Best Practices: Mitigating Insider Threats

Processes: The Security Architecture And Operations Playbook

by Joseph Blankenship and Claire O'Malley

November 2, 2017

Why Read This Report

Whether accidental or malicious, insider threat 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 in order 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 that 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

Processes: The Security Architecture And Operations Playbook

by Joseph Blankenship and Claire O'Malley
with Stephanie Balaouras, Merritt Maxim, Heidi Shey, Salvatore Schiano, Elsa Pikulik, Bill Barringham, and Peggy Dostie

November 2, 2017

Table Of Contents

Related Research Documents

Counteract Cyberattacks With Security Analytics

Creating Actionable Security And Privacy Policy

Market Overview: Security User Behavior Analytics (SUBA), 2016

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 that 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, Anthem BlueCross and BlueShield notified 18,000 of its customers who are Medicare members after an employee emailed their customer data to a personal email address and allegedly misused the data.[3] One especially evil incident had external hackers and insiders collaborating across multiple Chinese hospitals to breach and sell the personal information of 200,000 children.[4]
- **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. A financial services firm's senior systems administrator is facing up to 10 years in prison for allegedly writing malware to steal core data files necessary for proprietary algorithms related to stock trading.[5] Inside jobs aren't just limited to company employees, however. For example, third-party contractor Reality Winner faces charges of sharing classified information after she allegedly printed and distributed secret NSA documents to the press.[6]
- **Sabotage and destruction.** Insiders perform acts of sabotage such as corrupting data, breaking equipment, or damaging infrastructure maliciously.[7] A former Georgia-Pacific system administrator was sentenced to 34 months in prison after being convicted of remotely accessing systems at a company paper mill and causing damage to the plant's operations.[8] After 14 years on the job, another former sysadmin is accused of using an old laptop and a former subordinate's credentials to plant a logic bomb on company servers to delete critical financial data.[9]

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:

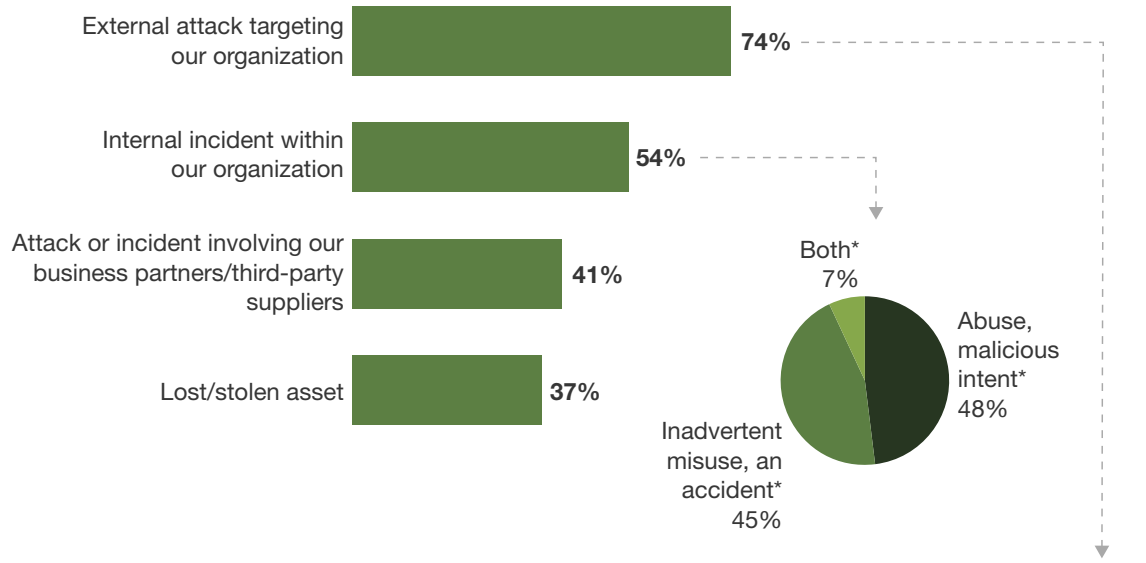
- **Everyone makes mistakes.** Inadvertent misuses of data make up 45% of the data breaches that our survey respondents attributed to insiders (see Figure 1). For example, an employee could accidentally violate security policy by sending unencrypted documents by email. It's also very common for healthcare 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. 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.[10]

› **Some employees choose to be malicious.** Your cubemate may be a wolf in sheep's clothing. For a variety of reasons, trusted insiders are turning rogue to steal data, commit fraud, or sabotage company assets.[11] In 2017, these malicious insiders accounted for 48% of our respondents' internal data breaches.[12]

FIGURE 1 Internal Incidents Were A Significant Cause Of Breaches In 2017

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



While 41% of external attacks were carried out via a software exploit, 44% involved some type of user interaction (e.g., a watering hole attack, phishing, malicious link, or email attachment).†

Base: 549 global network security decision makers whose firms have had a security breach in the past 12 months
*Base: 298 global network security decision makers whose firms have had an internal security breach in the past 12 months
†Base: 404 global network security decision makers whose firms have had an external security breach in the past 12 months
Source: Forrester Data Global Business Technographics® Security Survey, 2017

. . . 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 2).[13]
- **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 3).[14]

FIGURE 2 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 3 Early Indicators Of Malicious Insiders

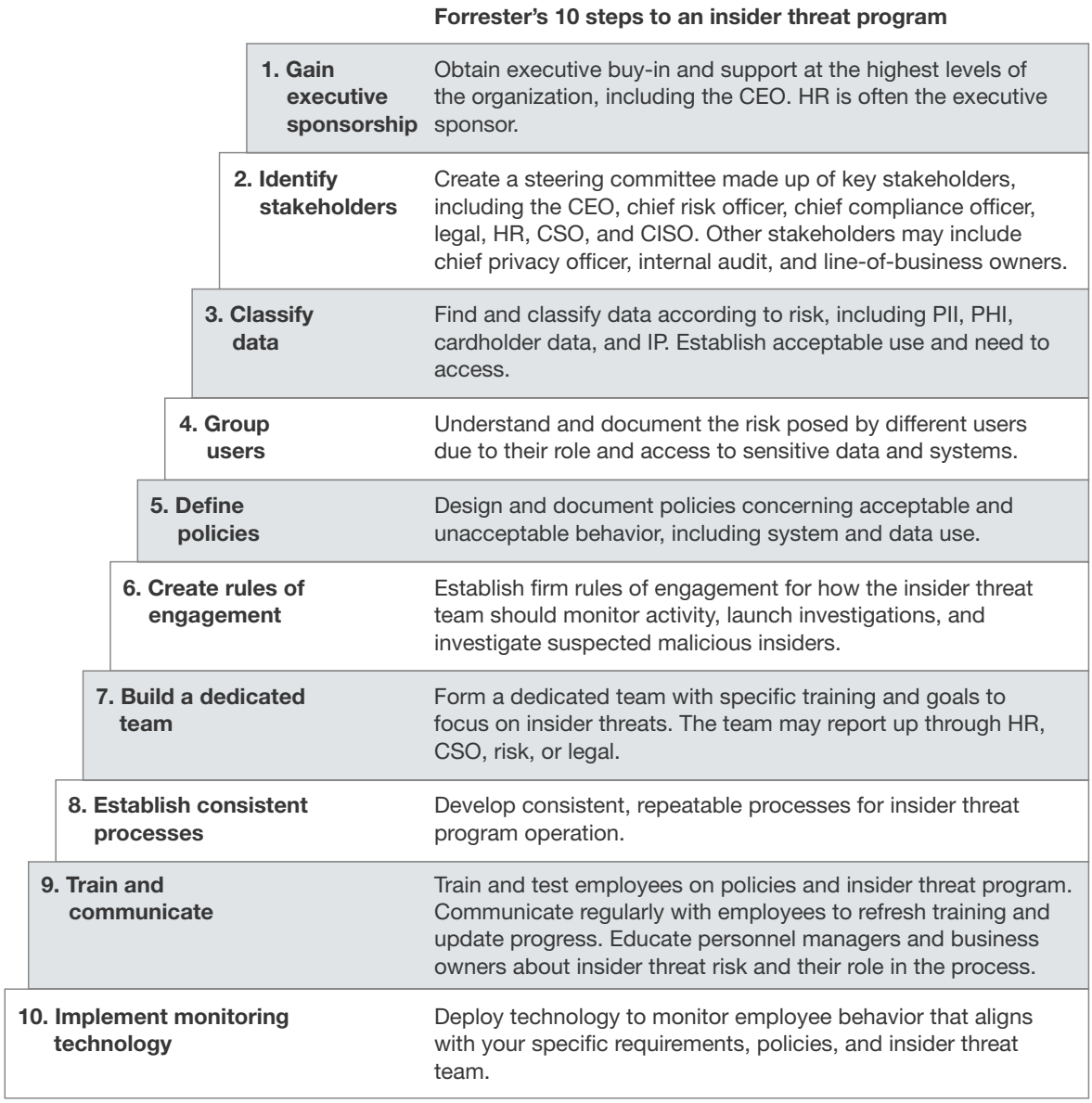
Sample indicators of insider threat
Poor performance appraisals
Voicing disagreement with policies
Disagreements with co-workers
Financial distress
Unexplained financial gain
Odd working hours
Unusual overseas travel
Leaving the company

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

Because insiders are trusted, they typically 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 to detection and response. In the words of one security leader interviewed for this report, "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 now required to have an insider threat program in place.[15]

Creating an insider threat program doesn't have to be daunting. We recommend that security leaders take these 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. Notice that implementing monitoring technology is the last step (see Figure 4). Build your program first, then choose a technology solution that works with your process.

FIGURE 4 10 Steps To Achieve Insider Threat Program Mastery



Best Practice No. 1: Accept That Technology Alone Won't Catch Malicious Insiders

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, the tools will be ineffective.[16] 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, security pros must first:

- **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, it may be necessary to use badging and surveillance logs for forensic reasons.

Best Practice No. 2: Carefully Plan 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. Since the team will be working with very sensitive data about employees (even executives), they also need to be trustworthy. Security pros must:

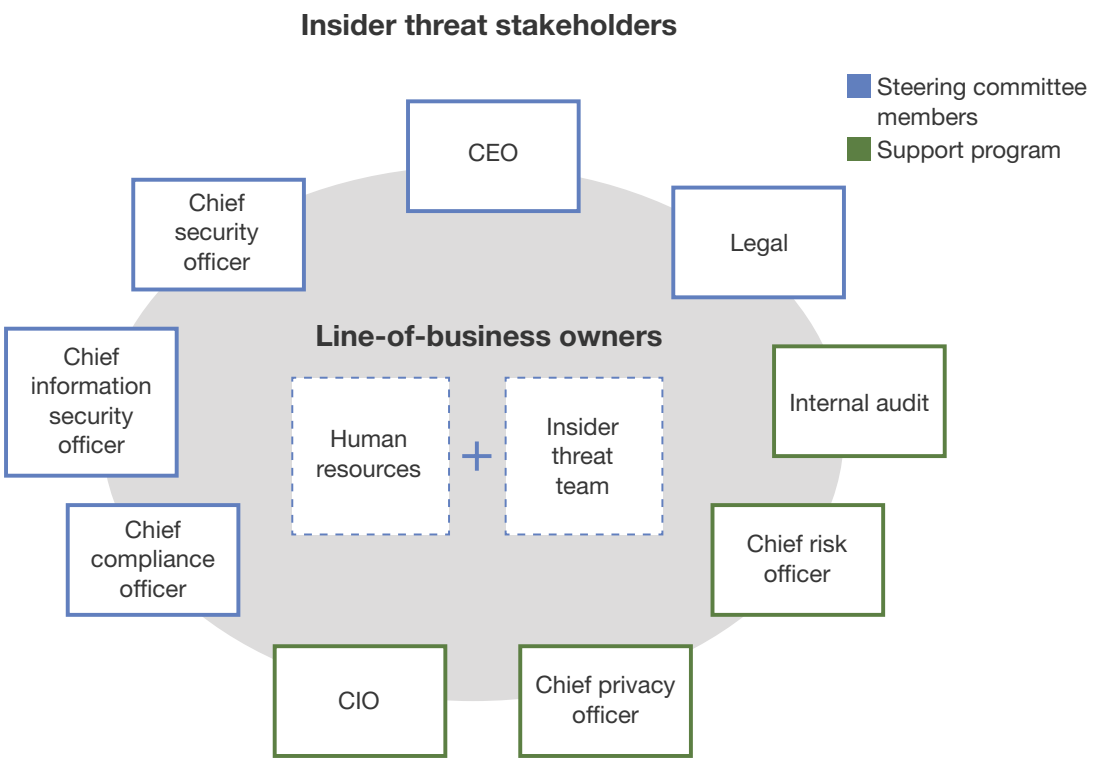
- **Build a separate insider threat team.** The team doesn't have to be large, but it does need to be almost entirely dedicated to insider threat. Most teams are small, consisting of one to three people, in even the largest organizations.
- **Place the insider threat function outside the cybersecurity team.** Insider threat is not a technical problem and should not be part of the IT organization. In some organizations interviewed, the insider threat team resides in human resources (HR). Others have insider threat as a function of the chief security officer (CSO), bridging physical security and cybersecurity, or reporting to 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 teams and 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 organization. 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 5).

FIGURE 5 Insider Threat Stakeholders



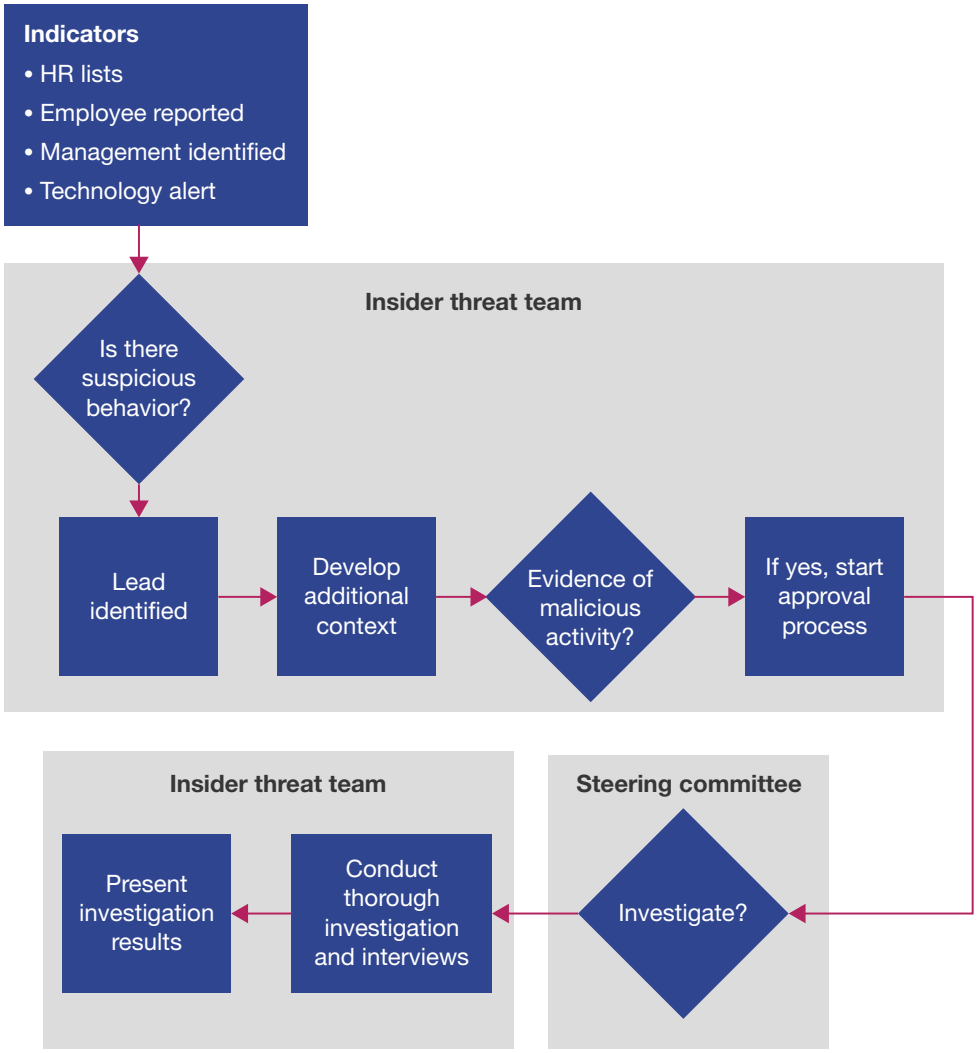
Best Practice No. 4: Build A Consistent Insider Threat Process

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 6). Establishing firm policies and processes and following them will not only help with evidence gathering, it will also help with employee relations and potential litigation. This means security pros must:

- **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.
- **Know your data.** Understanding what sensitive data (PII, PHI, PCI, and IP) you have and where it resides allows you to 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, proceed 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 Dtex Systems, Forcepoint, and Interset detect suspicious user activity. Solutions from companies like Digital Guardian, ObservelT, Thinair, and Varonis monitor user interactions with data to detect risky behavior.
- **Remember that insiders are your teammates, not adversaries.** 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 are made to feel uneasy. Don't let the program turn good employees into disgruntled insiders, which could possibly lead to more insider threats.
- **Don't forget contractors.** 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 sensitive data from other projects.
- **Keep in mind that executives are insiders, too.** 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).
- **Consider applicable laws and regulations.** Privacy laws vary from country to country. What works in the US may not work in Europe. Several of the professionals interviewed for this report cited problems launching programs especially in Germany due to privacy laws. Before starting an insider threat program, work with legal to ensure the program operates within applicable law.[21]

- **Be wary of watercooler talk.** Respect employee privacy. Technology solutions should obfuscate employee identities until the decision had been made to start an investigation. Insider threat analysts shouldn't discuss employees outside of the insider threat team.
- **Know what happens after the investigation is over.** 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.
- **Build relationships with law enforcement.** 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.
- **Get help from experts.** Service providers like Leidos, PwC, and Stroz Friedberg can provide guidance to establish the insider threat program.
- **Test the process annually.** With any luck, you won't be dealing with insider threats every day. Review the process annually to see if it needs updating.

FIGURE 6 Forrester's Insider Threat Program Model



Best Practice No. 5: Make Your Employees Advocates For The Program

Employees can be your greatest ally for stopping malicious insiders.[22] This requires security pros to:

› **Train employees about 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.
- **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] Like Varys' "little birds" in Game of Thrones, they are also your eyes and ears about what's happening with fellow employees.

What It Means

Don't Treat Your Users Like Machines

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 Data 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.

Forrester Data 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 Data 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

Aruba, a Hewlett Packard Enterprise Company
Dtex Systems
Forcepoint
Haystax Technology
Imperva
Interset
Leidos
ObserveIT
PwC
Stroz Friedberg
Verizon

Endnotes

[1] There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For today's digital business, this perimeter-based security model is ineffective against malicious insiders and targeted attacks. For more, see the Forrester report "No More Chewy Centers: The Zero Trust Model Of Information Security."

[2] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[3] Source: Jessica Davis, "Anthem: Insider theft exposes data of 18,000 Medicare members," Healthcare IT News, July 31, 2017 (http://www.healthcareitnews.com/news/anthem-insider-theft-exposes-data-18000-medicare-members).

[4] Source: Patrick Howell O'Neill, "Health care industry is king of the malicious insider threat," CyberScoop, March 29, 2017 (https://www.cyberscoop.com/health-care-industry-king-malicious-insider-threat/).

[5] Source: Patrick Howell O'Neill, "Insider charged with writing malware to steal Wall Street firm's crown jewel algorithms," CyberScoop, April 10, 2017 (https://www.cyberscoop.com/rogue-insider-charged-writing-malware-steal-wall-street-firms-crown-jewel-algorithms/).

[6] 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).

[7] 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.

[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] Source: Iain Thomson, "Sysadmin 'trashed old bosses' Oracle database with ticking logic bomb'," The Register, April 14, 2017 (https://www.theregister.co.uk/2017/04/14/sysadmin_crash_former_employers_oracle_db/).

[10] When Anthem (the nation's second largest health insurer) was breached in 2015, a database administrator discovered his credentials were being used to run a questionable query. Source: Steve Ragan, "Anthem: How does a breach like this happen?" CSO, February 9, 2015 (http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html).

[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] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[13] See the Forrester report "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016."

[14] 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).

[15] Source: Gaby Friedlander, "What IS NISPOM Conforming Change 2? All You Need to Know UPDATED," ObserveIT, 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."

[16] Security and risk leaders are struggling to prevent data breaches, threats from malicious insiders, and fraud. Security user behavior analytics (SUBA) solutions aim to provide S&R pros with a unified view of user activity across the enterprise in order to detect suspicious activity and stop it before it causes lasting harm to the business. For more, see the Forrester report "Market Overview: Security User Behavior Analytics (SUBA), 2016" and see the Forrester report "Vendor Landscape: Security User Behavior Analytics (SUBA)."

[17] Source: "CERT Training Courses," CERT (www.cert.org/training/).

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

[19] Forrester outlines seven principles to help craft an effective security strategy that respects employee privacy. 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 "Creating Actionable Security And Privacy Policy."

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

[22] 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/).

[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 "Elevate Human Performance With Workforce Enablement."

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.