Red River

THE TOP

CYBERSECURITY

THREATS TO BUSINESSES IN 2019

There is one universal constant in the cyberthreat landscape: It is constantly changing. As a result, cybersecurity professionals, IT staff, and all employees need to be vigilant and informed about the latest threats that their company can potentially face.

The world of cybercrime is an enormously deep and complex field, far too much to completely cover in a single publication, so this piece will detail the most commonly encountered types of cybercrime and actionable steps companies and employees can take to guard against them.

THE STATE OF CYBERSECURITY IN 2019

As the world becomes increasingly plugged-in and always online, cybercrime has grown as well. A 2018 study of cybercrime by Bromium found that cybercriminals were generating revenues of $1.5 trillion every year. Cybercrime is on pace to become more profitable than the global illicit drug trade, **if it has not already.**

Virtually every organization will face an attack at some point in its life, and the pace is only accelerating: The first quarter of 2018 saw more than 210 million global cyberattacks, a 62% yearly increase.

If you're an IT professional, you're likely all too aware of how common and effective these attacks can be. Only 38% of business/IT professionals surveyed in the ISACA 2015 Global Cybersecurity Status Report believed their organization was prepared to face a cyberattack. These attacks can be costly, too; a 2016 study estimated the average cost per data breach at $4 million.

MOST COMMON BUSINESS CYBERSECURITY THREATS

The best firewalls and most powerful AI analysis can only do so much to bolster the primary point of weakness: the user. A 2018 survey of black-hat hackers found that fully 88 percent of them used "social engineering techniques" in their attacks.

Human error can cost millions of dollars. It's important for you and other employees of your business to understand the most common types of cyberattacks, how they work, and how to avoid them.

Baiting: This attack exploits natural human curiosity in order to circumvent security practices. Often, these attacks involve sending physical media, like an unmarked CD with a strange, confusingly worded letter, or a USB drive left on the ground with a tempting label like "layoff plans." Sometimes, the attacks are wholly digital, involving links to deals or free items. When the link is clicked or the device inserted, malware is installed on the target computer.

Remind employees that if something seems too good to be true, it probably is. Never use a device or click on a link you don't trust.

Phishing: By far the most common type of cyberattack -- estimated to cause between 70 and 90 percent of successful data breaches -- phishing attacks attempt to acquire sensitive information like usernames, passwords, or credit-card details by masquerading as an entity that the target trusts, like a charity, bank, social-media site, or medical provider.

This is typically not a specific, targeted attack. Most phishing schemes cast a wide net using bulk email, profiting even if only several targets fall for the attack. Once an attacker has a target's information, they can access bank accounts or employee payroll sites and divert direct deposits into a bank account they control.

Employees should be wary of any email that asks for sensitive information like passwords or credit-card numbers, and should carefully check to make sure the email isn't spoofed. Typical phishing tricks include similar-looking letters or impersonated domains (e.g., @connpany.com or @company.real.com instead of @company.com).

Spear Phishing: Unlike the wide net cast by a phishing scheme, spear phishing is laser focused. Spear phishing is a targeted attack aimed at a specific company, organization, or individual. Unlike phishing, which targets common data like passwords or credit-card data, spear phishers are typically after more valuable, proprietary data like confidential information, corporate secrets, access to company networks, and the like.

Spear phishing attacks require research on the target, sometimes performing significant amounts, typically via sites like LinkedIn or the company's own website, where names of employees (in SMBs) or C-Suite leadership (in enterprise-level businesses) may be listed. This research allows a spear phisher to pose as a trusted source -- a coworker, manager, or frequently-used vendor -- giving the attack more credibility than a bulk email scam, and doing things like convincing an employee to buy $2,000 worth of iTunes gift cards.

Teach your employees to be wary of sudden, urgent-sounding requests to update invoices or do anything that might require transmitting or disclosing financial information. If something sounds suspicious, always confirm with the source, ideally by some method other than email.

Vishing: A combination of "voice" and "phishing," this is to phones what phishing is to emails. Vishing attacks use a spoofed caller ID to imitate a contact the employee might trust, and pretend to be calling about an urgent issue. They might claim to be from the local sheriff's office with a warrant out for the target's arrest or a representative from Microsoft Support wanting remote access to the target's computer.

The chief criminal benefit of vishing schemes is that they put pressure on targets to act quickly without having the chance to think things through. Remind all employees that there is rarely a situation so urgent it cannot be independently confirmed and to never give out any personal or private information over the phone to someone whose identity they have not verified.

Scareware: A variant of the "baiting" attack described above, scareware programs trick a user into downloading potentially dangerous software under the guise of antivirus protection. A popup message might come with a message like "Warning: Your computer is infected!" and direct the target towards a page where they can purchase or download an antivirus program that will remove the alleged infection. Of course, this phony antivirus program is the real malware, and it can even interfere with real security programs. This can make phony antivirus software very difficult to remove.

Your employees should remember that a website or popup ad that claims to have detected a virus on your system is almost certainly lying. If your employee fears that their computer or device has been infected, they should contact their IT department -- not trust some anonymous website.

Tailgating: Also called "Piggybacking," this is a physical social-engineering technique that involves unauthorized individuals following authorized individuals into an otherwise secure location. A person will impersonate someone like a delivery driver and wait outside a building or secure area for someone with authorization to enter, then ask them to hold the door. Once inside, the criminal may physically steal something valuable, or may plug a device like a USB drive into the network, opening a backdoor entryway for them to exploit later from a remote location.

It is understandable for your employees to want to be helpful. Remind them that even authentic-seeming unauthorized personnel must all follow proper entrance and authorization procedures. If you hold the door for a delivery person, make sure to accompany them to the front desk or other security station where their delivery can be authenticated.

KEEPING YOUR DATA SECURE IN A BYOD WORLD

As an organization, there are additional steps you can take to optimize cybersecurity and safety in the workplace.

- **Patch often.** Make sure all applications and operating systems are updated with the latest patches as frequently as you can.
- **Use DNS-level protection.** Security at the DNS level can block common malware or phishing sites and defend against botnets.
- **Maintain firewalls and email filters.** The best email filters can defeat many phishing attempts before an email hits an employee's inbox. Secondary benefit: This cuts down on the amount of spam your employees receive.
- **Scan the Dark Web.** Use trusted dark-web monitoring services to find any compromised credentials your employees might be using. This will help you shore up your defenses so one compromise doesn't start a cascading effect of future attacks.
- **Disable Autorun capability.** Ensure that when a foreign device is inserted into an employee's computer, it won't run potential malware automatically.

While these tips are all effective, they only serve to protect devices and computers in your workplace. Unfortunately, that isn't the only type of device being used in many modern organizations.

The increasing ubiquity of Bring Your Own Device (BYOD) philosophies at organizations that range from startups to major enterprise-level corporations has many benefits -- it's always nice to have your employees working on technology they're comfortable using. However, this also means that employees must practice proper security best practices at all times, whether on or off the clock.

Therefore, CWPS' number one must-do tip for improving your organization's defenses against cyberattacks should come as no surprise:

Train your users. We cannot overstate this enough -- your employees must have proper cybersecurity training. No firewall will help you as much as savvy users will. Ensure your employees are familiar with various types of cybersecurity attacks, tips for recognizing social engineering red flags, and what they should do if they encounter an attack at work or at home.

Your employees should know to verify claims from external organization. They should know to never reveal personal or financial information, or information about your organization, to someone over email or the phone, unless they are certain of that person's identity and authority to have the information. Your employees should know to never click on suspicious links or download suspicious programs. Passwords should be regularly changed and not reused, and data should be backed up regularly.

Make your employee an expert on recognizing cyberattacks so that they can teach their family, too, from parents and spouses to children. A personal attack on one of your trusted employees may as well be an attack on your company: It's a stressor, impacting their work, and it may even open them up to blackmail.

NEW THREATS ON THE HORIZON: CYBERCRIME IN 2019 AND BEYOND

Nobody can predict the future. However, a careful analysis of trends in cybercrime can give us some idea of where cybersecurity -- and cybercrime -- may be headed.

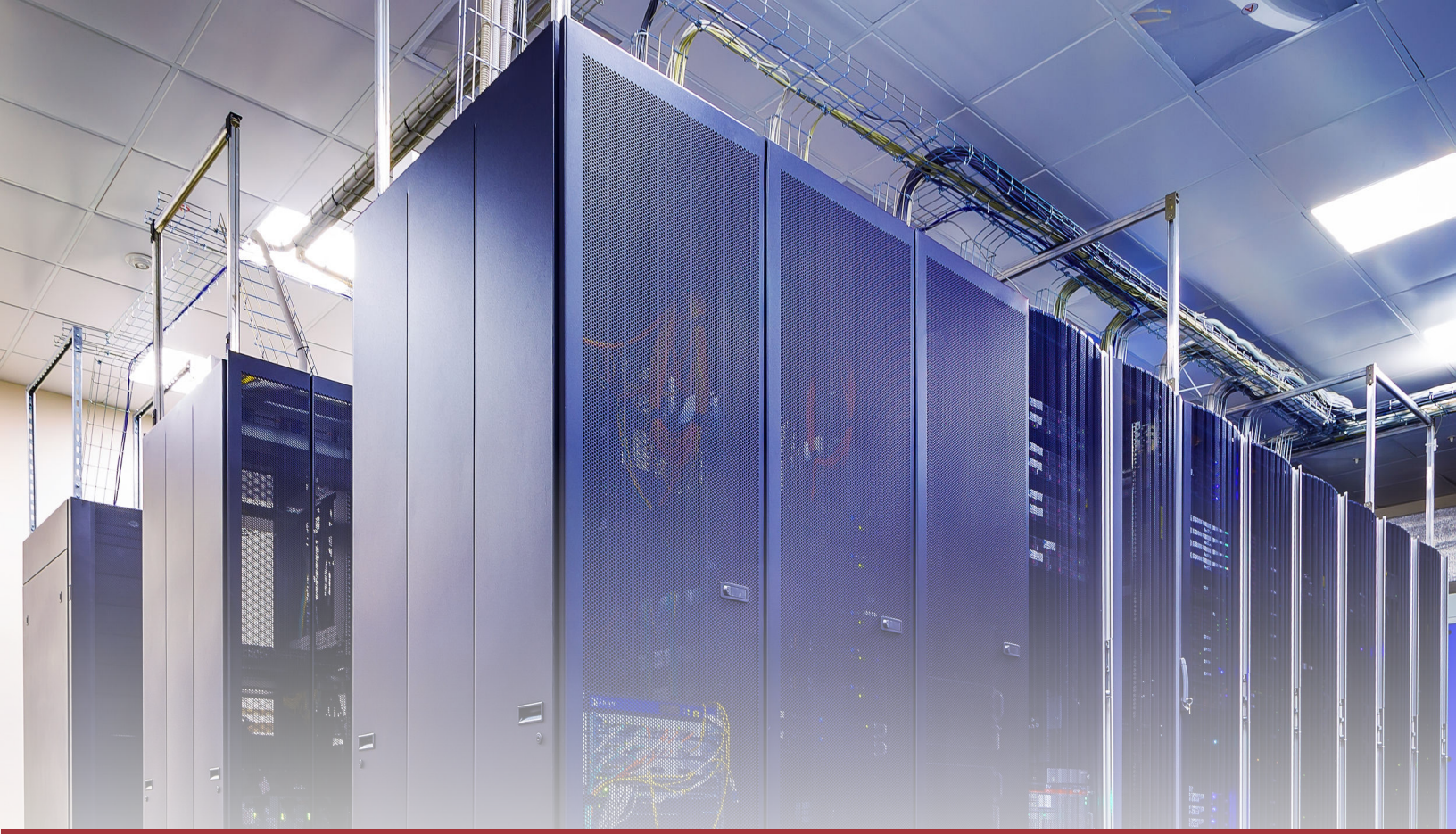
- More nations will develop offensive cyber capabilities. From Stuxnet to political hacks and beyond, many cyberattacks will not be the work of state-agnostic criminals, but rather be from, and targeted at, government agencies and contractors.

- Cybercriminals will step up attacks on the IoT. Hacking a phone, PC, or tablet is one thing. What happens when criminals can attack your smart refrigerator or your car?

- Antivirus software will continue its decline. Third-party antivirus and anti-malware programs have continued to see their user base shrink. As companies and individuals rely more on built-in OS-level protection, this trend will only continue.

- Multi-factor authentication will become the norm. It's easy to compromise one device. It's much harder to compromise several. This is a no-brainer for any organization that wants to keep itself, and its customers, safe.

- Utilities and industrial controls will be targeted with ransomware. Targeting an enterprise with ransomware can result in a loss of millions of dollars. Targeting a power or water company could have significantly more serious, even life-threatening effects.



SUMMARY

Cybersecurity threats have continued to evolve, and are both increasingly ubiquitous and increasingly dangerous. Cybercrime costs organizations around the globe billions of dollars every year. It is not a question of if your organization or business will be attacked, it is a question of when, and how well you and your employees will be prepared for it.

The vast majority of cybercrime in the modern era relies heavily on social engineering, targeting the most common weak point in any security system: the user. Common schemes like phishing, baiting, vishing, and scareware all rely on individual lapses of judgment, often exacerbated by an apparently urgent scenario, to gain access to sensitive or financial information.

Because cybercrime so often relies on human error to succeed, comprehensive employee training to recognize and defend against scams and schemes is one of the most effective ways you can improve your organization's cyber defenses.

The cyberthreat landscape is always changing, and there will doubtless be new emerging threats and attacks that no experts have seen coming. Rather than force your business to navigate an intimidating landscape by itself, CWPS can provide technological solutions as well as employee training in order to keep your organization up to date and ready for these emerging threats. Contact redriver to get started safeguarding your company's critical data today.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.