

Insider threat

Whether malicious or unintentional, the risk from employees – on premises or contracted – continues to pose challenges for business operations.

ebook
An SC Magazine publication

Sponsored by

 **Symantec.** | Website Security Solutions

The accidental threat

A laggard economy and the promise of rich reward can tempt employees to cross the line...and then there are those unintentional consequences from a staffer mishandling assets, but there are procedures and technologies that can alleviate the threat, reports Stephen Lawton.

While Edward Snowden's release of National Security Agency documents last year and Army Pvt. Bradley (Chelsea) Manning's 2010 leak of classified military documents and videos relating to the war in Iraq have made headlines, most incidents resulting from insider disclosures or abuse never draw attention. That may be changing, however. Likely owing to greater recognition of insider threats and compliance fines being increased for data breaches, insider attacks are moving to the forefront of corporate risk assessments.

The reality of insider threats is that not all attacks are done for political purposes or financial gain, although these motives certainly are part of the mix. In many cases, the damage from an insider is due to negligence, or sometimes a staffer carrying out an "attack" might not even be aware of what they are doing.

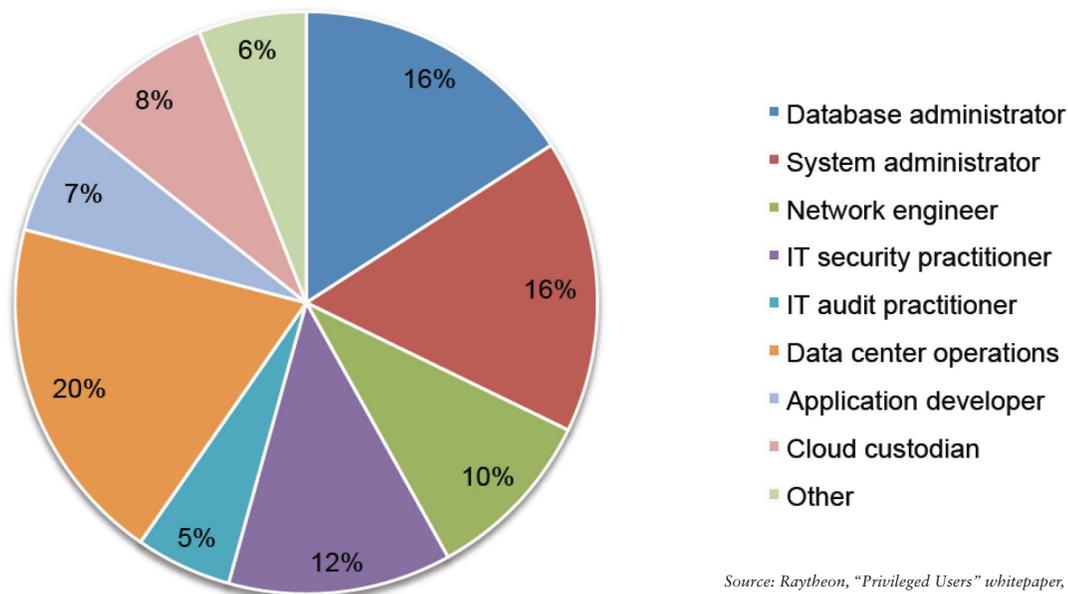
Whether malicious or not, Terry Jost, partner and principal at Ernst & Young, recommends that companies have strong internal controls that assume an insider attack is imminent. "You have to plan as if an attack will occur," he says. In order to do this effectively, an incident response plan is required.

First, Jost recommends that data be assigned a risk classification and that rules be written for each classification level. As data is expanding at an exponential rate, he says, it is essential that the business side of the enterprise understands the value of the data being created and assign a value so that resources can be expended appropriately to protect the most valuable data.

Second, he says, access to data needs to be monitored based on the rights of the employees. Generally speaking, he says, some 25 to

Who are *privileged users*?

Examples of jobs that have privileged user status.



Source: Raytheon, "Privileged Users" whitepaper, 2014

13%

of breaches resulted from privilege misuse and abuse.

– Verizon, "2013 Data Breach Investigations Report"

Insider threat

\$348B

a year in corporate losses can be tied directly to privileged user fraud.

– Raytheon, “Privileged Users” whitepaper, 2014

35 percent of employees have “inappropriate access” to data, creating risks and opening the company to a potential accidental insider breach based on these workers using their valid credentials to access data to which they should not be privy.

Next, he says, companies need to manage special cases and exceptions. For example, an employee who generally does not need access to certain data might be filling in for someone on vacation. If the special access is unmonitored, the employee with temporary access needs to have that privilege removed when the special case no longer exists. Problems arise, Jost says, when the temporary rights granted to employees is not revoked when the special circumstance ends, effectively making those rights permanent.

Randy Trzeciak, manager of the Community Emergency Response Team (CERT) Insider Threat Center, notes that some internal vulnerabilities are due to users being provided with authorized access to sensitive data for which they have no business reason for that access. An example might be an employee in manufacturing who has access to internal documents for the human resources department not needed for the manufacturing job. Because data has various levels of confidentiality, users only should be given access to data they require to do their jobs, he says.

Tools may or may not help

Defensive data security tools, such as data loss prevention (DLP) applications, will not identify a potential vulnerability if the

employee is whitelisted as a trusted user for sensitive material, even if they have no reason to access that data. Network managers need to ensure that users, be they direct employees or business partners with access to the internal network, have the appropriate rights and privileges on the network. A potential result of a user having inappropriate access to data is a successful phishing or social-engineering attack that provides the attacker with credentials their target should not have had.

Another potential possibility is that the stolen

credentials will give the criminal credentials that allow them to access a poorly designed network, giving them access beyond what the original credentials intended.

Companies that rely strictly on perimeter security tools to keep non-employees out of their networks are leaving gaping holes in their security as software as a service (SAAS), corporate partners and out-sourced IT services

“expand the boundaries of insiders” well beyond the corporate network, Trzeciak says.

Organizations need an internal service-level agreement (SLA) that defines who has access to what data, what data protection strategy is in place, what are the data-disposal policies and procedures, and how is this SLA going to be audited to ensure network security, he says.

While Trzeciak notes that only trusted employees should have access to sensitive data, verifying *who* is a trusted employee must be assessed on a regular basis.

Another major challenge network managers face today is the introduction of personal devices to the workplace, says Daniel Garrie,

Our experts: *Inside straight*

- **Ray Cavanagh**, VP at CGI Crescent Guardian Security; council member of the American Society for Industrial Security
- **Eric Cole**, fellow with the SANS Institute; founder and chief scientist at Secure Anchor Consulting
- **Michael Crouse**, director of insider threat strategies, Raytheon Cyber Products
- **Daniel Garrie**, executing managing partner, Law & Forensics
- **Terry Jost**, partner and principal, Ernst & Young
- **Randy Trzeciak**, manager, Community Emergency Response Team (CERT) Insider Threat Center

executing managing partner of Law & Forensics, a law firm that specializes in cyber security, digital forensics and e-discovery. He also is special counsel to law firm Zeichner Ellman & Krause. The bring-your-own-device (BYOD) trend opens up a variety of inherent risks, including web-based services and third-party vendors whose employees essentially become corporate insiders.

One of the biggest risks from BYOD is that the network manager often does not know what devices are attaching to the network, and therefore cannot necessarily build in pro-

“Is this owned by audit, security or IT?”
– Eric Cole,
Secure Anchor Consulting

tections. The company needs to have a terms of service agreement with all its employees and contractors that outlines the company's rights to wipe corporate data from personal devices, he says, as well as requiring employees to identify the personal devices they bring into the company.

It might not engender good will with the workforce, he says, but if an employee leaves the company, IT administrators need a way to ensure they can eliminate any potential corporate data from that worker's personal device. Former employees are unlikely to bring in their personal devices for their ex-employer to evaluate and current tools on the market do not sufficiently protect the company to do selective wipes.

That said, how can a company do comprehensive wipes of personal devices if it does not know what devices are connected to the network, he posits. As a general counsel, Garrie says, one of the issues that keeps him up at night is what happens if an employee loses a mobile device with unencrypted corporate data and they never tell the IT department. Executives who lose tablet computers

and smartphones, or former employees who leave logic bombs in their company-owned devices, also are a major concern for the legal department, he says.

Another problem that can occur when an employee leaves a company is that there is a lag between human resources separating with the employee and IT deactivating the employee's accounts. To prevent an occurrence, companies should have a “playbook” that lists all of the policies and procedures for employee separation for each stakeholder, such as the HR department, department managers and IT.

If the company knows in advance that an employee will be separated for reasons that might involve a potential vulnerability to the company, there are actions that should be taken in advance, Garrie says. For example, if a company plans to release an employee for inappropriate behavior, the IT department should monitor the employee's activity before he/she is released. This could provide insights into whether the staffer was accessing data to which they did not have rights. In cases where the employee is accessing data to which they did have rights, this monitoring could identify if they are downloading or printing out data that is sensitive or confidential.

Too, companies should have policies to begin monitoring an employee's network activity as soon as any issue shows up that could indicate a risk. Not only can monitoring the employee identify any possible breaches, it also can verify if the employee was acting appropriately with the data entrusted to them. Monitoring also can identify if a user is accessing data – with valid credentials – to which they should not have access. This could point to a problem with how credentials are approved and assigned, rather than indicate a possible breach or malicious intent.

The other guy

A fundamental error that companies tend to make *before* they realize they've been breached is that attacks happen to others, not to them, says Eric Cole, a fellow with the

64%
of privileged users believe they are empowered to access all the information they can view.

– Raytheon,
“Privileged Users”
whitepaper, 2014

Step one: *Classifying data*

It is a truism in information security that not all data is created equal. Press releases, data sheets and historic financial filings with the Securities and Exchange Commission that are in the public domain do not need the same security precautions as engineering drawings, customer databases or personally identifiable information of employees.

One popular best practice for identifying which data requires additional security controls and which does not is data classification, defined by the National Institute of Standards and Technology (NIST).

The NIST approach builds a grid that lists the potential impact of a breach on the X axis as low, moderate or high. The Y axis addresses security objectives of confidentiality, integrity and availability. As data is created, the standard recommends, it should be classified as to what the impact will be for each objective. The company then can build in security controls based on where the data falls in the matrix.

While there is general agreement that data can be classified as public (lowest level of risk), private (moderate level of risk) and restricted (greatest level of risk), *how* the classification is done can be a challenge. Additionally, experts agree that in order to take full advantage of this matrix, all data must be classified. However, in large or older companies where large amounts of legacy data exists, going back and classifying it all can be problematic.

Michael Crouse, director of insider threat strategies at Raytheon Cyber Products, says companies need specific guidelines to define how data is classified, and each employee who creates data needs to have a copy of the guidelines and training. A stakeholder on the data – be it legal, technical, financial, human resources or any other department – needs to approve how the data is classified so that there is consistency across all employees.

He says one approach a company can take is to have separate physical hard drives for the different levels of security required. Tools are available that can generate a hash of each document. An audit tool can then track the hash and follow the document throughout the network – identifying who gets access to the file – and then determine if they modify, email or print the document. If the document is confidential or otherwise should not be accessible to that individual, it could identify a possible insider threat.

SANS Institute and the founder and chief scientist at Secure Anchor Consulting in Reston, Va. Often, he says, the breaches are non-malicious and due to errors and omissions rather than a malicious attack by a criminal employed by the company.

Data breaches are not really a growing threat, he says. Rather, we're just becoming more aware of these events. Companies can purchase insurance against insider breaches, but Cole says many IT executives do not even know what the details of the insider breach insurance covers, even if they have it.

Cole cites three root causes of breaches by insiders: lack of asset management, lack of

configuration controls, and lack of change management controls. If these three basic security precautions are in place, the majority of non-malicious insider attacks could be stopped. However, he says, often the reason for these issues falling through the cracks is because no one takes ownership. "Is this owned by audit, security or IT?" he asks.

Like Garrie, Cole says when it comes to information security this need to be spelled out in detail in a playbook that specifies who within the company is responsible for what.

Security is not a metric used by the operations staff to determine their performance, Cole notes. While these issues are IT-related,

\$22B

in fines meted out to financial institutions by U.S. regulators in 2012 for breach violations.

– Raytheon, "Privileged Users" *whitepaper*, 2014

Insiders: Less obvious risks

In January, the CERT Insider Treat Center, in conjunction with Carnegie Mellon University, prepared an exhaustive report for the Department of Homeland Security, titled “Unintentional Insider Threats: Social Engineering,” addressing threats that are created without necessarily a malicious intent.

According to the report, some organizational factors can increase the likelihood of human errors (i.e., lapses in judgment) at the employee level:

- Poor management or management systems that may fail to assign sufficiently qualified personnel to tasks or that provide employees insufficient materials and resources;
- Inadequate information security systems or policies; and
- Work environments or work planning and control systems that impact employee satisfaction or cause stress or anxiety. Many human factors variables have also been identified as more immediate causal factors: lack of attention or lack of knowledge, which often cause people to ignore security cues, and a tendency to focus disproportionately on urgency cues.”

The report also stated: “Organizational factors can produce system vulnerabilities that adversaries may exploit in social engineering attacks. Management systems or practices that provide insufficient training, inadequate security systems and procedures, or insufficient resources to successfully complete tasks may promote confusion, reduce understanding, and increase employee stress, all of which increase the likelihood of errors or lapses in judgment that enable the attacker to successfully breach defenses.”

the IT director is more focused on making sure all systems are up and running effectively so that business can be done. In fact, security could work against an IT department’s measurable metrics by making access to sensitive data slower and more cumbersome.

The same is often true for physical security, he says. The IT team focuses on keeping attackers out of the computer systems, but tends to focus less on the physical security of the systems. Someone else is often responsible for the physical security of the building, although Cole characterized the physical security in some companies as trivial.

Ray Cavanagh, vice president at CGI Crescent Guardian Security and council member of the American Society for Industrial Security (ASIS), agrees that lack of physical security is a contributing factor to non-malicious insider threats. It is far easier to penetrate a network from within a company than from outside.

Radio frequency identification (RFID) badges, proximity badges and biometrics are

all tools that can be used to protect sensitive data from employees who do not require access to systems that can access this information, he says. Software controls that stop the inadvertent download of sensitive material to flash drives or the inclusion of such data as an email attachment also can stop many non-malicious insider threats.

Analytics that can identify when a user is taking an action that is outside their normal activities also can help identify if an insider’s credentials have been stolen, he says. An employee who lives in the U.S., for example, should not be identified as downloading data in the middle of the night from Asia.

Some basic physical security protocols, such as not writing down login names and passwords on Sticky Notes and then putting them under the keyboard, need to be enforced, he says. Today, passwords are used for so many websites and applications that it is becoming virtually impossible for users to remember so many different login creden-

42%
of IT practitioners
believe the threat will
continue to grow.

– Raytheon,
“Privileged Users”
whitepaper, 2014

tials. Simple password security applications that store encrypted passwords can eliminate a major physical security vulnerability, Cavanagh says.

Embedded applications also can be a vulnerability leading to an unintended breach, he says. Some devices, such as smartphones and tablets, will look for Wi-Fi connections automatically and can transfer data to or from the device without the user specifically authorizing the transfer. And sometimes, he adds, users who purchase new devices and recycle the old device, either by giving it to another family member or donating the device, could transfer confidential data without realizing it.

Creating technical observables

Michael Crouse, director of insider threat strategies at Raytheon Cyber Products, says companies need to understand their workforce in order to better understand what a potential insider threat is and what might be something innocuous. By building a baseline of employees' activity over time that shows how they normally access their workstations, the company can determine if an action represents normal activity, uncommon but approved activity, or perhaps something more sinister. He calls this creating technical observables.

An important part of determining appropriate behavior for users is identifying what credentials are approved for a given user as well. While monitoring the user's activity will show what resources the user accesses, auditing the company's applications and user privileges will determine what resources the user is authorized to access. Sometimes, he says, there is a disconnect where a user might have more authorized privileges than they require.

A layered security approach that might include data loss prevention software along with endpoint security tools, multifactor authentication and multi-employee authentication can help a company develop a defense that limits accidental or unauthorized access, Crouse says. No single tool can be pro-

grammed to meet all the variables, he adds, and companies should delay purchasing new security tools until they have completed a full risk assessment and understand where their vulnerabilities lie.

Analysis of network activity likely will provide nuggets of information that alone might not indicate a threat, but when combined with other tools can build a profile of a threat, he says. While there are products that can provide out-of-the-box rules, companies normally need to tailor the rules to meet their company's specific needs.

Crouse agrees with Cole that asset management, configuration control and change management are essential legs for the data security stool, but he adds one more leg to add stability: auditing. The audit trail is essential in making sure that the asset management, configuration controls and change management are all working the way they must. "It's trust, but verify," he says.



It's trust, but verify."

– Michael Crouse,
Raytheon Cyber Products

As companies begin focusing on insider threats, they could tend to lose focus on external threats, he says. However, insider breaches are exponentially greater than the threats from outsiders. So, rather than focusing efforts more on insider or outsider threats, he says, companies need to maintain a balanced approach.

While acknowledging that no company is going to be 100 percent secure all of the time, the key to building the most secure environment is to start at the center of the network and build a business case for preventing insider and outsider threats. While there is often pressure from management to buy something to make sure the network is safe, "companies jump in too quickly and don't do their due diligence up front," Crouse says.

14%

of breaches are
perpetrated by insiders.

– Verizon, "2013 Data
Breach Investigations
Report"

“There’s too much pressure to *do something*.” By asking the right questions up front, companies can identify their particular needs and can better identify the types of tools that will address those needs.

The size of the company should not be a defining factor to the potential risk, he notes. “Insider threats are not contained to large companies or government.”

According to published reports, the breach at Target was launched through credentials stolen from a service provider, Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and heating, ventilation and air conditioning (HVAC) systems. The *Wall Street Journal* and Reuters reported that the Secret Service is investigating that claim.

The company, which according to the

website InsideView has revenues of \$70 million and 60 employees, falls into the category of small to midsize company. If Fazio Mechanical does turn out to be the source of the stolen credentials, one question its internal investigation likely will look at is whether the stolen credentials were lost due to a malicious attack designed to steal company secrets or if it was due to an accidental loss of sensitive data.

Regardless of the result, it will mark another attack on a Fortune 500 company from one of its SMB business partners – effectively a trusted insider. ■

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



Protect your website and grow your business. Symantec Website Security Solutions include industry-leading SSL, certificate management, vulnerability assessment and malware scanning. The Norton™ Secured Seal and Symantec Seal-in-Search assure your customers that they are safe from search, to browse, to buy.

For more information, visit www.symantec.com/ssl-certificates

Sponsor

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
ASSOCIATE EDITOR Teri Robinson
MANAGING EDITOR Greg Masters
DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
PRODUCTION MANAGER Krassi Varbanov

SALES
VP, SALES David Steifman
REGION SALES DIRECTOR Mike Shemesh
WEST COAST SALES DIRECTOR Matthew Allington
ACCOUNT MANAGER Dennis Koster
SALES/EDITORIAL ASSISTANT Ashley Carman

Not all SSL certificates are the same.



We have the Internet's most trusted mark.

Symantec™ Website Security Solutions include industry-leading SSL, certificate management, vulnerability assessment and malware scanning, Express Renewal, and 24x7 support. The Norton™ Secured Seal and Symantec Seal-in-Search assure your customers that they are safe to search, to browse, and to buy. With 100 percent uptime since 2004, military-grade data centers, and industry-leading SSL, Symantec is the leading provider of website security for your business. Call (866) 893-6565 or visit www.symantec.com/ssl-certificates to learn more about Symantec Website Security Solutions.

Confidence in a connected world.

