CyrusOne

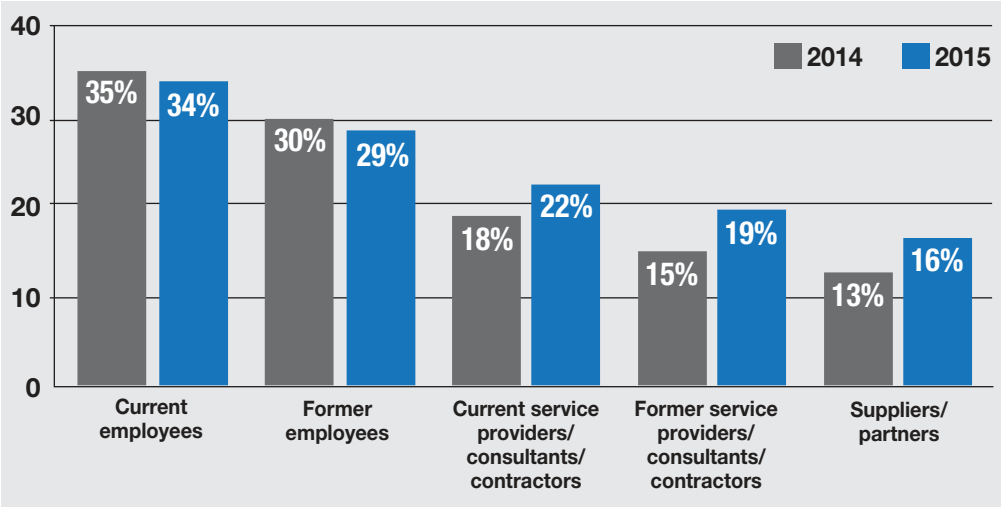
Executive Report

Are Your Own Employees Putting Your Business at Risk?

Six Vulnerabilities Hackers Love to Exploit and How CyrusOne Stops Them

Security personnel. High-powered cameras. Biometric screeners. Control keycards. Perimeter fences. Complex encryption. While companies invest millions of dollars in state-of-the-art security measures to protect their financial and intellectual assets, they typically overlook the biggest risk of all: their employees.

Sources of Security Incidents

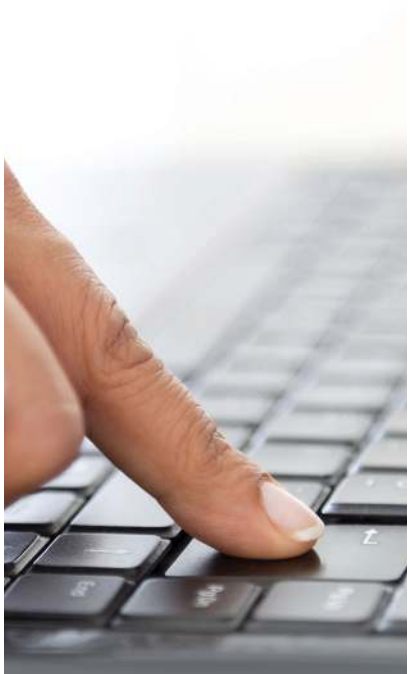


While employees remain the most cited source of compromise, incidents attributed to business partners climbed 22%.

Intentionally or unintentionally, humans cause 95% of all security failures, according to IBM's 2015 Cyber Security Intelligence Index. Nearly one in four recent breaches (22%) were caused by people that companies know and trust – people who were tricked into sharing sensitive information through phone calls, phishing emails and other techniques. Each breach costs companies an average of $2.5 million to resolve, according to PricewaterhouseCoopers' (PwC) "Global State of Information Security Survey 2016."

While many organizations put strong physical or logical security measures in place, they do a relatively poor job of educating employees to recognize possible threats. The PwC survey also revealed that only 53% of U.S. organizations deliver security training and education to their workforce. Social-Engineer, a security consulting and training firm, discovered that only 7% of U.S. organizations deliver phishing education.

Along with traditional security controls, the data center you entrust with financial and personal assets as well as intellectual property must have a security-awareness program in place. CyrusOne trains its staff to recognize potential phishing techniques and attackers – who are adept at combing through online sources and extracting information from well-meaning personnel – and defend against threats like these:



On average, it takes just 82 seconds before a phishing campaign gets its first click; 23% of phishing recipients open messages and 11% open attachments, releasing malware and viruses or allowing hackers into the system to rob companies – or their customers – blind.*

Verizon's 2015 Data Breach Investigation Report

1. Asking for Help

Recently, a hacker posing as a new FBI staffer called its information technology (IT) department seeking help to access the employee portal.[1] When asked if he had a security token, he replied, "no." The help-desk worker responded with "just use ours," and granted the imposter access to the network. Days later, the cyberthief publicly released the personal contact information of thousands of FBI and Department of Homeland Security employees – putting their identities and safety at risk.

By nature, people want to help. That's why hackers pose as employees, executives, vendors or even the media to request access to confidential files or data. While they sound legitimate and trustworthy, don't let your employees be fooled. To ensure multiple eyes and ears are on people at all times, CyrusOne trains its customer service staff to be the first line of defense when anyone calls or enters a data center. They learn how to spot suspicious behavior, breaks in protocol, and phony visitors or callers.

2. Sneaking in Behind Staff

Scam artists are well aware that people are uncomfortable being seen as rude, so they exploit that emotion. Appearing to be late for work or to a meeting, imposters often try to follow authorized personnel through a secured door in the hope they won't be stopped.

CyrusOne encourages companies to prohibit "piggybacking" outright and reinforce this policy to employees and visitors through training and signage – as it does. The company issues pre-programmed color-coded badges that restrict employee access to authorized areas depending on their role; the colors also make it easier for security teams or other personnel to recognize when someone is out of place.

3. Sending Phony Emails

Hackers pique employees' curiosity by sending legitimate-looking emails. Some lure victims to realistic-looking websites to perform phony security checks, download network or maintenance upgrades, view job postings and more. Others threaten to lock or disable accounts if the message isn't acted upon.

Breaches like these not only harm a company's reputation and shareholder value, but also its bottom line. The FBI reported that business email scams cost companies worldwide more than $1.2 billion in 2015.

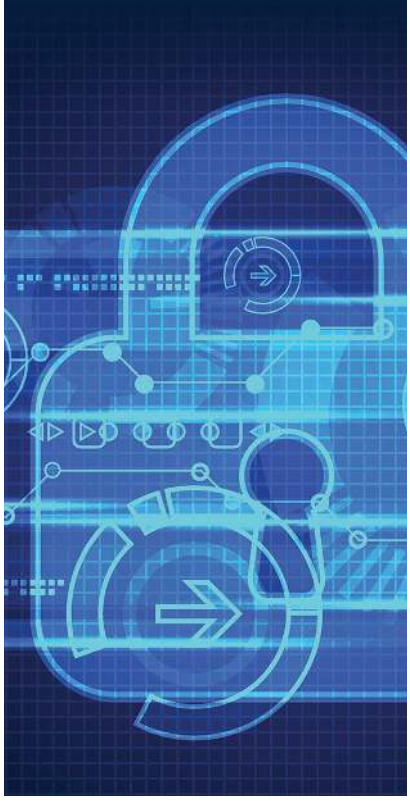
If you think your organization is immune, think again. One teen recently hacked the personal email account of the director of the CIA after looking up his cellphone number and discovering he was a Verizon customer.[2] The teen called Verizon's help desk, posing as a Verizon technician whose "tools were down" and claiming he needed to reach a customer on a scheduled callback.

[1] *http://motherboard.vice.com/read/hacker-publishes-personal-info-of-20000-fbi-agents*
[2] *http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/*

Daily Security Reminders

Each day, CyrusOne employees must complete the following before leaving their desks:

- Clean off and lock desks.
- Securely file or shred sensitive documents.
- Log off, shut down and lock up computers/other devices.
- Secure access to calendars, accounts and client files.
- Secure performance evaluations or disciplinary documentation.
- Lock up proposal requests and responses.
- Lock office doors.



After providing a fake employee code, the teen was granted access to the CIA director's account number, PIN, AOL email address and the last four digits of his bank card. He used this information to call AOL and reset the email password. This allowed him to view personal emails and a security clearance form, which contained sensitive information about the CIA director's family.

CyrusOne has adopted a "no-click policy" and regularly shares examples of scams with its workforce. The policy also prohibits employees from accessing personal email and other personal information online while at work.

4. Unlocking Weak Passwords

It is alarmingly easy for malicious insiders to access passwords and other sensitive information from indifferent colleagues. Many employees write passwords on sticky notes or put them under their keyboard – or share their passwords with others. They also select weak passwords such as "password1" and reuse that same password on all devices.

According to the 2015 TrustWave Global Security Report, it takes hackers just one day to crack an eight-digit password, but 591 days to crack 10-digit passwords. CyrusOne requires strong passwords and mandates that employees change their passwords frequently.

5. Hacking Exposed Devices

Employees often leave laptops and smartphones unattended or unlocked when they use the restroom, attend meetings or head to lunch. This gives disgruntled colleagues or building guests ample opportunity to access or steal the machines.

One physician learned this the hard way after he left his unsecured and unencrypted laptop in an unlocked office. Hackers laid their hands on the personal health information of more than 4,000 people and his hospital was fined $100,000.[3]

To prevent these types of incidents, CyrusOne instituted automated locking of all PC and laptop devices, office doors and other sensitive building areas. Additionally, it crushes and shreds workplace electronic equipment at their end of life, and wipes files clean when a worker resigns or is terminated.

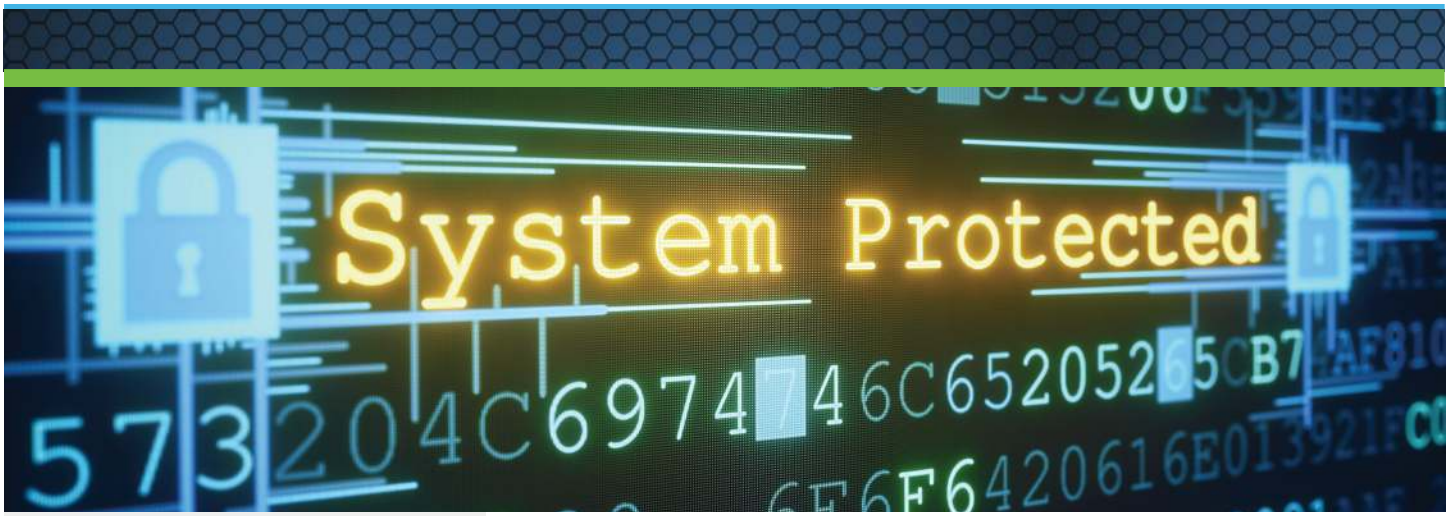
6. Leaving Behind Flash Drives

Portable thumb drives are easily concealable and can be used to introduce malware or a virus to a system, or to copy and externally share confidential files. Attackers are known to drop a few thumb drives in parking lots or other building areas, hoping a helpful employee will plug one into their own computer in hopes of identifying to whom it belongs.

To solve this problem, some organizations:

- Fill USB ports with clear silicone caulk to prevent flash-drive use.
- Use software that monitors all ports and encrypts data during file transfer, thereby requiring users to obtain an encryption key to access the information.
- Limit or disable the use of USB flash drives through a software program.[4]

[3]http://healthitsecurity.com/news/healthcare-security-breach-hits-washington-hospitals/
[4]http://www.cio.com/article/2400017/security0/how-to-prevent-thumb-drive-security-disasters.html



At CyrusOne, Security Awareness Programs Must:

- Meet stringent compliance and audit standards.
- Be easily deployable and understandable.
- Include social engineering training.
- Address evolving threats.
- Deliver fresh content and messaging.
- Assess employees' information needs.
- Evaluate awareness practices and protocols.
- Detect warning signs to make necessary refinements.

Thwart Attacks by Amplifying Awareness

Effective security-awareness training programs should meet rigorous certification requirements and internationally recognized guidelines.

CyrusOne keeps security teams abreast of the latest news in business crime and security each day, and shares this information – along with security best practices and protocols – to maintain employee vigilance.

The company also keeps training initiatives and reminders fresh, engaging and memorable to reinforce positive behavior.

Security Awareness at CyrusOne

Security is foundational at CyrusOne, where the highest security standards mitigate risk and deliver peace of mind. As the preferred data center provider of the Fortune 1000, the most demanding global companies trust CyrusOne for exceptional security, reliability and service.

In addition to the security measures described in this report, CyrusOne:

- Has its sales force conduct extensive due diligence before ever letting a prospective vendor or client walk in the door. All authorized visitors must have their identities verified, backgrounds reviewed and nondisclosure agreements signed. They are escorted to pre-approved areas.
- Gives its employees annual training – as well continuous reminders – on how to protect themselves and the data center from attempted attacks.
- Requires that its security teams pass a state security certification program and 40 hours of company training specific to its data centers, with refreshers provided monthly, quarterly and annually.

CyrusOne's employee training complies with rigorous standards set by trade groups and global certifying organizations[5], including the International Organization for Standardization, the National Institute of Standards and Technology Federal Information Security Management Act, and the Health Insurance Portability and Accountability Act.

[5] *http://www.cyrusone.com/data-center-technology-features/certifications*

About CyrusOne

CyrusOne specializes in providing highly reliable, flexible and scalable enterprise data center colocation that meets the specific needs of customers across its broad portfolio of carrier-neutral data center facilities in the United States, Europe and Asia. CyrusOne employs its Massively Modular® engineering and design approach to optimize design and construction materials sourcing and enable just-in-time data hall inventory to meet customer demand.

The company engineers its facilities with redundant power technology, including an available 2N architecture. CyrusOne customers can mix and match data centers to create their own production and/or disaster recovery platforms by combining facilities via the low-cost, robust interconnectivity provided by the CyrusOne National Internet Exchange (IX).

CyrusOne
Built for Tomorrow. Ready Today.