HBR.ORG
Harvard Business Review
SEPTEMBER 2014
REPRINT R1409G

The Danger from Within

The biggest threat to your cybersecurity may be an employee or a vendor.

by David M. Upton and Sadie Creese


P*SSW*RD

ILLUSTRATION: DALE EDWIN MURRAY

David M. Upton is the American Standard Companies Professor of Operations Management at Oxford University's Saïd Business School.

Sadie Creese is the professor of cybersecurity at Oxford and director of its Global Cyber Security Capacity Centre. Upton and Creese are principal investigators in the Corporate Insider Threat Detection research program.

THE DANGER FROM WITHIN

The biggest threat to your cybersecurity may be an employee or a vendor.

by David M. Upton and Sadie Creese

We all know about the 2013 cyberattack on Target, in which criminals stole the payment card numbers of some 40 million customers and the personal data of roughly 70 million. This tarnished the company's reputation, caused its profits to plunge, and cost its CEO

and CIO their jobs. What's less well known is that although the thieves were outsiders, they gained entry to the retail chain's systems by using the credentials of an insider: one of the company's refrigeration vendors.

Target's misfortune is just one recent example of a growing phenomenon. External attacks—pervasive intellectual-property hacking from China, the Stuxnet virus, the escapades of Eastern European gangsters—get plenty of attention. But attacks involving connected companies or direct employees pose a more pernicious threat. Insiders can do much more serious harm than external hackers can, because they have much easier access to systems and a much greater window of opportunity. The damage they cause may include suspension of operations, loss of intellectual property, reputational harm, plummeting investor and customer confidence, and leaks of sensitive information to third parties, including the media. According to various estimates, at least 80 million insider attacks occur in the United States each year. But the number may be much higher, because they often go unreported. Clearly, their impact now totals in the tens of billions of dollars a year.

> "The best way to get into an unprepared company is to sprinkle infected USB sticks with the company's logo around the car park."

Many organizations admit that they still don't have adequate safeguards to detect or prevent attacks involving insiders. One reason is that they are still in denial about the magnitude of the threat.

Over the past two years we have been leading an international research project whose goal is to significantly improve the ability of organizations to uncover and neutralize threats from insiders. Sponsored by the Centre for the Protection of National Infrastructure (CPNI), which is part of the United Kingdom's MI5 security service, our 16-member team combines computer security specialists, business school academics working on corporate governance, management educators, information visualization experts, psychologists, and criminologists from Oxford, the University of Leicester, and Cardiff University.

Our cross-disciplinary approach has led to findings that challenge conventional views and practices (see the sidebar "Common Practices That Don't Work"). For example, many companies now try to prevent employees from using work computers to access websites not directly connected with their jobs, such as Facebook, dating sites, and political sites. We think they should instead give employees the freedom to go where they want on the web but use readily available security software to monitor their activities, thus yielding important information about behaviors and personalities that will help detect danger. In this article we share our findings on effective ways to minimize the likelihood of insider attacks.

An Unappreciated Risk

Insider threats come from people who exploit legitimate access to an organization's cyberassets for unauthorized and malicious purposes or who unwittingly create vulnerabilities. They may be direct employees (from cleaners up to the C-suite), contractors, or third-party suppliers of data and computing services. (Edward Snowden, who famously stole sensitive information from the U.S. National Security Agency, worked for an NSA contractor.) With this legitimate access they can steal, disrupt, or corrupt computer systems and data without detection by ordinary perimeter-based security solutions—controls that focus on points of entry rather than what or who is already inside.

According to Vormetric, a leading computer security company, 54% of managers at large and midsize organizations say that detecting and preventing insider attacks is harder today than it was in 2011. What's more, such attacks are increasing both in number and as a percentage of all cyberattacks reported: A study by KPMG found that they had risen from 4% in 2007 to 20% in 2010. Our research

Idea in Brief

THE THREAT
Cyberattacks involving insiders—employees, suppliers, or other companies legitimately connected to a company's computer systems—are pernicious and on the rise. They account for more than 20% of all cyberattacks. Widely used safeguards are ineffective against them.

THE KEY
To reduce their vulnerability to insider attacks, companies should apply the same approach they used to improve quality and safety: Make it part of everyone's job.

THE SOLUTION
Employees should be monitored rigorously and told what threats are likely so that they can report suspicious activities. Suppliers and distributors should be required to minimize risks and should be regularly audited. Leaders should work closely with their IT departments to ensure that crucial assets are protected.

suggests that the percentage has continued to grow. In addition, external attacks may involve the knowing or unknowing assistance of insiders. The Target incident is a case in point.

Causes of Growth

A number of factors in the changing IT landscape explain this rising threat. They aren't particularly surprising—and that's just the point. The doors that leave organizations vulnerable to insider attacks are mundane and ubiquitous.

A dramatic increase in the size and complexity of IT. Do you know which individuals are managing your cloud-based services, with whom you cohabit in those servers, and how safe the servers are? How trustworthy are those who provide you with other outsourced activities, such as call centers, logistics, cleaning, HR, and customer relationship management? In 2005 four Citibank account holders in New York were defrauded of nearly $350,000 by call center staffers based in Pune, India. The culprits were employees of a software and services company to which Citibank had outsourced work. They had collected customers' personal data, PINs, and account numbers.

"Dark Web" sites, where unscrupulous middlemen peddle large amounts of sensitive information, now abound. Everything from customers' passwords and credit card information to intellectual property is sold on these clandestine sites. Insiders are often willing to provide access to those assets in return for sums vastly less than their street value, contributing to the "cybercrime-as-a-service" industry.

Employees who use personal devices for work. Increasingly, insiders—often unwittingly—expose their employers to threats by doing work on electronic gadgets. Our team and others have found that companies' security groups cannot keep up with the dangers posed by the explosion of these devices. According to a recent Alcatel-Lucent report, some 11.6 million mobile devices worldwide are infected at any time, and mobile malware infections increased by 20% in 2013.

It's not just smartphones and tablets that are to blame: The devices can be as simple as flash drives or phone memory cards. "The best way to get into an unprepared company is to sprinkle infected USB sticks with the company's logo around the car park," says Michael Goldsmith, a member of our team and an associate director of Oxford's Cyber Security Centre, referring to the 2012 attack on DSM, a Dutch chemical company. "Some employee is bound to try one of them."

It was widely reported that delegates attending a G20 summit near Saint Petersburg in 2013 were given USB storage devices and mobile phone chargers laden with malware designed to help steal information. And the Stuxnet computer worm that sabotaged Iran's uranium-refinement facility in 2008–2010 was reportedly introduced via USB flash drives into systems not connected to the internet.

In truth, we are all vulnerable.

The explosion in social media. Social media allow all sorts of information to leak from a company and spread worldwide, often without the company's knowledge. They also provide opportunities to recruit insiders and use them to access corporate assets. The so-called romance scam, in which an employee is coaxed or tricked into sharing sensitive data by a sophisticated conman posing as a suitor on a dating website, has proved to be particularly effective. Other strategies include using knowledge gained through social networks to pressure employees: A cyberblackmailer may threaten to delete computer files or install pornographic images on a victim's office PC unless the sensitive information is delivered.

Why They Do It

A number of government and private case studies have established that insiders who knowingly participate in cyberattacks have a broad range of motivations: financial gain, revenge, desire for recognition and power, response to blackmail, loyalty to others in the organization, and political beliefs.

One example we heard about during our research was a 2014 attack by a spurned suitor on a small but growing virtual-training company. A manager there had complained to his superior about the person in question—a systems administrator who had been sending him flowers at work and inappropriate text messages and had continually driven past his home. Once clearly rejected, the attacker corrupted the company's database of training videos and rendered the backups inaccessible. The company fired him. But knowing that it lacked proof of his culpability, he blackmailed it for several thousand euros by threatening to publicize its lack of security, which might have damaged an upcoming IPO. This costly incident—like most other insider crimes—went unreported.

Insider collaboration with organized crime and activist groups is becoming increasingly common. Many countries are now operating computer emergency readiness teams (CERTs) to protect themselves against this and other types of attack. Of the 150 cases that were analyzed by the CERT Insider Threat Center at Carnegie Mellon University for its 2012 report *Spotlight On: Malicious Insiders and Organized Crime Activity,* 16% had links to organized crime.

One case was the 2012 theft by a Russian gang of details of 3.8 million unencrypted bank accounts and almost 4 million tax returns from the South Carolina Department of Revenue. Forensics showed that the attack was facilitated by an employee who clicked on a link in an e-mail, enabling the gang to steal the employee's credentials and access the state's data servers.

Monica Whitty, a psychologist at the University of Leicester and a member of our team, and many others say that insiders who willingly assist or engage in cyberattacks suffer from one or more conditions in the "dark triad": Machiavellianism, narcissism, and psychopathy. Supporting this view, a 2013 study by CPNI found that inside attackers typically have some combination of these personality traits: immaturity, low self-esteem, amorality or lack of ethics, superficiality, a tendency to fantasize, restlessness and impulsiveness, lack of conscientiousness, manipulativeness, and instability.

Roger Duronio, a UBS Wealth Management systems administrator convicted of using a malicious "logic bomb" to damage the company's computer network in 2006, exhibited a number of these traits. Duronio was worried about the security of his job

Managers in the Dark

We asked 80 senior managers about their awareness of insider cybersecurity threats and followed up with in-depth case studies of actual incidents. Here's a summary of what we found:

- Managers across all countries and most industries (banks and energy firms are the exception) are largely ignorant of insider threats.
- They tend to view security as somebody else's job—usually the IT department's.
- Few managers recognize the importance of observing unusual employee behavior—such as visiting extremist websites or starting to work at odd times of the day—to obtain advance warning of an attack.
- Nearly two-thirds of internal and external security professionals find it difficult to persuade boards of directors of the risks entailed in neglecting the insider-threat issue.
- Few IT groups are given guidance regarding which information assets are most critical, what level of risk is acceptable, or how much should be invested to prevent attacks.

and became livid when he received only $32,000 of the $50,000 bonus he had expected. So he shorted the company's stock and set off the bomb. It took down as many as 2,000 servers in UBS offices around the United States; some of them couldn't make trades for several weeks. The company suffered $3.1 million in direct costs and millions of dollars more in undisclosed incidental losses. Duronio was sentenced to 97 months in prison for the crime.

How to Think About the Problem

Managing insider cybersecurity threats is akin to managing quality and safety. All were once the responsibility of one specialty department. But organizations can no longer anticipate every risk, because the technology environment is so complex and ever changing. Thus the leaders of enterprises large and small need everyone in the organization to be involved. Here are five steps they should take immediately:

Adopt a robust insider policy. This should address what people must do or not do to deter insiders who introduce risk through carelessness, negligence, or mistakes. The policy must be concise and easy for everyone—not just security and technology specialists—to understand, access, and adhere to. The rules must apply to all levels of the organization, including senior management. A framework provided by the State of Illinois is one model. Here's a link to it: www.illinois.gov/ready/SiteCollectionDocuments/Cyber_SOSSamplePolicy.pdf

Employees should be given tools that help them adhere to the policy. For example, systems can be designed to flash a warning message on the screen when someone attempts to log into a subsystem that holds sensitive materials. The system could ask whether the person is authorized to be there and record and track those who are not.

Policy violations should incur penalties. Obviously, an employee who commits a serious offense such as selling customers' personal data or knowingly inserting malware in company systems should be fired and prosecuted. A first offense for something less serious, such as sharing passwords to enable trusted colleagues to access corporate systems, might result in a warning that goes into the employee's record.

Common Practices That Don't Work

The most common cybersecurity safeguards are much less effective against insiders than against outsiders.

ACCESS CONTROLS
Rules that prohibit people from using corporate devices for personal tasks will not keep them from stealing assets.

VULNERABILITY MANAGEMENT
Security patches and virus checkers will not prevent or detect access by malevolent authorized employees or third parties using stolen credentials.

STRONG BOUNDARY PROTECTION
Putting critical assets inside a hardened perimeter will not prevent theft by those authorized to access the protected systems.

PASSWORD POLICY
Mandating complex or frequently changed passwords means that they often end up on Post-it notes—easy pickings for someone with physical access.

AWARENESS PROGRAMS
Simply requiring employees to read the company's IT security policy annually will not magically confer cyberawareness on them. Nor will it prevent staff members from taking harmful actions.

What Can *You* Do?

Some of the most important activities that nontech leaders should ask of their IT departments are:

- monitoring all traffic leaving enterprise networks via the internet or portable media, and promptly reporting anything unusual or in violation of policy
- staying current with best practices for supporting cybersecurity strategy and policy
- rigorously implementing network defense procedures and protocols that take into account the operational priorities of the business
- actively updating user accounts to ensure that employees never have more access to sensitive computer systems than is absolutely necessary
- making frequent threat assessments and briefing the company's leadership on them

You should also help employees understand how to safely conduct day-to-day tasks. Policy should be regularly reinforced with information sessions and internal communications campaigns, which might include posters in the workplace. Some companies screen videos demonstrating how policy violations can enable cyberattacks and how safer practices might have prevented them.

Raise awareness. Be open about likely threats so that people can detect them and be on guard against anyone who tries to get their assistance in an attack. Customize training to take into account what kinds of attacks workers in a particular operation might encounter. Phishing is a common way to gain entry: Phony e-mails trick employees into sharing personal details or access codes or into clicking on a link that downloads malware. (Many people don't realize that the "from" address in an e-mail is easy to forge.) It is possible to test your staff's vulnerability to such attacks—either on your own or by employing an external security service.

Even so, it can be difficult to defend insiders against a determined outsider. In April 2013 a French multinational company was the object of a clever attack. One vice president's administrative assistant received an e-mail that referenced an invoice on a cloud-based file-sharing service. She had the sense not to open the file, but minutes later she received a phone call from someone who convincingly claimed to be another vice president at the company and instructed her to download and process the invoice. She complied. The invoice contained a remote-access Trojan that enabled a criminal enterprise apparently based in Ukraine to take control of her PC, log her keystrokes, and steal the company's intellectual property.

Encourage employees to report unusual or prohibited technologies (for example, a portable hard drive in an office where employees normally access data and software via the network) and behavior (an unauthorized employee or vendor asking for confidential data files), just as they would report unattended luggage in an airport departure lounge.

Look out for threats when hiring. It is more critical than ever to use screening processes and interview techniques designed to assess the honesty of potential hires. Examples include criminal background checks, looking for misrepresentations on résumés, and interview questions that directly probe a candidate's moral compass. Our team is developing tests that will allow employers to determine whether prospective employees have dangerous personality traits like those identified by CPNI.

During the interview process you should also assess cybersafety awareness. Does the candidate know what an insider threat is? When might he share passwords with a team member? Under what circumstances might he allow team members to use his computer as himself? If candidates are strong in all other ways, you may go ahead and hire them, but make sure that they are immediately trained in your organization's policies and practices. If someone is being considered for a job in a highly sensitive environment, however, you should think carefully about bringing him or her on board.

Employ rigorous subcontracting processes. As the Target breach demonstrates, you must ensure that your suppliers or distributors don't put you at risk—by, for example, minimizing the likelihood that someone at an external IT provider will create a back door to your systems. If a supplier's risk of failure or a breach is much smaller than yours, it may not adopt the controls you require. Seek out partners and suppliers that have the same risk appetite and culture your organization does, which will

make a common approach to cybersecurity much more likely.

Ask potential suppliers during precontractual discussions about how they manage insider-related risk. If you hire them, audit them regularly to see that their practices are genuinely maintained. Make it clear that you will conduct audits, and stipulate what they will involve. A company might require of suppliers the same controls it uses itself: screening employees for criminal records, checking the truth of job candidates' employment histories, monitoring access to its data and applications for unauthorized activity, and preventing intruders from entering sensitive physical premises.

Monitor employees. Let them know that you can and will observe their cyberactivity to the extent permitted by law. You cannot afford to leave cybersecurity entirely to the experts; you must raise your own day-to-day awareness of what is leaving your systems as well as what is coming in. That means requiring security teams or service providers to produce regular risk assessments, which should include the sources of threats, vulnerable employees and networks, and the possible consequences if a risk becomes a reality. You should also measure risk-mitigation behaviors, such as response times to alerts.

Often routers or firewalls can monitor outgoing channels, but you should make sure that the functionality is activated. If you don't have the equipment to monitor outgoing traffic, buy it. You must also log and monitor other means of exfiltration—USB flash drives and other portable storage media, printouts, and so on—through spot checks or even permanent, airport-style searches of people entering and exiting your buildings. (General Electric and Wipro use these in Bangalore.)

For monitoring to be effective, you must diligently manage the privileges of all employees—including those with the highest levels of access to company systems, who are often the instigators of insider attacks. Prune your list of most privileged users regularly—and then watch the ones who remain to verify that they deserve your trust. Look for insider-threat-detection systems that can predict possibly preventable events as well as find events that have already occurred. Big data can be helpful in linking clues and providing warnings.

Malware-detection software can be useful. Particularly in outsider-insider collaborations, a key initial step is introducing malware into the network. When you find malware, consider that it might be part of an insider attack; an analysis of how the malware is being used may provide clues to the identity and wider objectives of the attacker.

Monitoring to this degree will increase everyone's workload but will pay off by building the resilience of and reducing the risk to your enterprise.

THE MOST effective strategy for defusing the cyberthreat posed by insiders is to use the protective technologies available and fix weak points in them, but focus ultimately on getting all insiders to behave in a way that keeps the company safe. People need to know what behaviors are acceptable or unacceptable. Remind them that protecting the organization also protects their jobs.

HBR Reprint R1409G

"Sorry to see you go, Doug. You leave us with some big shoes to outsource."

CARTOON: JOHN CALDWELL