THE ULTIMATE REFERENCE GUIDE TO CYBERSECURITY THREATS

A field manual documenting what you're up against, what you can do on your own – and when you need to call in the experts to help you manage it all.

Trustwave®

01
PHISHING

RANSOMWARE 02

03 CRYPTOMINING

OTHER MALWARE 04

05 POINT-OF-SALE

DISTRIBUTED DENIAL OF SERVICE (DDoS) 06

07 MOBILE

SOCIAL MEDIA 08

09
WEB APPLICATIONS

10
VULNERABILITIES & MISCONFIGURATIONS

11
INTERNET OF THINGS

12
SUPPLY CHAIN

Social engineering emails containing malicious links or attachments are a common way that hackers establish an initial foothold within a targeted environment, generally through credential theft or malware delivery. Phishing facilitates more than half of all compromises in corporate networks. Hackers prefer this method of attack because it takes advantage of human behavior and tendencies, like inherent trust, helpfulness and curiosity. It's psychological manipulation at its finest and capitalizes on techniques that con artists have used for millennia.

THREAT:

PHISHING

CURRENT THREAT LEVEL:
—

WHAT DOES AN ATTACK LOOK LIKE?

A few of your employees are targeted with bogus (but realistic-looking) emails from a cloud storage service that lead to them divulging their system credentials. Or your accounting team receives an email claiming to be from your CEO, asking for money to be wired to a certain destination.

WHAT YOU AND YOUR TEAM CAN DO

You won't have a problem with phishing if your users never fall for the bait. Easier said than done, though. You can work toward the goal of responsible email practices by training them to be skeptical and recognize the tell-tale signs of deceptive emails. These signs will usually include things like a request for urgent action or acknowledgment of a current event, and leverage a sketchy-looking hyperlinked URL or attachment, as well as poor grammar and spelling (although that's not always the case). When in doubt, verify the sender. You should also ensure your client software is fully patched to avoid known vulnerabilities from being exploited and that users are operating with the least set of privileges necessary to do their jobs.

WHAT EXTERNAL PROFESSIONALS CAN DO

Outside experts can amplify your internal efforts. For instance, they can help you build a sound security awareness education program that includes mock phishing exercises. The pros can also help you manage protection through email and web security gateways that can flag and block malicious links and attachments in real time, as well offer the appropriate policy controls and filters to help fight spoofing. There's also another component to the phishing plague: brand abuse. If you're worried about your company's name being dragged through the mud in phishing emails, you can subscribe to a service that monitors for criminals seeking to exploit trust in your brand.

The prevalence of ransomware has soared in recent years for one simple reason: It works. Attackers use this type of malware to render sensitive files inaccessible until the victim pays a ransom (usually by some urgent deadline). Even then, there is no guarantee the attackers are cleared from your network or will actually release your data. In some extreme cases, the attackers may be distributing ransomware with the specific goal of destroying data as opposed to turning a handsome profit. There is some good news: Some studies in the first half of 2018 suggested that the number of ransomware incidents was falling, but beware: Now is no time to get complacent. Ransomware attacks result in heavy costs to victims, and the FBI recently warned of an expected spike in new cases.

THREAT:

RANSOMWARE

WHAT DOES AN ATTACK LOOK LIKE?

One of the most rancorous attacks in recent years was a ransomware worm known as WannaCry, which spread via a Windows software vulnerability known as EternalBlue. A more common example would be if one of your users opens a malicious email attachment or clicks on a suspicious link - which prompts an immediate screen notification that your data has been encrypted and alleged instructions for how to decrypt.

WHAT YOU AND YOUR TEAM CAN DO

The work you can do is mostly on the preparation side. Perform regular backups for your important data and keep your patches and anti-virus up to date. If you do fall victim, immediately disconnect the affected system (likely a workstation) from the web and begin the data restoration process.

WHAT EXTERNAL PROFESSIONALS CAN DO

External security specialists can help arm you with proactive technology solutions, such as vulnerability testing, anti-malware, email and endpoint protection, and application whitelisting. Good endpoint detection and response (EDR) products identify ransomware immediately, based on the combination of malicious behaviors it exhibits, and suspends the encryption process before it can hold files hostages, let alone move laterally across the network. All of these solutions can help halt these attacks at their source. If ransomware does evade your front-line defenses, the pros can help you prepare for such an event, respond if an incident occurs and forensically review what happened.

THREAT:

CRYPTOMINING

As the blockchain grows, it becomes increasingly computationally expensive to perform the calculations necessary to generate new digital coins. Attackers have decided: Why not have a victim perform cryptocoin mining on their behalf? Malware that steals cryptocurrency is only effective on computers storing such currency, but malware that mines currency – usually Monero – can run on any computer it infects. Criminals use such "miners" as payloads in malware attacks, slowing the computer's performance and wasting electricity for the benefit of the attacker. While cryptomining malware must be installed, mining scripts like Coinhive just need to be added to website code. However, mining scripts have a notable drawback. They run only if the browser is open and stays on that affected website. As soon as the user closes the browser or navigates away from that site, the script will not run anymore.

CURRENT THREAT LEVEL:
—

WHAT DOES AN ATTACK LOOK LIKE?

One of your users unknowingly visits a website that has been compromised and seeded with a dozen or so lines of script to harness the CPU and electricity of the user's computer to generate digital coins.

WHAT YOU AND YOUR TEAM CAN DO

Try to ferret out where the CPU hogging is coming from to help confirm that cryptomining is, indeed, the culprit. There are plenty of third-party ad blockers and browser extensions that specifically block cryptomining scripts.

WHAT EXTERNAL PROFESSIONALS CAN DO

Anti-virus software can usually remove a cryptomining infection. But as this threat becomes more lucrative and prolific for the crooks behind it, nastier strains are beginning to show up that evade detection – so you'll need to make sure you're running advanced security software.

THREAT:

OTHER MALWARE

With all the focus on ransomware and cryptomining malware, it is important to remember that traditional malware, usually designed to steal data, is alive and well. Password stealers, banking malware, remote access toolkits and backdoors are still prevalent and remain a major threat. This includes fileless malware, which can gain control of computers by leveraging common tools to hide in memory, thus evading anti-malware protections that monitor your hard drive.

CURRENT THREAT LEVEL:
—

WHAT DOES AN ATTACK LOOK LIKE?

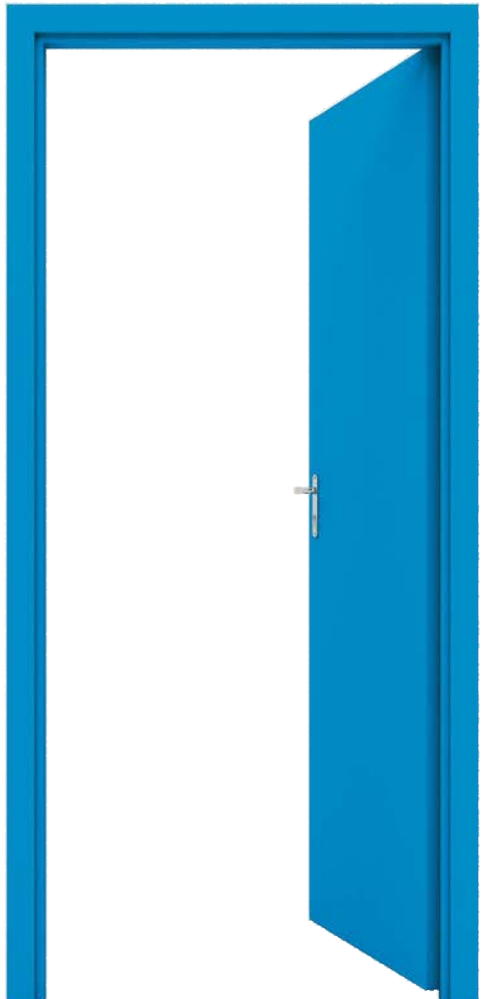
A user falls for a phishing email that infects their PC with a remote access toolkit that gives criminals complete control over the system and ensures future access at any time. This is nearly impossible to detect because everything is done in memory without writing any malicious files to disk.

WHAT YOU AND YOUR TEAM CAN DO

Ensure anti-malware software is current on all systems and configure it to automatically update virus definitions. Sometimes this takes some additional work, so you need to make certain you have a valid virus definition license and the software is properly accessing new definitions. Whitelisting is another option by only allowing pre-approved applications to run. If you suspect malware is, or was, on a system, you may want to completely wipe and rebuild the system to fully confirm the threat has been removed.

WHAT EXTERNAL PROFESSIONALS CAN DO

To handle the more sophisticated malware that is custom built to duck conventional anti-virus, you will likely need to bring in pros who can provide a proper risk assessment of your network so you can better understand how you may be threatened by custom malware. Managed security specialists can also take you beyond traditional, prevention-focused security measures with detection and response capabilities. These fuse threat hunting, threat intelligence, and incident mitigation to help you monitor logs and alerts, investigate anomalies and remediate malware.



Thanks to the move from magnetic strip readers to chip-based terminals, malware targeting point-of-sale (POS) systems is diminishing. Yet high-profile retailers continue to experience infections, and new variants of payment data-targeted malware, like PinkKite and TreasureHunter, continue to surface and carry a small footprint in order to avoid detection. POS malware often sits on hacked terminals for many months before being flagged.

THREAT:

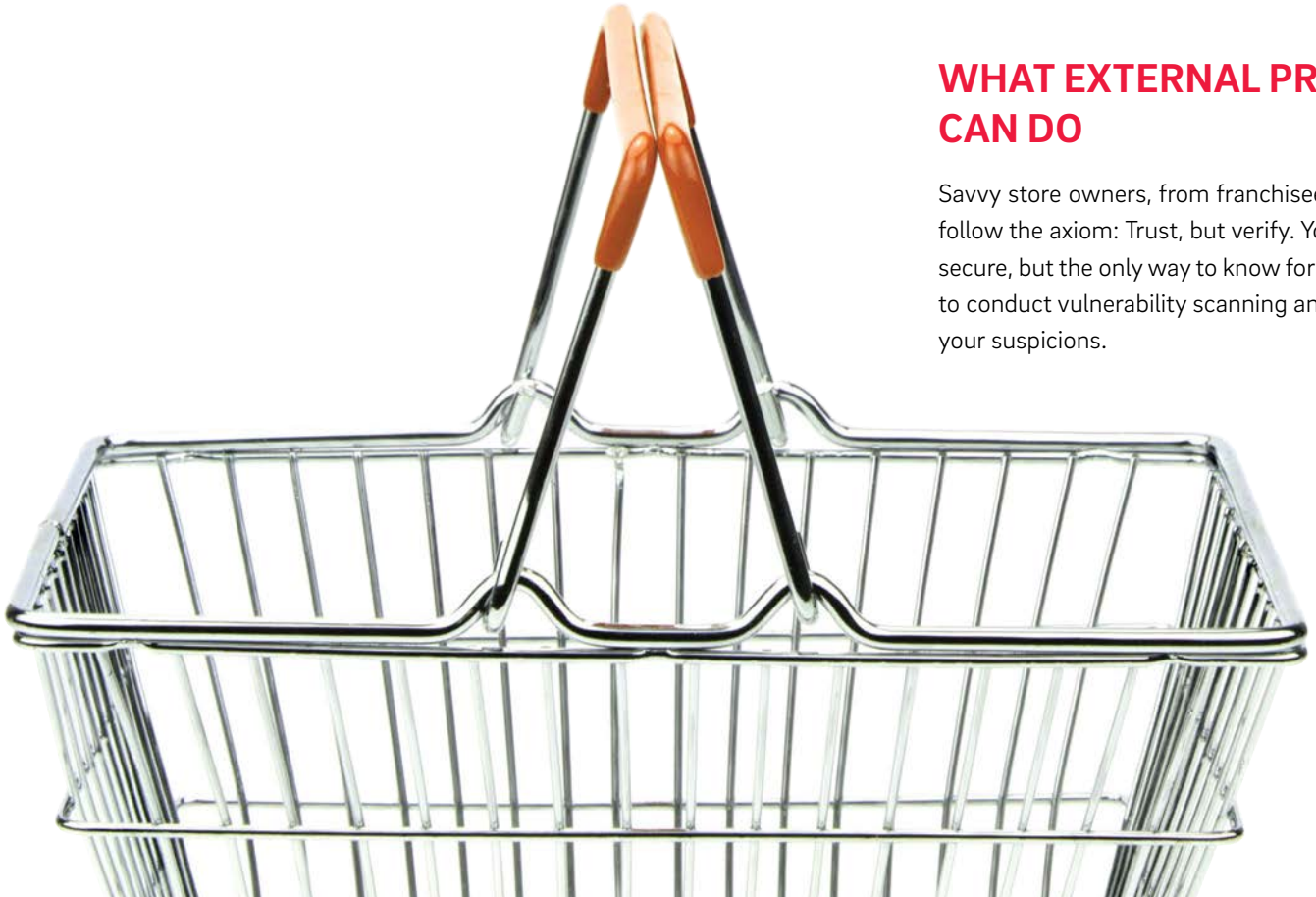
POINT-OF-SALE

WHAT DOES AN ATTACK LOOK LIKE?

When it comes to POS malware, victims tend to make it easy on the adversaries: Crooks scan the web for vulnerable POS systems and can often rely on default or simple credentials for common remote administration utilities. These tools are used to perform legitimate remote administrative functions on POS systems and software. Once these are compromised, intruders plant memory-scraping malware that captures credit card data. The saboteurs may also choose to go right to the source – POS system vendors – and insert malicious code into the devices during the supply chain process.

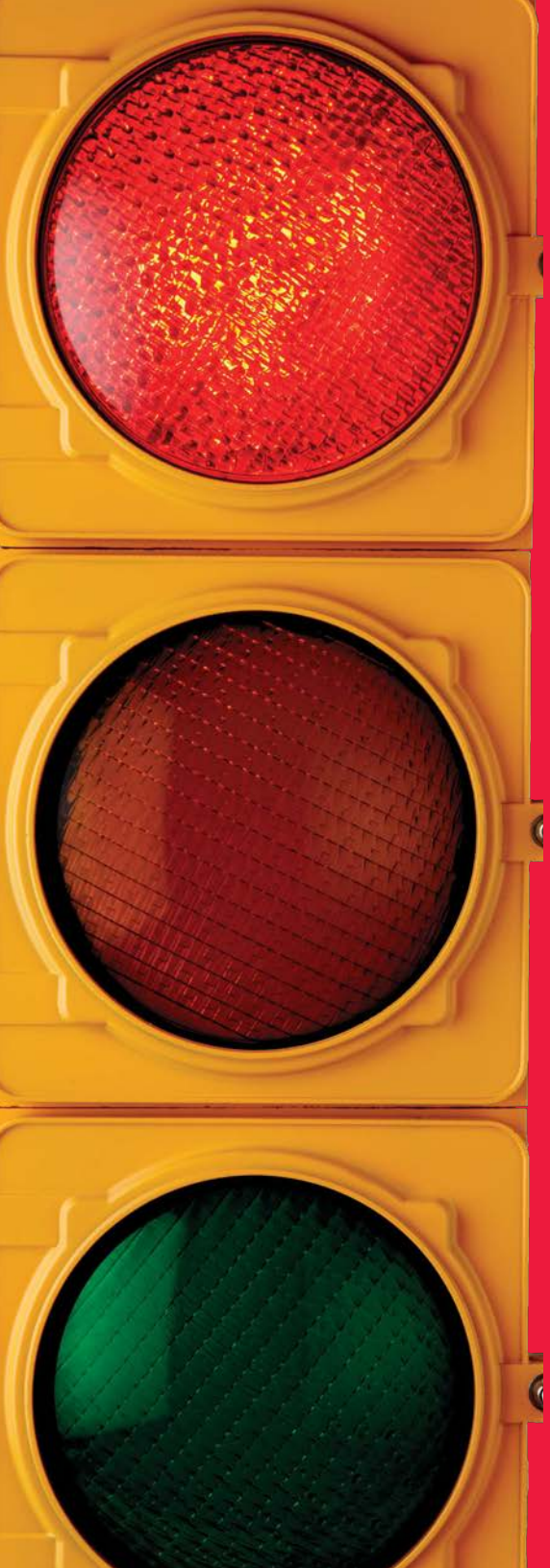
WHAT YOU AND YOUR TEAM CAN DO

A common way attackers hijack POS systems is with remote scanning and access tools, as well as the exploitation of easy-to-crack passwords. In other words, '123456' isn't going to cut it. Respond by disabling remote access and employing strong (non-default) passwords – or better yet passphrases. Also, govern who can access terminals, use network segmentation and restrict web access on systems and stations. For added confidence, vet your POS terminal providers to ensure they take security seriously.



WHAT EXTERNAL PROFESSIONALS CAN DO

Savvy store owners, from franchisees up through big-box retail, will follow the axiom: Trust, but verify. You believe your POS systems are secure, but the only way to know for sure is by bringing in the experts to conduct vulnerability scanning and penetration testing to confirm your suspicions.



THREAT:

DISTRIBUTED DENIAL OF SERVICE (DDoS)

DDoS attacks have been around for decades, but they are rapidly increasing in intensity and impact thanks to new "amplification attacks" and, in some cases, due to armies of compromised IoT devices. Using this method of attack, a Fall 2016 ambush against internet infrastructure provider Dyn is considered one of the largest DDoSes in history. Meanwhile, shorter, lower-volume attacks sometimes act as a distraction for more serious network intrusions that are already underway.

WHAT DOES AN ATTACK LOOK LIKE?

DDoS attacks will bombard their victims with massive amounts of fake traffic to overwhelm web servers and render a website inaccessible. Externally, your customers will be entirely unable to reach your site or will experience lengthy delays for pages to load. Internally, you can also experience disruptions to your file servers and other operational systems. The attacks usually start slowly, only to progress to the ultimate goal: consuming all available bandwidth and resources to shut you down.

WHAT YOU AND YOUR TEAM CAN DO

Companies whose business success relies on its web presence must take DDoS attacks seriously. You should proactively audit your firewall rule base to discover what traffic you are allowing in and out – and confirm whether you are able to stop unnecessary protocols and packets at the perimeter. Generally, though, the DDoS threat is one that will need outside help.

WHAT EXTERNAL PROFESSIONALS CAN DO

DDoS mitigation services can help handle high-volume, intense attacks. You can also talk to your internet service provider to ensure they are performing mitigation methods, such as protocol filtering.

THREAT:

SOCIAL MEDIA

Social media sites are often an overlooked attack vector because users tend to let their guards down in these seemingly friendly and trusted environments. Wrong move! Not only are these sites prime territory for perpetuating malware and other fraudulent schemes, but also serve as an optimal reconnaissance tool for attackers seeking to gather information about employees that can be later used in targeted phishing attacks and other social engineering ploys.

WHAT DOES AN ATTACK LOOK LIKE?

Beware of the over sharers in your organization. For example, the details that an executive posts about her travel could be used by attackers to craft a spear phishing attack. Or a member of your engineering group thinks he is privately messaging another team member about project specs, but mistakenly shares them on a social media account.

WHAT YOU AND YOUR TEAM CAN DO

Banning social media channels is rarely an option considering how tightly woven they are into our personal and business lives. (Think of how quickly the masses freak out whenever Twitter or Facebook is down.) Instead, turn to acceptable-use policies and education to propel your users to safely navigate these sites – keeping in mind that the information posted on personal accounts can offer reconnaissance that can be used to access corporate email accounts and the like. For example, if an attacker knows your interests or is aware of something like your dog's name, they can send you a phishing message related to that activity or have a better chance of accessing your password. As for your business' social media accounts, conduct a thorough inventory, as "sprawl" can be a real problem. Sometimes workers will set up specialty accounts without corporate marketing's approval. In addition, monitor your accounts for signs of information leakage, compromise or some other abnormal activity.

WHAT EXTERNAL PROFESSIONALS CAN DO

The experts can bring in the technological firepower to help stop malware attacks or data leakage that may originate on social media sites. This includes web security gateways and data loss prevention solutions. Monitoring your employees' social media activities is another option where an outside firm can assist, but if you go this route, make sure employees are aware their expectation of privacy may be limited.

THREAT:

MOBILE

Gone are the days when you could say "sorry, not sorry" to employees wanting to use mobile devices for their jobs. Nowadays, mobile devices are ingrained into every aspect of our lives, including our work. The good news is that while some control naturally may be lost to this phenomenon, if organizations embrace enterprise mobility properly, you can reap huge rewards of worker productivity and efficiency. But mobility presents obvious risks, including ad and click fraud and malware that can lead to wider corporate network attacks.

WHAT DOES AN ATTACK LOOK LIKE?

One of your users receives a text message enticing them to download an app. The app turns out to be spyware that gives attackers access to steal credentials, which can be used to enter the enterprise network.

WHAT YOU AND YOUR TEAM CAN DO

You must build a smart mobile security strategy that your users won't find to be overly intrusive or bothersome and can be confident their personal data is being respected. They will respond best to clear policies that include guidelines around app downloads and Wi-Fi use. And because things we can bring everywhere – like smartphones, laptops and tablets – tend to get lost easily, you may want to consider having functionality to wipe corporate data if an endpoint goes missing.

WHAT EXTERNAL PROFESSIONALS CAN DO

The experts can augment your ability to provide risk assessments, device management, malware mitigation and penetration testing. While the mobile landscape still isn't quite as prized among cybercriminals, now is the time to get serious and learn how specialists can assist you, with studies agreeing that mobile threats are rising precipitously.

CURRENT THREAT LEVEL:
—

THREAT:

WEB APPLICATIONS

Think of web applications as the front door to your sensitive data, and with more than a billion websites out there, that adds up to a lot of entryways for malicious hackers. A perfect 100 percent of all applications Trustwave tested last year contained at least one vulnerability (with a median of 11 per app). While this doesn't mean that all companies should brace for a breach tomorrow – after all, not all of these vulnerabilities are easily discoverable or attractive to exploit – it certainly raises red flags that businesses aren't doing a good enough job of flagging and stomping out these bugs.

WHAT DOES AN ATTACK LOOK LIKE?

An attacker scans your website, discovers an unpatched SQL server vulnerability and exploits it to establish an initial foothold in the network. They might also deploy a web shell on a targeted server to maintain control and pivot to part of the network holding and processing cardholder data.

WHAT YOU AND YOUR TEAM CAN DO

If you're building your website in-house, you must assemble a team that is security competent and is educated in developing and reviewing resilient code. Another option is to implement a bug bounty program through which individuals receive compensation or recognition for discovering vulnerabilities residing on your websites and in your software. Awards programs are a trend picking up steam among businesses by incentivizing third-party "good guys" to help accent your in-house security. Also, in general, you should keep your web servers patched, include your web apps in your risk assessments, implement strong passwords and monitor the integrity of files on web servers.

WHAT EXTERNAL PROFESSIONALS CAN DO

Web apps lead to lots of compromises, so a multi-layer defense strategy is mandatory. The experts can bring in web application firewalls to help customers stay sheltered from a wide range of attack techniques. WAFs provide protection against exploitation by monitoring HTTP requests and responses for known attacks and anomalous behavior, using static rulesets and active learning. But the only way to know for sure that your application is deplete of vulnerabilities is to scan and penetration test.

Even if you build an application using secure platforms, technologies and development principles, a single, obscure misconfiguration or vulnerability can open a door for an attacker to compromise your system. A simple slip-up of a security setting on a cloud storage system, or failure to patch a minor flaw (and there were more than 20,000 of them in 2017 – a record – according to Risk Based Security) can make life much easier on your adversaries. Remember, malicious hackers can afford to make many mistakes as they just look for just one oversight you made in securing your network.

THREAT:

VULNERABILITIES & MISCONFIGURATIONS

WHAT DOES AN ATTACK LOOK LIKE?

You mistakenly activate 'Guest' access when adding a new user account to your cloud storage. This leaves your cloud storage "buckets" open to the public, which exposes everything form sensitive data to decryption keys. In another example, one of your team members adds new firewall rules, which leaves more ports open than policy permits – and allows malicious traffic to enter onto your network.

WHAT EXTERNAL PROFESSIONALS CAN DO

Risk assessments are a good place to start. You should regularly conduct external and internal scanning to proactively find and remediate vulnerabilities. Conduct annual external and internal penetration testing and after any significant infrastructure or application upgrade. Another option that is gaining in prominence among more security-mature companies (which have already performed well on penetration tests) is red team assessments, which take things one step further to test the effectiveness of a company's security program.

WHAT YOU AND YOUR TEAM CAN DO

Ensure system-hardening guidelines are in place and that you have a plan to patch known vulnerabilities as soon as they are available. As for configuration efforts, execute a strong change-control process to track all changes made to systems in your environment.

THREAT:

INTERNET OF THINGS

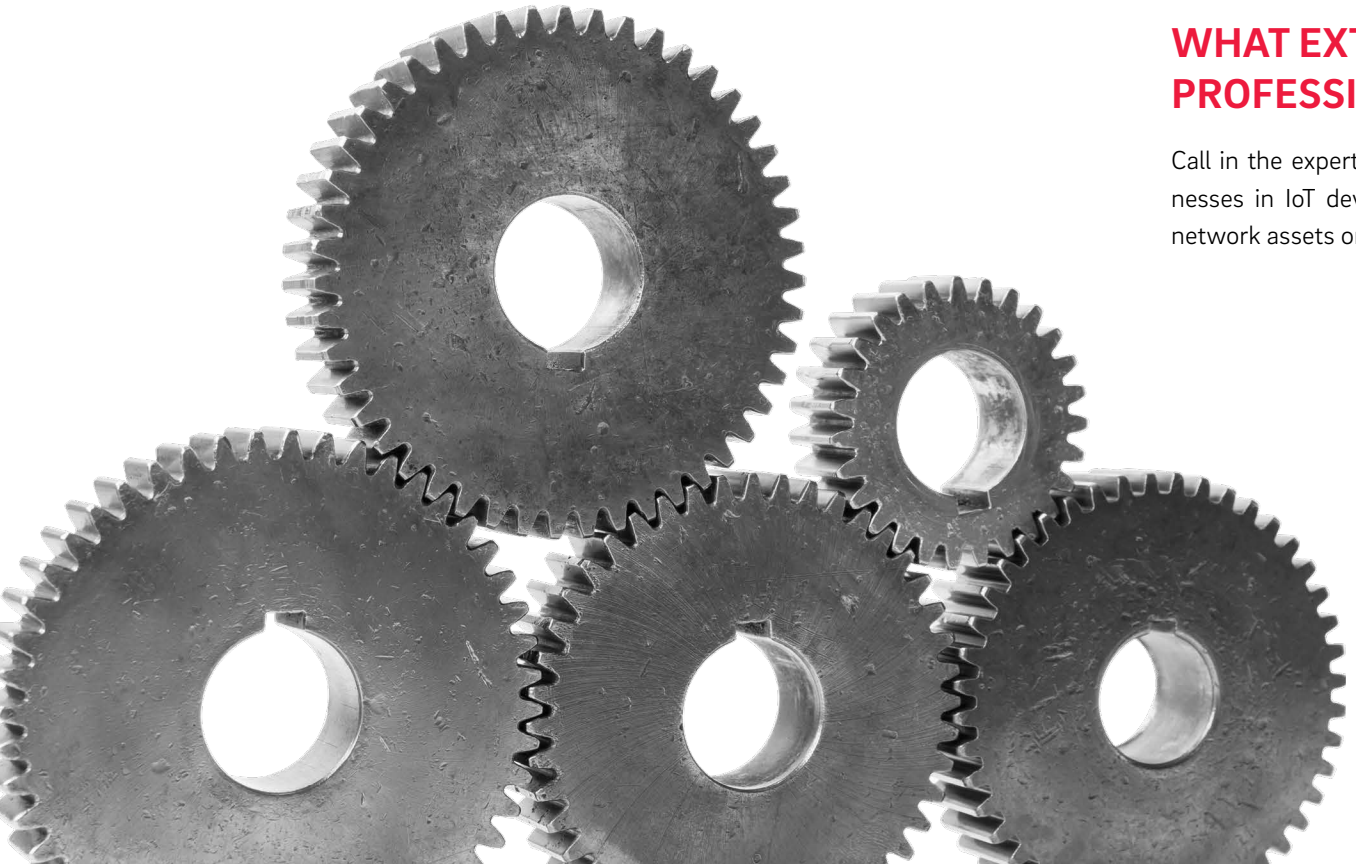
The Internet of Things (IoT) often lacks the same visibility on the threat landscape compared to many on this list. This is partly because smart technologies are still relatively nascent and partly because they lack the traditional look of a vulnerable endpoint – having no traditional keyboard or screen in many cases. But there is plenty to fret about. Every new web-enabled endpoint or asset you connect to your network, from routers to refrigerators, potentially adds another attack vector. What makes embedded devices particularly at risk is a lack of software hardening often due to a rush to market, as well as the common difficulty of distributing software updates and patches to these devices.

WHAT DOES AN ATTACK LOOK LIKE?

Let's pretend you're a food supplier: An attacker takes advantage of an unpatched vulnerability to take complete control of one of your warehouse thermostats. They then raise the temperature so that your inventory spoils or decrease the dial so that your pipes burst during cold weather. Aside from leveraging connected devices to directly impact your business, adversaries may also be interested in using these technologies to simply stake a foothold on your network as they look for other vulnerable targets.

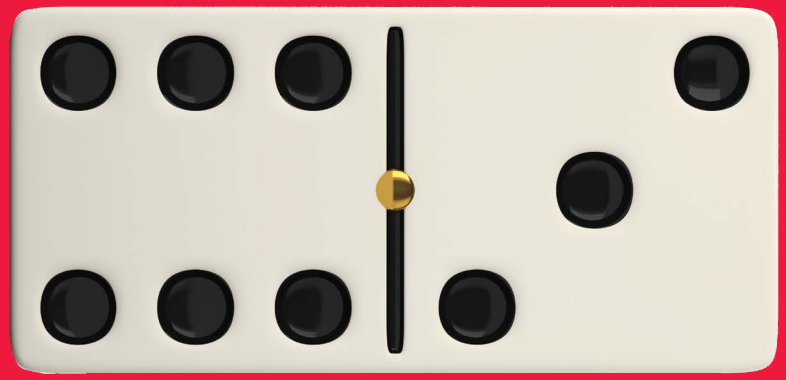
WHAT YOU AND YOUR TEAM CAN DO

Vendors of IoT may not consider the security of their products as important as you do. Learn as much as you can about the technologies you buy, how they handle data collection and how they are protected. Do the vendors have a history of insecure products? Have they been compromised before? After purchasing, swap out your default passwords for something much stronger and place the device behind your enterprise firewall and perhaps on its own protected segment dedicated to potentially risky IoT devices. Finally, make sure it is patched and up to date moving forward.



WHAT EXTERNAL PROFESSIONALS CAN DO

Call in the experts to help test for security weaknesses in IoT devices and then to monitor these network assets once they are up and running.



THREAT:

SUPPLY CHAIN

If you think you're safe because your security posture is making strong headway, don't let your friends drag you down. You may view your partners as extensions of your own success, but they pose real danger if not properly controlled. While critical infrastructure sectors are most susceptible to these type of attacks, adversaries have subverted the supply chain to also compromise everything from health care companies to big-box retailers. And despite vast numbers of recent data breaches originating at third-party sites, recent studies have shown that most companies don't hold their vendors to the same security standards as they do themselves. Regulations are starting to require companies do more around third-party risk – expect that to only increase.

WHAT DOES AN ATTACK LOOK LIKE?

Because the supply chain is so expansive, these types of attacks take on a wide variety of looks and feels. Incidents can range from your law firm being compromised to steal sensitive client information to your climate control vendor being hit with data-stealing malware that pilfers network credentials to equipment and software you're buying being infiltrated to deposit malware before it ever reaches your or your customers' hands.

WHAT YOU AND YOUR TEAM CAN DO

Trust nobody, even those who help enable your business. Quiz your third-party developers on their security standards. Create a mature policy that requires them to agree to follow your organization's policies and guidelines. Ensure network segmentation is in place so tech installed by your suppliers never touches more sensitive parts of the corporate network, like point-of-sale systems.

WHAT EXTERNAL PROFESSIONALS CAN DO

It's likely necessary that you turn to outside help for a more professional and through risk assessment. And if that evaluation uncovers glaring imperfections, experts can help you test for vulnerabilities that may be opening your partners – and in turn, you – up to sabotage and compromise. Businesses are also notoriously slow to detect and respond to supply chain attacks, so you'll want to turn to external specialists for help in this department as well.

FOR MORE INFORMATION AND ASSISTANCE IN ADDRESSING THESE 12 THREATS, VISIT TRUSTWAVE.COM