers who experienced an external attack when their company was breached
Note: Percentages do not total 100 due to rounding.
Source: Forrester Analytics Global Business Technographics® Security Survey, 2018

FIGURE 2 Malicious Insiders Are On The Rise



Base: 176 to 343 network path security decision makers who experienced an internal attack when their company was breached

Source: Forrester Analytics Global Business Technographics® Security Surveys, 2015 to 2018

. . . AND UNDERSTAND INSIDER THREAT MOTIVATIONS AND INDICATORS

When it comes to external threat actors, security pros spend a lot of time learning the details of their motivations, intent, and capabilities, but they don't develop this kind of intelligence for internal threats. To understand the dangers within, security pros must:

- **Learn the typical motivations and intentions of malicious insiders.** Insiders' ability to blend in among us is what makes them so scary and such a challenge for security teams. Unlike the employees who suffer a compromise of their credentials or accidentally cause a data breach, malicious insiders make a choice to act (see Figure 3).[12]
- **Familiarize themselves with the early indicators of malicious insiders.** As poker players may have tells that signal when they're bluffing, users may display behavior that is indicative of their likelihood to be a threat. Security teams can use these indicators to develop and focus on leads (see Figure 4).[13]

FIGURE 3 Common Motivations And Intentions Of Malicious Insiders

Motivation	Description
Financial distress	Employee may seek a quick monetary gain to address financial problems.
Disgruntled employee	An angry employee may wish to get back at an employer over a perceived wrong.
Entitlement	Some employees feel entitled to sensitive information and IP.
Announcement or fear of layoff	In response to a layoff announcement, employees may think they are entitled to data or desire to damage the organization.
Revenge	An employee may feel mistreated by a manager or the organization and wish to get even.
Work conflict	Disagreements with other employees may lead to malicious behavior.
Ideology	Political or religious beliefs may motivate an insider to take malicious actions.
Outside influence	Criminal organizations or state-sponsored espionage agencies recruit insiders and use motivations like monetary rewards and blackmail to turn insiders.

FIGURE 4 Early Indicators Of Malicious Insiders

Sample indicators of insider threat
Poor performance appraisals
Voicing disagreement with policies
Disagreements with coworkers
Financial distress
Unexplained financial gain
Odd working hours
Unusual overseas travel
Leaving the company

Follow Forrester's Six Best Practices For An Insider Threat Program

Because insiders are trusted, they have easy access to sensitive data and systems. Waiting until a malicious insider acts may mean the damage is done before you can respond, causing significant harm to the business. Finding potentially malicious insiders requires a focused, cross-organizational approach. In the words of one security leader, "If any company thinks they don't have an insider threat problem, they aren't looking." In the US, federal government agencies and Department of Defense contractors are required to have an insider threat program in place.[14]

Creating an insider threat program doesn't have to be daunting. Security leaders should take 10 steps to establish an insider threat program: 1) Gain executive sponsorship; 2) identify stakeholders; 3) classify data; 4) group users; 5) define policies; 6) create rules of engagement; 7) build a dedicated team; 8) establish consistent processes; 9) train and communicate; and 10) implement monitoring technology (see Figure 5). Once your program is in place, follow Forrester's six best practices for continued success.

FIGURE 5 Ten Steps To Achieve Insider Threat Program Mastery

Forrester's 10 steps to an insider threat program	
1. Gain executive sponsorship	Obtain executive buy-in and support at the highest levels of the organization, including the CEO. HR is often the executive sponsor.
2. Identify stakeholders	Create a steering committee made up of key stakeholders, including the CEO, chief risk officer, chief compliance officer, legal, HR, CSO, and CISO. Other stakeholders may include chief privacy officer, internal audit, and line-of-business owners.
3. Classify data	Find and classify data according to risk, including PII, PHI, cardholder data, and IP. Establish acceptable use and need to access.
4. Group users	Understand and document the risk posed by different users due to their role and access to sensitive data and systems
5. Define policies	Design and document policies concerning acceptable and unacceptable behavior, including system and data use.
6. Create rules of engagement	Establish firm rules of engagement for how the insider threat team should monitor activity, launch investigations, and investigate suspected malicious insiders.
7. Build a dedicated team	Form a dedicated team with specific training and goals to focus on insider threats. The team may report up through HR, CSO, risk, or legal.
8. Establish consistent processes	Develop consistent, repeatable processes for insider threat program operation.
9. Train and communicate	Train and test employees on policies and insider threat program. Communicate regularly with employees to refresh training and update progress. Educate personnel managers and business owners about insider threat risk and their role in the process.
10. Implement monitoring technology	Deploy technology to monitor employee behavior that aligns with your specific requirements, policies, and insider threat team.

BEST PRACTICE NO. 1: APPLY TECHNOLOGY AS ONLY ONE OF MANY SAFEGUARDS

Security vendors are pushing tools like security user behavior analytics (SUBA) for insider threat hunting. However, without a focused approach, good governance, consistent process, and education, tools will be ineffective.[15] As one interviewee stated, "Companies that only have a technical solution, rather than a program involving HR and legal, have a DLP solution, not an insider threat solution." To be effective:

- **Know your insiders.** Managers, co-workers, and HR professionals have insights into insiders and their behavior beyond what security teams can monitor. One of the professionals interviewed for this report noted, "Some behaviors can't be detected with technology; they have to be done by discussing and understanding the nontechnical indicators."
- **Understand business context.** Understanding how users use systems and interact with data helps to identify suspicious behavior. For example, you need to understand what systems your sales force uses on a regular basis and what typical download sizes are. In some contexts, there is high value in understanding where your employees are; if you have users entering and exiting high-risk areas, you may need to use badging and surveillance logs for forensic reasons.

BEST PRACTICE NO. 2: SEPARATE YOUR INSIDER THREAT FUNCTION

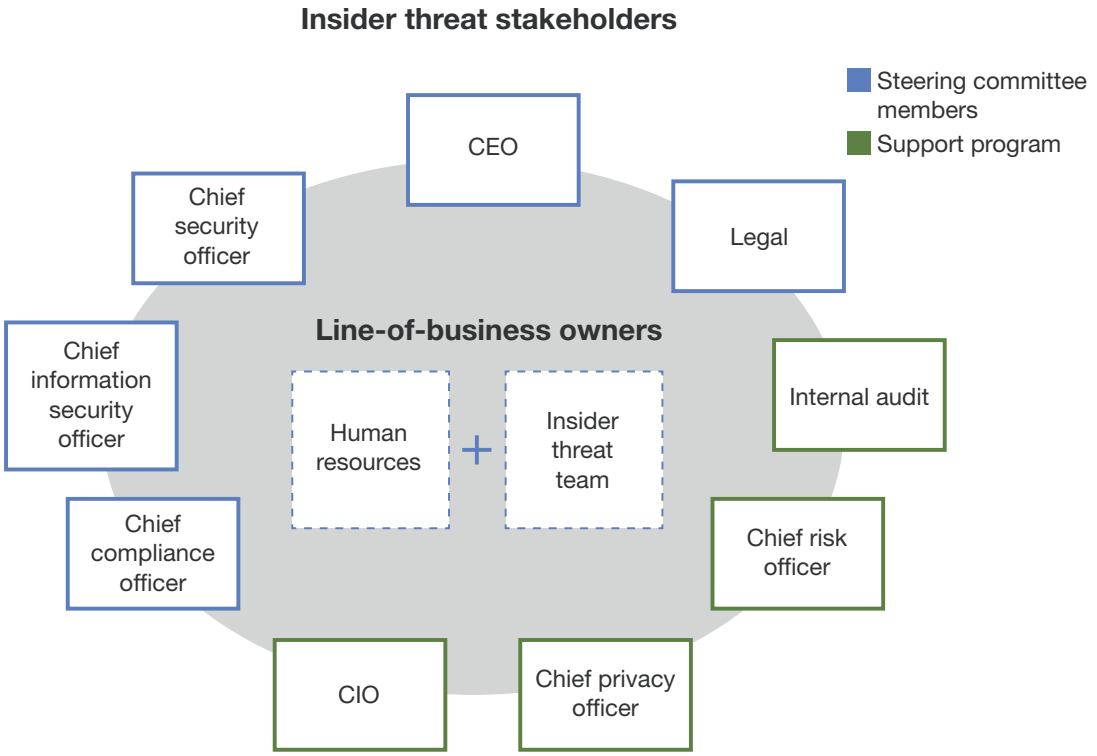
Investigating insiders is different from protecting against external threats, so treat it as a separate function. While building your team, look for investigative experience in law enforcement or counterintelligence.[16] Since the team will be working with very sensitive data about employees (even executives), they also need to be trustworthy. To define your insider threat function:

- **Build a separate insider threat team.** The team doesn't have to be large, but it does need to be almost entirely dedicated to insider threat. In even the largest organizations, most teams are small, consisting of one to three people.
- **Place the insider threat function outside the cybersecurity team.** Insider threat is not a technical problem and should not be part of the IT organization. In some organizations, the insider threat team resides in HR. Others make insider threat a function of the chief security officer (CSO), bridging physical security and cybersecurity, or of the general counsel. Find the fit that works best in your culture.
- **Invest in specialized training for your team.** To be successful, your insider threat analysts need specialized training in investigations and managing malicious insiders. The CERT Insider Threat Center offers training and certification for insider threat managers.[17]
- **Respect employee privacy.** The biggest mistake with combating insider threat is cultivating an adversarial relationship with employees, turning your own employees into the enemy and treating them as such.[18] Take employee privacy and monitoring requirements (and labor law restrictions) into consideration as you develop processes to address insider threats.[19] The employee experience will affect customer experience and business performance.

BEST PRACTICE NO. 3: IDENTIFY CROSS-FUNCTIONAL STAKEHOLDERS

Your insider threat program needs to work across the organization. The insider threat team will depend on input from all parts of the company, especially HR, legal, and technology. Executives from the top down must buy into the program, including the CEO and the board. Several of the firms interviewed stated that HR was the executive sponsor for their program, while others were championed by the chief security officer (CSO), CEO, or general counsel. Include departments (or functions) like HR, legal, privacy, and security as part of your steering committee. Functions like internal audit, risk, privacy, and the CIO should be part of your support organization. Line-of-business owners provide business context for employee behavior (see Figure 6).

FIGURE 6 Insider Threat Stakeholders



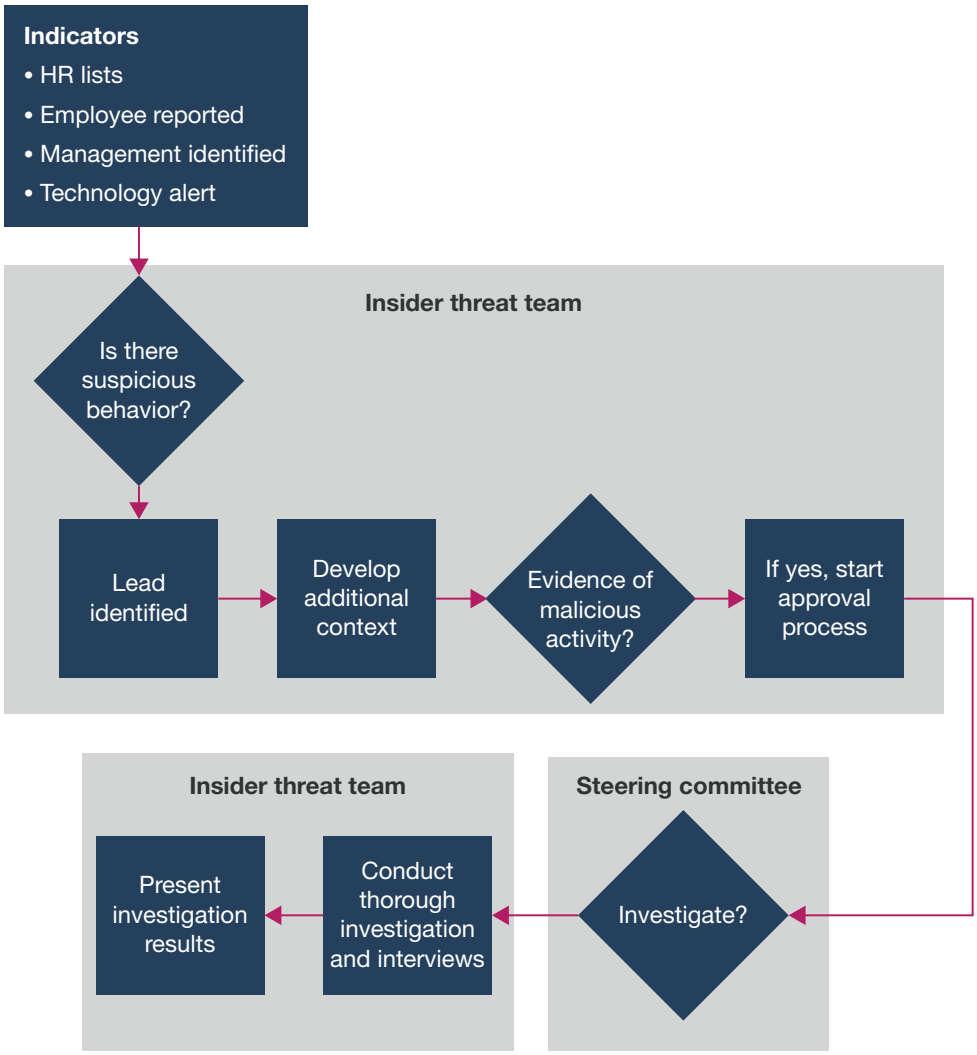
BEST PRACTICE NO. 4: BUILD A CONSISTENT INSIDER THREAT PROCESS

Consistency and fairness should be hallmarks of your insider threat program. Carefully consider how you determine when to start an investigation. HR, legal, compliance, and security are important functions in determining when to investigate an insider (see Figure 7). Establishing and following firm policies and processes will not only help with evidence gathering, it will also help with employee relations and potential litigation. To build your process:

- **Leverage existing policies and processes when possible.** There's no use recreating the wheel. If you have effective policies and controls for handling employee theft, put those to use. This should also include having an up-to-date acceptable use policy for your computing devices and requiring users to sign it annually. This can help better prepare you to defend against the "I didn't know this activity wasn't allowed" defense from malicious employees. With any luck, you won't be dealing with insider threats every day. Review the process annually to see if it needs updating.
- **Know your data.** Understanding what sensitive data you have (PII, PHI, PCI, and IP) and where it resides lets you prioritize the response based on the risk to that data.[20] This should include the physical locations of the servers where such data is stored as well as the physical location of hard-copy records (such as medical records).
- **Treat every investigation as if it will end up in court.** After you've made the decision to start an investigation, move forward as if you are entering a legal investigation. Even if you decide not to prosecute, having evidence that you followed the process will help you if an employee decides to sue. If policies are not enforced consistently, the investigation may be challenged in court. This is another reason for having an updated acceptable use policy.
- **Use technology to enable process.** Once your insider threat hunting process is established, choose technology tools that best fit your needs. SUBA solutions like those from Aruba Networks, Bay Dynamics, Dtex, Gurucul, Haystax, Securonix, and Veriato detect suspicious user activity. Solutions from companies like Digital Guardian, Forcepoint, Jazz Networks, ObserveIT, and Varonis monitor user interactions with data to detect risky behavior.
- **Remember that insiders are your teammates, not adversaries.** Respect employee privacy. Technology solutions should obfuscate employee identities until the decision has been made to start an investigation. Insider threat analysts shouldn't discuss employees outside of the insider threat team. False positives will happen. Never level an accusation against an employee until the investigation is complete. You don't want the program to come off as George Orwell's Big Brother, where employees feel spied on. Don't let the program turn good employees into disgruntled ones, which could possibly lead to more insider threats. Make sure innocent employees are protected and not harmed. Have a data destruction process in place (that adheres to regional laws) to destroy evidence in the event an employee is innocent.

- **Don't forget executives and contractors.** Policies must be enforced consistently, even if it's an executive who is under investigation. Establish processes for handling malicious executives (including the CEO and steering committee members). Third-party contractors often have the same access and can be hard to differentiate from employees. Know when contracts are expiring, and plan accordingly. For higher risk projects, consider requiring contractors to sign a nondisclosure agreement (NDA), especially since specialized contractors could potentially engage with projects at competitors and inadvertently disclose your sensitive data.
- **Get help from experts.** According to interviewees, most cases are not prosecuted. Instead, the offending employee is terminated. If you decide to prosecute, having relationships with local law enforcement or the FBI beforehand will be helpful. Service providers like Accenture, Aon, Deloitte, EY, KPMG, Leidos, PwC, and Rapid7 can provide guidance to establish the insider threat program.

FIGURE 7 Forrester's Insider Threat Program Model



BEST PRACTICE NO. 5: TURN YOUR EMPLOYEES INTO ADVOCATES FOR THE PROGRAM

Employees can be your greatest ally for stopping malicious insiders.[21] To turn your employees into advocates:

› **Train them on the impact of insider threats.** Lost IP, lost customer data, or sabotage can destroy a business. Let your employees know the stakes. Engage in regular training about insider threats and acceptable use policies. Track the training, so there are no excuses for breaches of policy.

- **Communicate the program openly.** Don't make the insider threat program a secret. Let the employees know you're watching and how the program works (in general terms). After a recent ruling by the European Court of Human Rights in favor of an employee who had been monitored and fired, this is mandatory, not just a best practice, for any firm with European employees.[22]
- **Establish an anonymous employee tip line.** In the theme of "If you see something, say something," encourage your users to make anonymous tips about suspicious behavior they've observed. Be careful with the language you choose, as one interviewee reported that the word "report" had a negative connotation with users.
- **Let employees know they're part of the security team.** Users are the last line of defense for security. The decisions they make will directly impact the success or failure of a phishing scheme or social engineering attempt.[23] They are also your eyes and ears about what's happening with fellow employees.

BEST PRACTICE NO. 6: ENSURE YOUR PROGRAM COMPLIES WITH APPLICABLE LAWS AND REGULATIONS

Laws and rules about how employees' data must be collected, processed, and stored vary from country to country and largely affect how you can monitor employees. What works in the US may not work in Europe. For example, the European General Data Protection Regulation (GDPR) extends privacy protection and safeguards to the personal data of European employees, but the recently adopted California Consumer Privacy Act does not. Several of the professionals interviewed for this report also cited the need to pay attention to work councils' requirements and labor laws, in addition to privacy laws, when launching programs. Before starting an insider threat program, work with legal and compliance to ensure the program operates within applicable law.

What It Means

Insider Threats Will Increase And Bring Logical And Physical Impacts

Malicious insiders can affect organizations that may not typically consider themselves at risk. Every organization, however, has assets and people that it needs to protect. Build an insider threat function that addresses what matters most to your organization. Knowing the signs of an employee becoming malicious may not only save your valuable data, it could also save lives in the event the threat changes from digital to physical. It's crucial to put process ahead of technology, and to involve teams like HR that understand culture building and employee motivation.[24] As employee satisfaction wanes, employees

may be more likely to commit malicious acts. Security teams that treat users like machines will fail.

Supplemental Material

SURVEY METHODOLOGY

The Forrester Analytics Global Business Technographics® Security Survey, 2018, was fielded between May and June 2018. This online survey included 3,089 respondents in Australia, Canada, China, France, Germany, the UK, and the US from companies with two or more employees.

The Forrester Analytics Global Business Technographics Security Survey, 2017, was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

The Forrester Analytics Global Business Technographics Security Survey, 2016, was fielded in March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

The Forrester Analytics Global Business Technographics Security Survey, 2015, was fielded in April through June 2015 of 3,543 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

COMPANIES INTERVIEWED FOR THIS REPORT

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Aon

Code42

Digital Guardian

Dtex Systems

Exabeam

Forcepoint

Gurucul

Haystax Technology

HPE Aruba

Imperva

Insider Threat Management Group

Interset (Micro Focus)

KPMG

Leidos

ObserveIT

PwC

Securonix

Varonis

Verizon

Endnotes

[1] Forrester's Zero Trust Model of information security is a conceptual and architectural model for how security teams should redesign networks into secure microperimeters, strengthen data security using obfuscation techniques, and limit the risks associated with excessive user privileges. See the Forrester report "The Zero Trust eXtended (ZTX) Ecosystem."

[2] Source: Forrester Analytics Global Business Technographics Security Survey, 2018.

[3] Source: Suparna Goswami, "Mitigating the Insider Threat: Lessons From PNB Fraud Case," BankInfoSecurity, February 21, 2018 (https://www.bankinfosecurity.com/mitigating-insider-threat-lessons-from-indian-fraud-case-a-10674).

[4] Source: Liane Yvkoff, "Apple Engineer Arrested, Accused Of Stealing Autonomous Vehicle Trade Secrets," Forbes, January 30, 2019 (https://www.forbes.com/sites/lianeyvkoff/2019/01/30/apple-engineer-arrested-accused-of-stealing-autonomous-vehicle-trade-secrets/#14275411602d).

[5] Source: Lois Beckett, "The arrest of Reality Winner highlights US intelligence vulnerability," The Guardian, June 6, 2017 (https://www.theguardian.com/us-news/2017/jun/06/reality-winner-nsa-contractors-leaks).

[6] Source: Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak, The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Addison-Wesley Professional, 2012.

[7] Source: Lisa Vaas, "Sacked IT guy annihilates 23 of his ex-employer's AWS servers," Naked Security by Sophos, March 22, 2019 (https://nakedsecurity.sophos.com/2019/03/22/sacked-it-guy-annihilates-23-of-his-ex-employers-aws-servers/).

[8] Source: "Former Systems Administrator Sentenced to Prison for Hacking into Industrial Facility Computer System," US Department of Justice press release, February 16, 2017 (https://www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer).

[9] Emily Sullivan, "House Intern Arrested, Charged With Doxing Senator During Kavanaugh Hearing," NPR, October 4, 2018 (https://www.npr.org/2018/10/04/654264122/house-intern-arrested-for-reportedly-doxing-senator-during-kavanaugh-hearing).

[10] See the Forrester report "How Insiders Use The Dark Web To Sell Your Data."

[11] In one mysterious instance, a seemingly harmless network administrator employed by the city of San Francisco was charged with four counts of computer tampering after he took the network hostage. Source: Paul Venezia, "Why San Francisco's network admin went rogue," InfoWorld, July 18, 2008 (http://www.infoworld.com/article/2653004/misadventures/why-san-francisco-s-network-admin-went-rogue.html).

[12] See the Forrester report "Lessons Learned From The World's Most Notable Privacy Abuses And Security Incidents, 2017."

[13] It's important to note, however, that this is a very tricky area outside of the US because of worker privacy rights and concerns. There is also some growing concern around US organizations performing credit checks as part of the new-hire process. Source: Lisa Guerin, "Can Prospective Employers Check Your Credit Report?" Nolo (http://www.nolo.com/legal-encyclopedia/can-prospective-employers-check-your-credit-report.html).

[14] Source: Gaby Friedlander, "What IS NISPOM Conforming Change 2? All You Need to Know UPDATED," ObserveIT blog, June 2, 2016 (http://www.observeit.com/blog/what-nispom-conforming-change-2-all-you-need-know-updated).

For more information about US Executive Order 13587 and the requirement for US government agencies and contractors to have an insider threat program in place, see the Forrester report "Brief: How To Meet November's Deadline And Build A Valuable Insider Threat Program."

[15] See the Forrester report "The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019."

[16] See the Forrester report "Recruiting And Retaining Insider Threat Analysts."

[17] Source: "CERT Insider Threat Program Manager Certificate," Software Engineering Institute, Carnegie Mellon University (https://www.sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=15170).

[18] See the Forrester report "Protect Your Intellectual Property And Customer Data From Theft And Abuse."

[19] See the Forrester report "Employee Data Security And Privacy Matter More Than You Think."

[20] To learn how to define toxic data using the 3P + IP = TD model, see the Forrester report "Rethinking Data Discovery And Classification Strategies" and see the Forrester report "Develop Effective Security And Privacy Policies."

[21] In the 2011 to 2016 television drama Person of Interest, a wealthy programmer built an artificial intelligence surveillance program known as the "Machine" that predicts crime. Using the Machine, hacked camera systems, and human surveillance, the primary characters attempt to stop crimes before they happen, only knowing the identities of people involved in the crime but having no knowledge of what the crime will be beforehand. Source: "Person of Interest," IMDb (http://www.imdb.com/title/tt1839578/).

[22] Source: Louise Lawrence, "Can employers carry out covert surveillance on staff?," Personnel Today, April 26, 2019 (https://www.personneltoday.com/hr/can-employers-carry-out-covert-surveillance-on-workers/).

[23] Productivity and collaboration tools are an essential technology component of workforce enablement, and because of its economics, scale, and familiar interfaces, Microsoft's Office 365 online productivity and collaboration suite has become very popular. However, firms don't always understand and prepare for the security considerations of a hosted environment — particularly for hosted email. See the Forrester report "Brief: Five Key Capabilities For Microsoft Office 365 Email Security."

[24] What's missing from most workforce technology strategies is an understanding of what makes people truly engaged and productive employees and how this relates to customer experience and financial performance for the company. See the Forrester report "Transform The Employee Experience To Drive Business Performance."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

DEPARTING EMPLOYEES ARE YOUR SINGLE BIGGEST INSIDER THREAT TO DATA LOSS.

Last year, 40 Million people changed jobs. 60% of them admit to taking data when they leave and 70% do it 30 days before they quit. Prevention will fail. Data will get out. 90% of data loss when employees quit goes undetected for months. By the time you find out about it – the damage is done and you're wrapped up in a lawsuit. Our job is to make sure you're not blindsided by it. We provide real time detection and response so you can remediate before damage is done.

Code42 specializes in next-gen data loss protection. Our Customers know when they are bleeding data when an employee quits. We help them setup a process to quickly detect employee data theft and take action before it's too late. Their old employee o boarding process made sure departing employees turned in their badge and laptop. With Code42, they now make sure employees don't take company data on the way out.

Learn more about us at www.code42.com