Hunting Insider Threats

Forrester's Model For Establishing An Insider Threat Team

by Joseph Blankenship

July 20, 2016

Why Read This Report

Insider threats are a real risk to business because they threaten both customer and employee trust. Accidental or malicious misuse of the firm's most sensitive and valuable data can result in customer identity theft, financial fraud, intellectual property theft, or damage to infrastructure. Because insiders have privileged access to data in order to do their jobs, it's difficult for security pros to detect suspicious activity. 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.

Key Takeaways

Insiders Are Responsible For Many Breaches
With trusted access to your most sensitive data, insiders represent a real threat to your business. Insiders accounted for 39% of data breaches in 2015 through accidental and 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.

Hunting Insider Threats

Forrester's Model For Establishing An Insider Threat Team

by Joseph Blankenship
with Stephanie Balaouras, Merritt Maxim, Heidi Shey, Salvatore Schiano, and Peggy Dostie

July 20, 2016

Table Of Contents

Notes & Resources

Forrester interviewed 13 vendor and user companies, including Dtex Systems, Imperva, Interset, Lockheed Martin, Niara, ObserveIT, PwC, RedOwl, Stroz Friedberg, and Verizon.

Related Research Documents

Counteract Cyberattacks With Security Analytics

Instill A Culture Of Data Security And Privacy

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. Access is either obtained by actors who, using compromised credentials, masquerade as insiders, or is 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. Because users are, by and large, trusted, detecting insider threats can be difficult. Since insider threats led to 39% of data breaches in 2015, security leaders can't afford to ignore insiders as a threat vector.[2] Unfortunately, most security teams today focus their security controls on external threats. The impacts include:

- **Fraud.** Insiders can use their privileged access to modify records or steal/transfer money for financial gain. In one case, an IT contractor almost got away with stealing close to $2 million from four credit unions for whom he performed IT services.[3]
- **Intellectual property theft.** Insiders can steal intellectual property such as secret formulas, source code, blueprints, or M&A documentation to sell or use outside the company. A 2015 Intel Security report found that 43% of data exfiltration was perpetrated by internal actors.[4] Inside jobs aren't just limited to a company's employees, however. In April 2016, a federal jury ruled in favor of Epic Systems, an EMR software vendor, to the tune of $940 million when Epic filed suit against a former contractor, Indian firm Tata Consultancy Services (TCS). The suit alleged that a TCS employee had illegally downloaded Epic's software and trade secrets while employed as a contractor.[5]
- **Sabotage and destruction.** Insiders can perform acts of sabotage such as corrupting data or breaking equipment or infrastructure maliciously.[6] One instance involved a DuPont research scientist who successfully (and illegally) accessed and downloaded confidential documents while working at the company. The confidential documents were valued at $400 million; his activities were only discovered after he announced his plans to leave DuPont, when the company realized unusually high usage of the EDL server, putting him far above the baseline for his user's role.[7]

Security Pros Must Accept That Their Own Users Are A Threat . . .

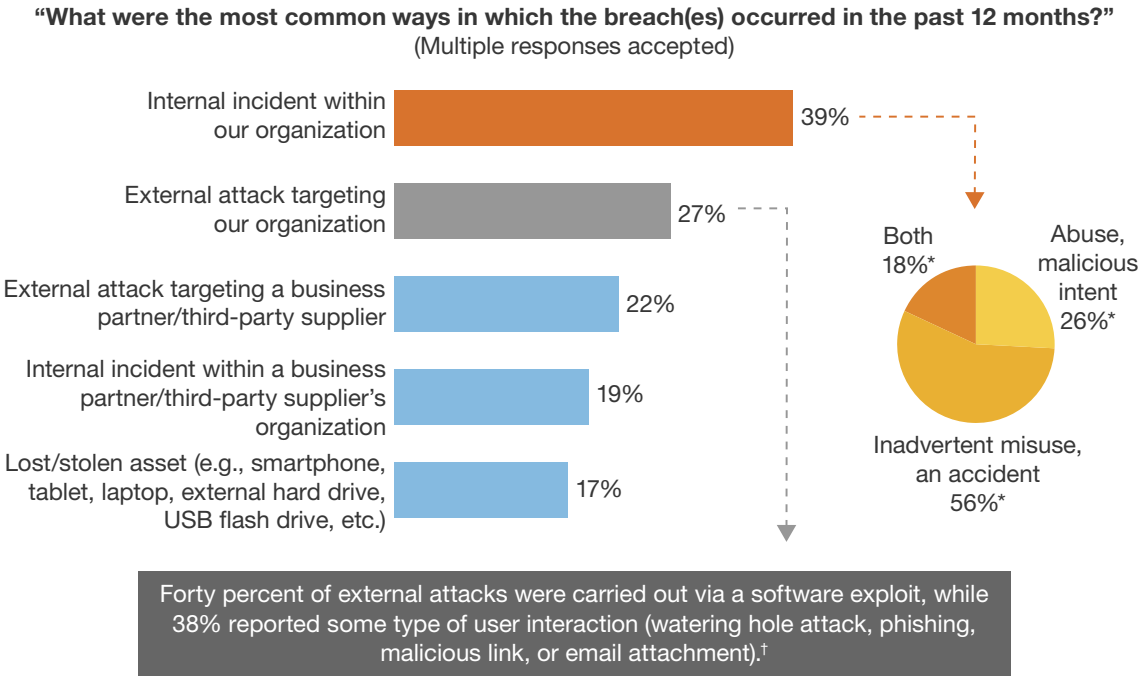
Generally, we have a very trusting nature. We want to trust our employees and our peers and believe they would not be capable of doing anything malicious. Most of the time, this trust is well placed and allows us to conduct business. However, users become a threat when they intentionally or unintentionally contribute to a data breach. In its latest data breach report, Verizon tracked 10,489 insider incidents in 2015, and of those, 172 resulted in data disclosure.[8] In general, there are three types of insider threats: unintentional misuse, compromised account, and malicious insider. Security pros must realize that:

- **Even the good guys make mistakes.** Sometimes people make honest mistakes like downloading sensitive data to a thumb drive and taking the information home to use on an unsecured PC (very common in healthcare industries). They may accidentally violate security policy by sending unencrypted documents by email. These types of unintentional misuses of data make up 56% of data breaches attributed to insiders (see Figure 1).[9]

› **Sometimes the bad guys look like good guys.** Malicious actors often compromise the credentials of privileged users in order to get access to data. When this happens, it's difficult to tell that it's not a trusted administrator who has accessed cardholder accounts, but a cybercriminal who plans to steal the data and sell it.[10]

› **Say it ain't so, Joe; sometimes employees choose to be malicious.** Yes, your cubemate may be a wolf in sheep's clothing. One day you're both gossiping in the breakroom, the next day he's on the lam and the company is in a panic. Malicious insiders account for 26% of data breaches traced to insiders.[11] For a variety of reasons, trusted insiders turn rogue and steal data, commit fraud, or sabotage company assets.[12]

FIGURE 1 Internal Incidents Were The Most Common Cause Of Breaches In 2015



Base: 358 North American and European network security decision-makers who have experienced data breaches in the past 12 months (20+ employees)
*Base: 184 North American and European network security decision-makers who have experienced the specified breaches (20+ employees)
†Base: 156 North American and European network security decision-makers who have experienced the specified breaches (20+ employees)

Source: Forrester's Global Business Technographics® Security Survey, 2015

. . . And Understand Insider Threat Motivations And Indicators

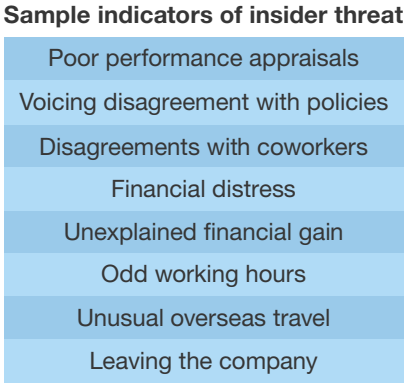
When it comes to external threat actors, security pros spend a lot of time learning the details of their motivations, intent, and capabilities, but they don't always develop this kind of intelligence about insiders. Security pros must:

- **Learn the typical motivations and intentions of malicious insiders.** Unlike insiders who suffer a compromise of their credentials or accidentally cause a data breach, malicious insiders make a choice to act. Their ability to blend in among us is what makes them so scary and such a challenge for security teams. There are a variety of reasons trusted insiders turn malicious (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 leads on which to focus (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

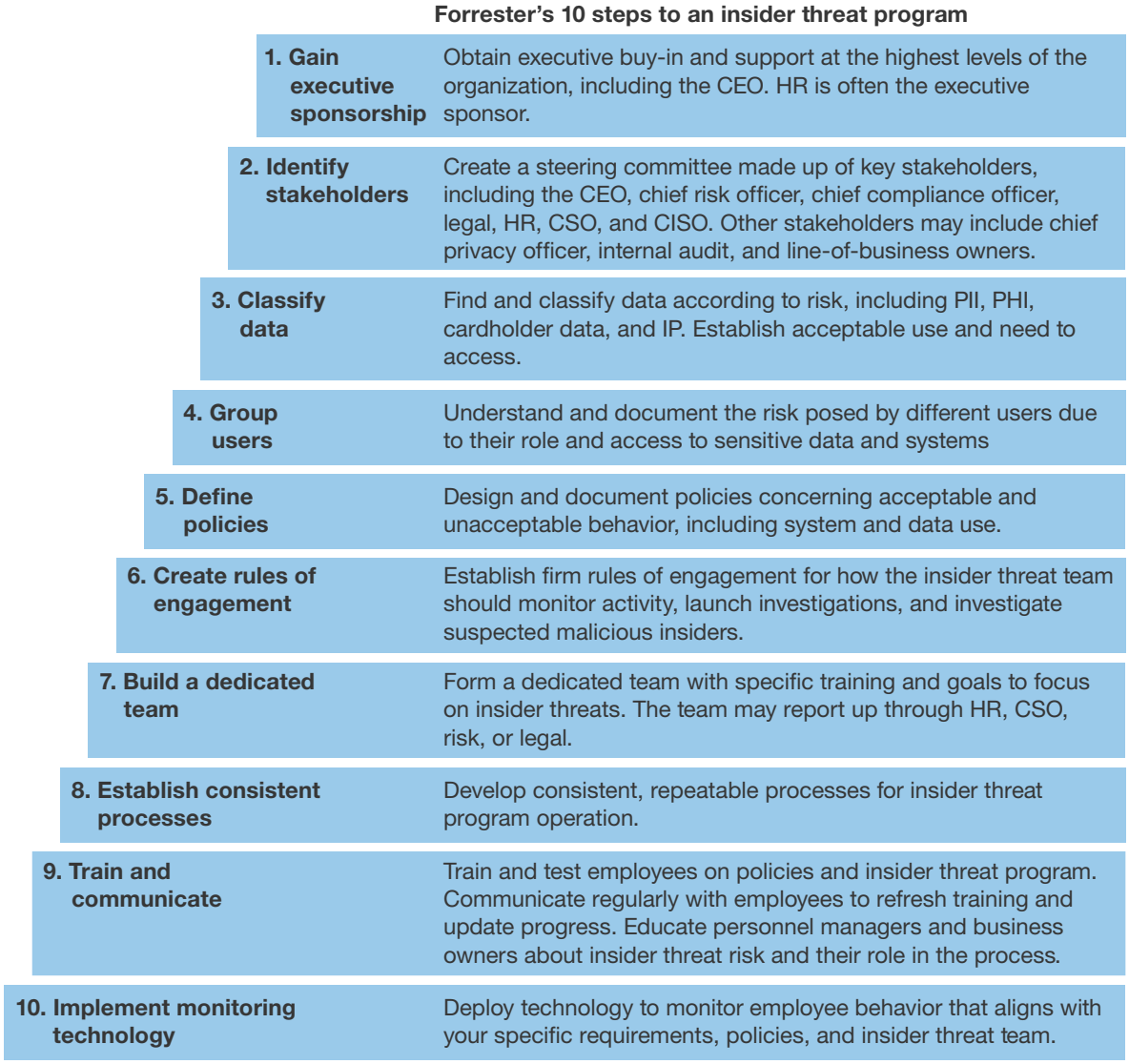


Follow Forrester's 10 Steps To An Insider Threat Program

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 act, 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 by November 30, 2016.[15]

Creating an insider threat program doesn't have to be a daunting task. We recommend that security leaders follow 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



Technology Alone Won't Catch Malicious Insiders

Security vendors are pushing tools like security user behavior analytics (SUBA) for insider threat hunting.[16] The tools are helpful in identifying suspicious and potentially malicious behavior, but they won't be effective without a focused approach, consistent processes, and education. 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:

- **Know your insiders.** Managers, coworkers, and HR professionals have insight into insiders. 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 the case of the DuPont employee, his download activity is what sparked the investigation. And 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.

Carefully Plan Your Insider Threat Function

Investigating insiders is different from protecting against external threats, and you must treat it as a separate function. As you build 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:

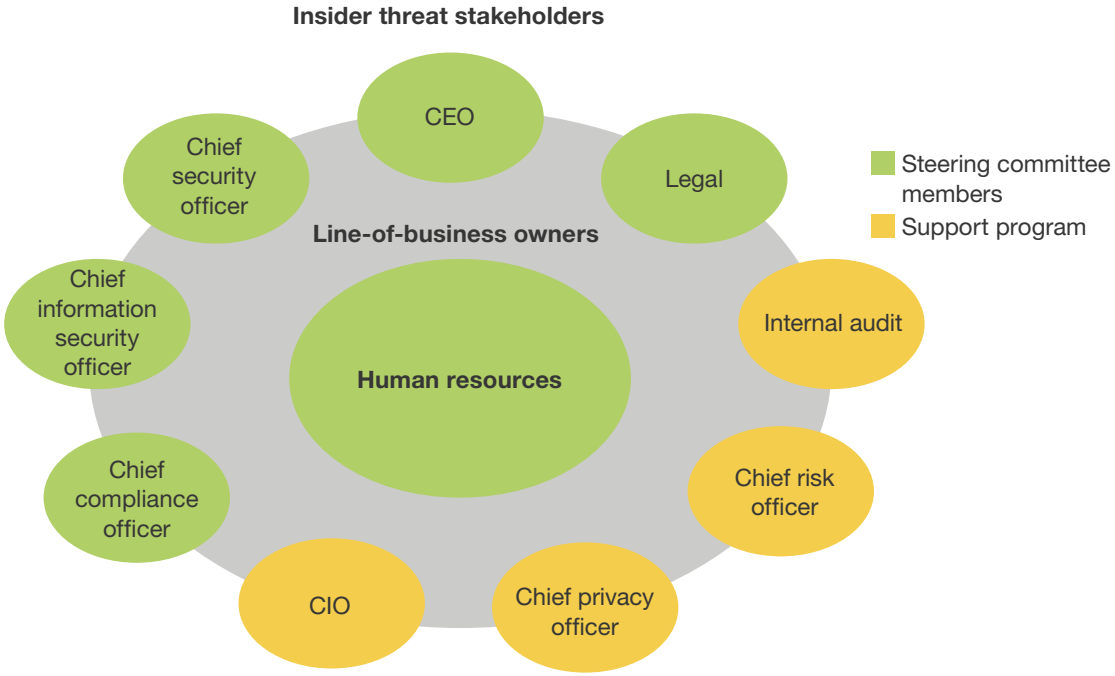
- **Build a separate insider threat team.** The team doesn't have to be large, but it does need to be focused on insider threat. Most teams are small, consisting of one to three people, in even the largest organizations.
- **Place the insider threat function outside the security team.** Insider threat 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. 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] You must 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.

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 management (TM). 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) or the CEO. 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



Build A Consistent Insider Threat Process

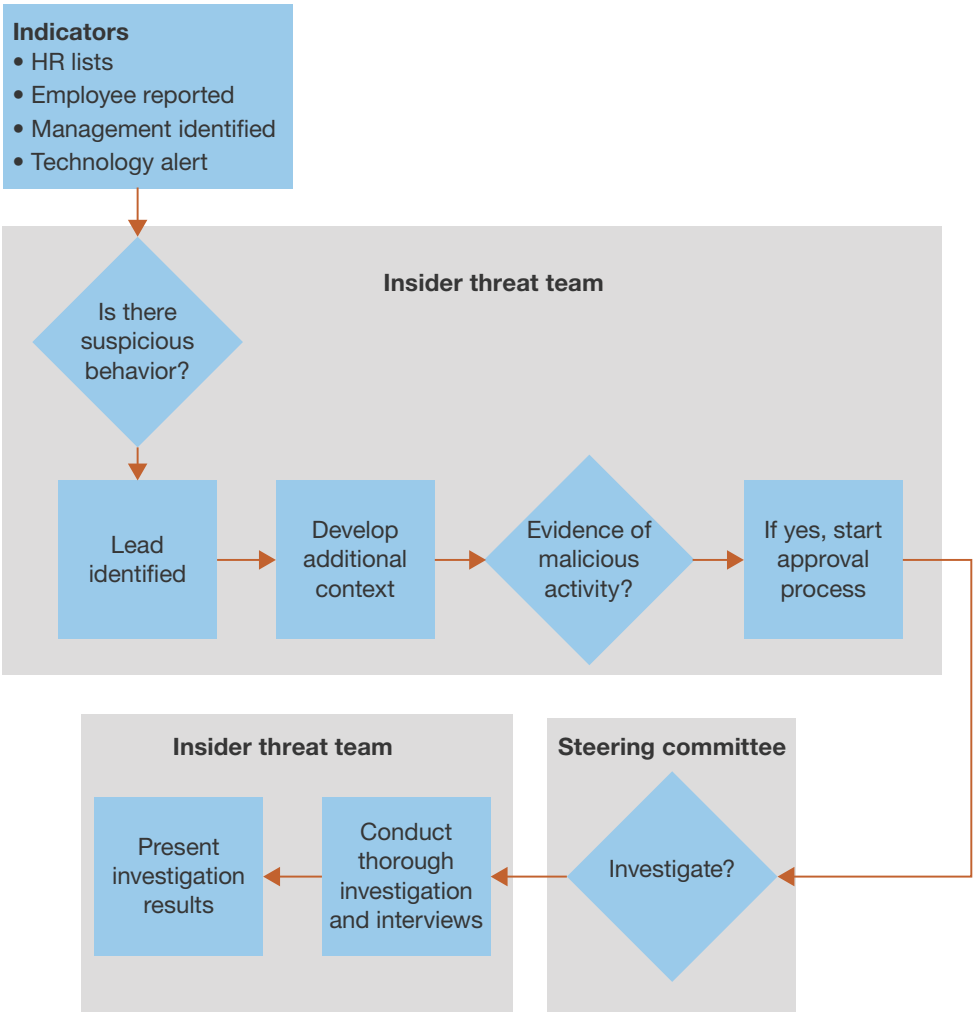
Consistency and fairness should be hallmarks of your insider threat program. Carefully consider how you determine when to start an investigation. HR, legal, compliance, and security are important functions in determining when to investigate an insider (see Figure 6). Establishing firm policies and processes 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 (AUP) for your computing devices and requiring users to sign the AUP 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 the decision to start an investigation has been made, treat the following steps in the process like a legal investigation. Even if you decide not to prosecute, having evidence that the process was followed 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 AUP.
- **Use technology to enable process.** Once your insider threat hunting process is established, choose technology tools that best fit your needs. Malicious-insider-hunting solutions like those offered by Lockheed Martin and Stroz Friedberg help insider threat analysts identify indicators that an insider may turn malicious. SUBA solutions like those from Interset, Niara, and RedOwl detect suspicious user activity.
- **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 forget contractors.** 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, especially Germany. Several of the professionals interviewed for this report cited problems launching programs 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 Lockheed Martin, 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 updates are required.

FIGURE 6 Forrester's Insider Threat Program Model



Make Your Employees Advocates For The Program

It may be difficult for your employees not to feel as if they are on an episode of *Person of Interest*, followed by cameras at every turn, but they 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.** Don't make the insider threat program a secret. Let the employees know you're watching and how the program works (in general terms).
- **Establish an 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. This is why it's so important to put process ahead of technology, and to involve teams like HR that understand culture building and employee motivation.[24] As employee satisfaction wanes, they may be more likely to commit fraud. Understand that security teams that treat users like machines will fail.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

Analyst Advisory

Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

Supplemental Material

Survey Methodology

Forrester's Global Business Technographics® Security Survey, 2015 was an online survey 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 the US from companies with two or more employees.

Forrester's Business Technographics provides demand-side insight into the priorities, investments, and customer journeys of business and technology decision-makers and the workforce across the globe. Forrester collects data insights from qualified respondents in 10 countries spanning the Americas, Europe, and Asia. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Companies Interviewed For This Report

Dtex Systems

Imperva

Interset

Lockheed Martin

Niara

ObserveIT

PwC

Stroz Friedberg

RedOwl

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. Security and risk (S&R) pros must eliminate the soft chewy center and make security ubiquitous throughout the digital business ecosystem — not just at the perimeter. To learn more, see the "No More Chewy Centers: The Zero Trust Model Of Information Security" Forrester report.

[2] Source: Forrester's Global Business Technographics Security Survey, 2015.

[3] Source: Jaikumar Vijayan, "IT contractor gets five years for $2M credit union theft," Computerworld, April 29, 2010 (http://www.computerworld.com/article/2517826/cybercrime-hacking/it-contractor-gets-five-years-for--2m-credit-union-theft.html).

[4] Source: "Grand Theft Data," McAfee (http://www.mcafee.com/us/resources/reports/rp-data-exfiltration.pdf).

[5] Source: Chidanand Rajghatta, "US jury fines TCS $940m for healthcare software 'theft,'" ETHealthworld.com, April 17, 2016 (http://health.economictimes.indiatimes.com/news/health-it/us-jury-fines-tcs-940m-for-healthcare-software-theft/51861855).

[6] Source: Dawn M. Capelli, 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: Jaikumar Vijayan, "Former DuPont worker gets 18-month sentence for insider data thefts," Computerworld, November 7, 2007 (http://www.computerworld.com/article/2539663/cybercrime-hacking/former-dupont-worker-gets-18-month-sentence-for-insider-data-thefts.html).

[8] Source: "Verizon 2016 Data Breach Investigations Report," Verizon (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2016).

[9] Source: Forrester's Global Business Technographics Security Survey, 2015.

[10] When Anthem (the nation's second largest health insurer) was breached, 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 Online, February 9, 2015 (http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html).

[11] Source: Forrester's Global Business Technographics Security Survey, 2015.

[12] 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).

[13] In one example, AT&T had a breach that involved insiders in the contact center who were stealing confirmation PINs in order to unlock stolen phones to then sell on the black market. For more information, see the "Lessons Learned From The World's Biggest Customer Data Breaches And Privacy Incidents, 2015" Forrester report.

[14] However, it's important to note 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 orgs doing 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," ObserveIT blog, June 2, 2016 (http://www.observeit.com/blog/what-nispom-conforming-change-2-all-you-need-know-updated).

[16] Security and risk (S&R) leaders are struggling to prevent data breaches, threats from malicious insiders, and fraud. Solutions for security user behavior analytics (SUBA) 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 information, see the "Market Overview: Security User Behavior Analytics (SUBA), 2016" Forrester report.

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

[18] The company's biggest adversary should not be itself. Focus on the real adversaries, and create a culture of data security and privacy among your workforce. To learn more, see the "Instill A Culture Of Data Security And Privacy" Forrester report.

[19] Legal rights to privacy in the workplace will keep evolving, and security monitoring of employees will require a regional approach. Forrester outlines seven principles to help craft an effective security strategy that respects employee privacy. For more information, see the "Employee Data Security And Privacy Matter More Than You Think" Forrester report.

[20] To learn how to define toxic data using the 3P + IP = TD model, see the "Rethinking Data Discovery And Data Classification Strategies" Forrester report and see the "Know Your Data To Create Actionable Policy" Forrester report.

[21] Although firms understand that privacy is important to the customer experience, few appreciate its importance to the employee experience. Yet, employee privacy contributes greatly to the quality of the interactions between employee and employer, and it affects employee job commitment, business performance, and, in the end, the customer experience, too. However, security teams struggle to balance the business, ethical, and regulatory requirements for employee privacy with the security benefits of monitoring employee activity. For more information, see the "Employee Data Security And Privacy Matter More Than You Think" Forrester report.

[22] In the television drama Person of Interest, a wealthy programmer has 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. To learn more, see the "Brief: Five Key Capabilities For Microsoft Office 365 Email Security" Forrester report.

[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. To gain that understanding and put it into practice, infrastructure and operations (I&O) professionals should use an approach Forrester calls "customer-obsessed workforce enablement" to rethink how to deliver technology to the people who drive the business. For more information, see the "Elevate Human Performance With Workforce Enablement" Forrester report.

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.