Insider threat

Employees, trusted contractors and other insiders can wreak havoc on an organization by exposing sensitive information or leaving the door wide open to cybercrime.

ebook
An SC Magazine publication

Insider threat

In the movies and in enterprise security, the most damaging attack on just about anything is an inside job, reports Larry Jaffee.

In science fiction, antagonists often morph into somebody they're not. Similarly, in cyber attacks, hackers typically disguise themselves enough so that no one would suspect the intruders don't belong. Undetected, these interlopers quietly wreak havoc.

The "inside job" constitutes the most insidious type of network breach because it's the worst kind of mistaken identity. Empowered by social engineering tactics that result in the divulgence of information, attackers cleverly mask themselves with privileged access. Inside attacks blur the lines between what's inside and outside. Hackers often make it through the pearly gates with help from authorized individuals who unwittingly get duped into being an accessory to the crime or without understanding they're on the wrong side of the law.

OUR EXPERTS: Inside threat

Sol Cates, CSO, Vormetric
Thomas Coughlin, president, Coughlin Associates
Bobby Ford, CISO, Exelis
David Geracioti, former editor-in-chief, Registered Rep
Avivah Litan, VP & distinguished analyst, Gartner
Raj Samani, VP & CTO EMEA, McAfee, part of Intel Security
Mike Tierney, COO, SpectorSoft

Internal attacks do not occur nearly as frequently as external, and they're harder to detect. In fact, in a SpectorSoft survey of 355 IT professionals last year, 75 percent of respondents admitted to insider crimes going unnoticed, 61 percent confided they couldn't deter such attacks, and 59 percent were not able to detect one. Those figures only tell part of the story: 35 percent admitted to suffering an insider attack.

Similarly, the "2015 Vormetric Insider Threat Report," a survey of more than 800 senior business managers and IT professionals, found that 34 percent of them were "very" or "extremely vulnerable" to insider attacks. Globally, 89 percent of the respondents saw their organizations being more at risk from insider attacks than outside.

"I hear statistics widely ranging that the insider threat is 30 percent to 70 percent to 100 percent," says London-based Raj Samani, VP and CTO EMEA at McAfee, part of Intel Security. "The truth is nobody really knows."

One of the reasons why the insider risk can't be better quantified is that the line can be blurred between who's inside and outside. "A lot of the outsiders are colluding with the insiders," says Avivah Litan, VP and distinguished analyst at Rockville, Md.-based Gartner. Subsequently, "insider threats are much more serious when they happen."

Sol Cates, CSO of Vormetric, a San Jose, Calif.-based provider of data security solutions, points out that 97 percent of the time it's a privileged account that gets abused. "From a risk perspective, I have to assume anybody is compromizable," he says.

Insiders come in various flavors, ranging from those with criminal intent to sell PII and credit card account numbers on the black market to absented-minded employees who lose a company-owned mobile device or forget to logout of their desktop at the end of the work day.

Too, personal crises can prompt previously honest people to fall prey to illegal acts. Or, unsatisfied workers can cross the line. Motivations of disgruntled employees run the gamut of losing out on a promotion to impressing a competitor with proprietary information to seal a new job, illustrated by two pending court cases.

Venture capital firm TPG Capital LP sued

78%
of employees surveyed are using their own personal device at work.

– Webroot, "Fixing the disconnect between employer and employee for BYOD," July 2014

its former managing director of global affairs, accusing him of extortion after being turned down for a partnership position. TPG claims he threatened to distribute damaging information to the media.

Lyft, a developer of a mobile phone ride-sharing app, filed a complaint against its former COO, alleging that he breached his confidentiality agreement and transferred sensitive company information to his personal Dropbox account before resigning. He's currently a VP at Lyft's competitor Uber.

Raj Samani, VP & CTO EMEA, McAfee

Exacerbating the situation, lax corporate cultures focused on hiring talented professionals, whether in IT or other departments, often contribute to insider vulnerabilities. Company policies must be laid down on day one being on the payroll. Yet, that's only the first step in an employee's lifecycle. At any point a circumstance could change the way an individual views a job.

There is no doubt of the challenges todays' enterprises face from employees going rogue. The consensus of the experts who we spoke with for this ebook is that the continual deluge of high-profile cyber attacks during the past year reinforces the need for organizations to be cognizant of risks under their roofs.

Monitoring: invasion of privacy?

Employee monitoring can flag errant behavior, as was the case last December when a Morgan Stanley employee allegedly siphoned account information of 350,000 wealth-management clients, some of which later was found on his home computer and an external website.

"It's very uncomfortable for companies to watch their employees," says Litan. "There's the creepy factor." Nevertheless, she suggests organizations use every kind of intelligence source one can get outside and inside. "It's really about continual identity assurance and continuous authentication. There are a lot of different data sources and you've got to put them together." Litan adds out that analytical tools acquired to catch outsiders also catch insiders as effectively.

From the employee perspective, many question whether monitoring is an invasion of privacy? Well, many say, that depends on location. In Europe, especially Germany, employers do not have the leeway that they do in the United States, for example.

The 2012 EU Data Protection Regulation redefines consent of individuals. No longer is it sufficient for consents to be "freely given, specific and informed." Instead, at least in Europe, consent must be "explicit" and evidenced by a statement or by a clear affirmative action. For a global organization, one HR policy size cannot not fit all, says Raj Samani, the London-based vice president and CTO, EMEA for McAfee, part of Intel Security.

"Very few people have an expectation of privacy in the [U.S.] workplace," says Mike Tierney, COO of SpectorSoft, a Vero Beach, Fla.-based firm which provides employee monitoring solutions. So, in addition to non-compete and non-disclosure agreements, as well as background and reference checks, it behooves employers as a best practices measure to let new hires know they'll be watching for unacceptable activity during office hours. Ultimately, such a policy is in employees' own interest because of the debilitating nature of a cyber hack, Tierney asserts. "The majority of people will say, 'That makes sense. You're telling me the boundaries.'"

Obtaining explicit consent helps employers pass legal muster in a wrongful dismissal suit, especially if things turn ugly and the

12%

of employees surveyed are using a device issued by their employer.

– Webroot, "Fixing the disconnect between employer and employee for BYOD," July 2014

Inside risk: The Snowden effect

How can an organization thwart a privileged insider with an agenda?

Edward Snowden reportedly hacked into the National Security Agency's systems to steal the answers to the agency's admissions test and used his stellar performance on the test to attract an offer from the NSA and then, ultimately, from Booz Allen. He subsequently released troves of data exposing inner workings of several government agencies.

Such "people with a cause" might consider themselves whistleblowers or what SpectorSoft's Mike Tierney refers to as "insider activists." In any case, they are out to embarrass or damage an entity's reputation, or expose what they consider to be a major injustice.

Sol Cates, CSO, Vormetric

The U.S. Office of Personnel Management, an independent agency of the government that manages the civil service of the federal government, administers honesty and integrity tests that do not eliminate the potential for dishonesty or theft at work, the feds admits. An overt or clear-purpose integrity test is designed to directly measure attitudes relating to dishonest behavior, and often contains questions that ask directly about the applicant's own involvement in illegal behavior or wrongdoing. The test's shortcoming is that the jobseeker's private thoughts and feelings may not be revealed. Some clever applicants might be able to fake or distort test scores in their favor. Nevertheless, an integrity test typically is given to someone whose job performance requires a high level of honesty. So how effective are psychological tests in rooting out potential insiders?

"That's a good question," says Vormetric CSO Sol Cates. Typical vetting, such as background, reference and credit checks, even polygraph tests, are great indicators of past history. "But it does nothing to mitigate what their future behaviors, endeavors or motives might be," notes Cates. "It's not 100 percent foolproof. You can't predict someone's intentions or how they might change in the future."

Once Snowden hit the news, defense contractor Exelis expanded monitoring capabilities, says Exelis CISO Bobby Ford. "It wasn't necessarily because of Snowden, but it didn't hurt. He was a malicious insider who had privileges. So we started looking at who had privileges and who needs to have those privileges."

company needs to prove removed data had nothing to do with his or her job, notes McAfee's Samani.

Employers need to be direct. "It is company information, not employees' information," Vormetric's Cates points out. Further, the policy should insist that office computers may not to be used for personal matters. "From a security standpoint, that's pretty standard practice. Put a rule in place that all activity should be only for corporate, not personal business."

If an organization allows employees to use the company's computers for personal matters, such as online banking, Tierney notes a company focused on maintaining employee privacy can take simple steps, such as not recording employees' online banking sites.

Whose data is it?

In the mid-2000s, financial advisers on Wall Street were jumping to competitor investment

70%

of employee devices only have the security installed when the device was purchased.

– Webroot, "Fixing the disconnect between employer and employee for BYOD," July 2014

banks for bigger salaries, commissions and even signing bonuses, or setting up their own shops, says David Geracioti, editor-in-chief of *Registered Rep.*, a trade magazine for financial advisers, which in 2012 became known as WealthManagement.com.

> “How do you stop an individual who’s determined to leave your organization with sensitive data to which they previously had access?”
>
> *– Bobby Ford, CISO, Exelis*

“They were poaching each other’s advisers,” Geracioti says. Of course, when the brokers and other financial professionals left the premises, so did their customer lists, much to the chagrin of the jilted bank. His magazine covered a bunch of court cases related to taking client lists.

Something of a self-regulatory agreement was struck. The banks recognized a truce was in their mutual interest. Only names, email addresses and phone numbers of clients could be taken, but not account numbers or the monetary value of holdings.

Bobby Ford, CISO, Exelis

In any industry, salespeople generally have a sense of entitlement to the client lists they develop and consider their property and not the company’s. “If you put a lot of effort, time and skills into building up a client base in a territory and bring in new business, salespeople very naturally view those contacts, those relationships as theirs,” notes Tierney. Coders feel the same way, he adds. “They have a sense of entitlement to their work product. A lot of times, that is a motivating factor if they’re getting ready to change jobs. They’ll say, ‘That’s as much mine as the company’s. I’m going to take it with me.’”

It’s probably too late to prevent the loss. Bobby Ford, CISO of defense contractor Exelis, a McLean, Va.-based supplier of GPS satellite technology, says it takes a “herculean effort” to protect data from an employee who has a new gig lined up. “How do you stop an individual who’s determined to leave your organization with sensitive data to which they previously had access? You want individuals to give you prior notice, a heads-up they’re leaving. They haven’t just found out two weeks prior, they’ve always known.”

It’s not just the individual who is leaving, but all the parties the employee interacted with during his or her tenure who could potentially leave an organization vulnerable to an attack. When an employee is decommissioned – either terminated or by the employee’s choice – a complete account shutdown is necessary.

Passive or active monitoring?

Software can log every keystroke, but what good is that if no one is reviewing reports? Organizations must classify their most important data and protect with encryption, etc., as well as monitor employee access of those files. “Most organizations are very poor at auditing at what’s actually happening,” says Vormetric’s Cates.

Passive monitoring collects and stores all relevant information. But the data is not actively reviewed because there is no known cause to do so yet. However, you might want to take a look at what “Joe” has been doing when he resigns.

Thousands of keywords and phrases used in emails could indicate individuals engaged in unauthorized activity. When phrases like

98%

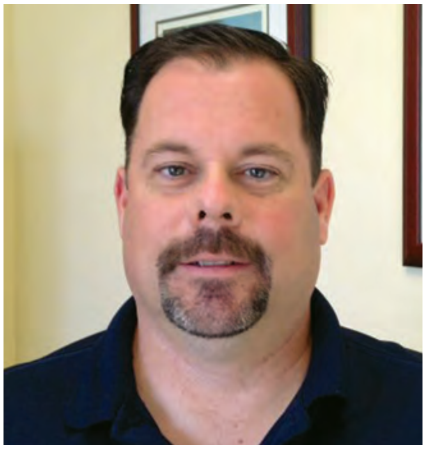
of employers have a mobile security policy in place for access to corporate data.

– Webroot, “Fixing the disconnect between employer and employee for BYOD,” July 2014

Writing on the wall: Anticipating a problem

You'll probably want to keep a closer eye on an unhappy or disgruntled employee, whose unhappiness could be triggered by layoffs, resulting in additional work.

Here's another typical scenario: A salesperson is given a poor annual review, or repeatedly not hitting a monthly quota, prompting a 30- to 60-day "plan" to improve.



Mike Tierney, COO, SpectorSoft

"That's a pretty clear indicator to the sales rep that the time with the company may be coming to a close," notes SpectorSoft COO Mike Tierney. Seeing the writing on the wall, the employee typically starts pulling customer lists for his or her next career move.

Tierney thinks the best way to nip a potential inside job in the bud is to work closely with human resources. "HR is an incredible source of people's personal circumstances." For example, he explains, HR knows this fictional Joe is taking hardship loans against his 401K, or payroll receives notices that a garnishment has been placed on somebody's paycheck. "They can see signs of financial strain, such as a divorce. We know a change in financial situation can change their behavior. It's a precursor to an insider threat."

HR can then say to IT, "I can't tell you why, but there's a higher risk associated with Joe, and we need to keep a closer eye on him for a while," Tierney says.

"gray area" or "hold the quarter open" are used very infrequently and then all the sudden spike, an alert is triggered, suggesting active monitoring of a particular person, SpectorSoft's Tierney explains.

As well, a CRM system that shows a vast amount of downloads could indicate an employee's intention to depart, notes McAfee's Samani, especially if the records are beyond the normal job profile.

For her part, Gartner's Litan believes that organizations must be continually vigilant in surveillance at the desktop and network levels. "Good people go bad over time and they have financial difficulties and they go crazy," she says. "Security clearances don't mean anything three months after you get them."

At Exelis, Ford says, employees are fully aware they're being monitored. "There's a fine line between privacy and security," he admits. "We carefully navigate that line. We make our security program as transparent as possible," he says. The program has approval of HR and general counsel. Employees are notified about monitoring enhancements. "We let them know some things we weren't catching, but we can now," Ford says.

BYOD: A weak link?

One way for organizations to minimize the insider risk is to not allow employees to use their own devices for their jobs. The Vormetric study found that 38 percent of respondents believed personal mobile devices presented "a high risk area of concern." Meanwhile, Webroot's July 2014 study, "Fixing the disconnect between employer and employee for BYOD," found only 19 percent of employees installed a full security app and 64 percent of them used only the security features that came with their devices. Subsequently, 95 percent of companies expressed

89%

of companies surveyed feel at least somewhat vulnerable to insider attacks.

– 2015 Vormetric Insider Threat Report

concern about security risks from employees' personal devices.

Exelis doesn't support BYOD, notes Ford. Access controls curb such activity. "We're not oblivious to the fact that individuals work on proprietary documents or information from their personal devices. We're able to kick them off immediately," Ford says. Exelis also prohibits employees from employing their own IT, such as DropBox for storage, or emailing company documents to a Gmail or other personal email account.

Thomas Coughlin, president, Coughlin Associates

"We try to have the mindset: What if an individual has access to data everywhere all the time," Ford says, adding that company-provided devices allow Exelis employees to work remotely.

McAfee recently studied BYOD and found 78 percent of respondents used their own devices at work, of which 77 percent felt "very confident" or "confident" their employers took all the necessary steps to protect all the data. Nearly two-thirds thought it was IT's responsibility for protecting personal data on work devices.

Cloud: weak link?

With the trend of organizations using third-party cloud providers, could that be another potential weak link to inside threats? The 2014 Ponemon survey, "Privileged User Abuse and the Insider Threat," commissioned by defense contractor Raytheon, found that 38 percent of the 693 respondents thought cloud-based applications were most at risk, an increase from 35 percent in 2011.

Thomas Coughlin, president of Coughlin Associates, an Atascadero, Calif.-based data storage consultancy, points out that cloud service provider agreements specify data protections. Customers are highly segregated on different servers to minimize the chance that one client, or interloper, could look at someone else's files. Some cloud services will encrypt data for another level of security. Firewalls and key management providing further barriers to prevent data getting into the wrong hands are becoming more common for enterprise applications.

"If it can be hacked, that's always a possibility, so you can't totally discount it either," Coughlin says. He hasn't heard of any cloud providers being implicated in a breach. "Knock on wood, but it doesn't seem rampant." Outsourced suppliers generally take more measures than internal IT because their reputations are at stake, he adds.

As a best practice, Cates suggests organizations use "slightly different" controls, depending on the stakeholder, such as cloud vendor, only exposing them to data they need to provide the service.

SpectorSoft's Tierney says the Snowden episode serves as a wakeup call that a lot of people have way too much access to privileged information. In large organizations, he asks, should the executive team have access to everything in the corporation? "Maybe not." However, it is oftent the case that the nature of an administrator's job requires universal access to even sensitive data.

More and more organizations see administrators as potential risks to outside attackers," notes Cates. "The key is removing them from the equation."

Awareness not enough

Most employees are honest and thankful for their jobs in a tough economy. But, psychological triggers still can leave an organization vulnerable – even if they tell employees not do certain things.

"Awareness doesn't work," declares McAfee's Samani. "All the biggest hacks

92%

of companies surveyed are looking to increase or maintain existing spending on IT security and data protection.

– 2015 Vormetric Insider Threat Report

always use social engineering to attack the subconscious of the individual." He cites the 2005 Carronade project undertaken by the United States Military Academy at West Point, whose more than 400 cadets were given four hours of training to not click on virus-embedded hyperlinks and email attachments they received from people they did not know. The result: despite the instruction, 80 percent of cadets – 90 percent of freshman – clicked on the embedded link of an email message that appeared legit.

> "All the biggest hacks always use social engineering..."
>
> *–Raj Samani, VP & CTO EMEA, McAfee, part of Intel Security*

Ford notes that Exelis' patch management program protects the network if employees "do something stupid," such as click on a link containing malware.

Summing up, internal attacks tend to be extremely damaging because culprits have permission for access to the most sensitive data, notes SpectorSoft's Tierney. "They know what they're doing and what they're looking for. And they've already defeated security."

Samani agrees. "What most people don't recognize is that any organization is just simply one click from compromise." ■

For more information about ebooks from SC Magazine, *please contact Illena Armstrong, VP, editorial, at illena.armstrong@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, sales, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

7%

of companies surveyed said they felt safe from insider threats.

– 2015 Vormetric Insider Threat Report

Sponsors

Centrify

Centrify provides unified identity management across cloud, mobile and data center environments. Centrify solutions deliver single sign-on (SSO) for users, privilege management and auditing for security and compliance, and a simplified identity infrastructure for IT. Centrify User Suite provides a single Active Directory- or cloud-based login to corporate resources, including mobile devices, Macs or cloud apps like Office 365, Salesforce.com and WebEx.

For more information, visit www.centrify.com

HP Enterprise Security is a leading provider of enterprise security solutions designed to mitigate risk and defend against today's most advanced threats. With market-leading products, services and innovative research, HP Enterprise Security product enables organizations to take a proactive approach to security, integrating information correlation, application analysis and network-level defense.

For more information, visit www.hpenterprisesecurity.com.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
ASSOCIATE EDITOR Teri Robinson
teri.robinson@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com
PRODUCTION MANAGER Krassi Varbanov
krassi.varbanov@haymarketmedia.com

SALES
VP, SALES David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
REGION SALES DIRECTOR Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

Secure and Manage Privileged Identities

Centrify provides a unified solution for securing and managing privileged users' identities. Centrify leverages an organization's existing identity infrastructure to enable identity consolidation, privilege management and auditing for security and compliance, and a simplified identity infrastructure for IT.

Identity consolidation

- Rapidly consolidate user identities into Active Directory
- Reduce TCO vs. managing fragmented identity silos

Privilege management

- Control access and granularly manage privileges
- Increase security and prove compliance by implementing a least-privilege model

Privileged session monitoring

- Eliminate anonymous activity and audit privileged sessions
- Reduce compliance costs with robust access and activity reporting

Centrify®

Free trial: www.centrify.com/free-trial

Learn more: www.centrify.com/resources

Change your view of security with instant clarity into threats.

HP ArcSight. Understand the threat potential of every event across your organization. HP ArcSight analyzes the broadest set of data sources, such as log data from devices on premise or in the cloud. Then it prioritizes events based on risk level, and displays them on a customizable dashboard to turn data into actionable intelligence. So you can get to bad guys before they get to you. Learn more at **hp.com/go/ArcSight**

Think like a bad guy.