YOUR BUSINESS IS UNDER ATTACK

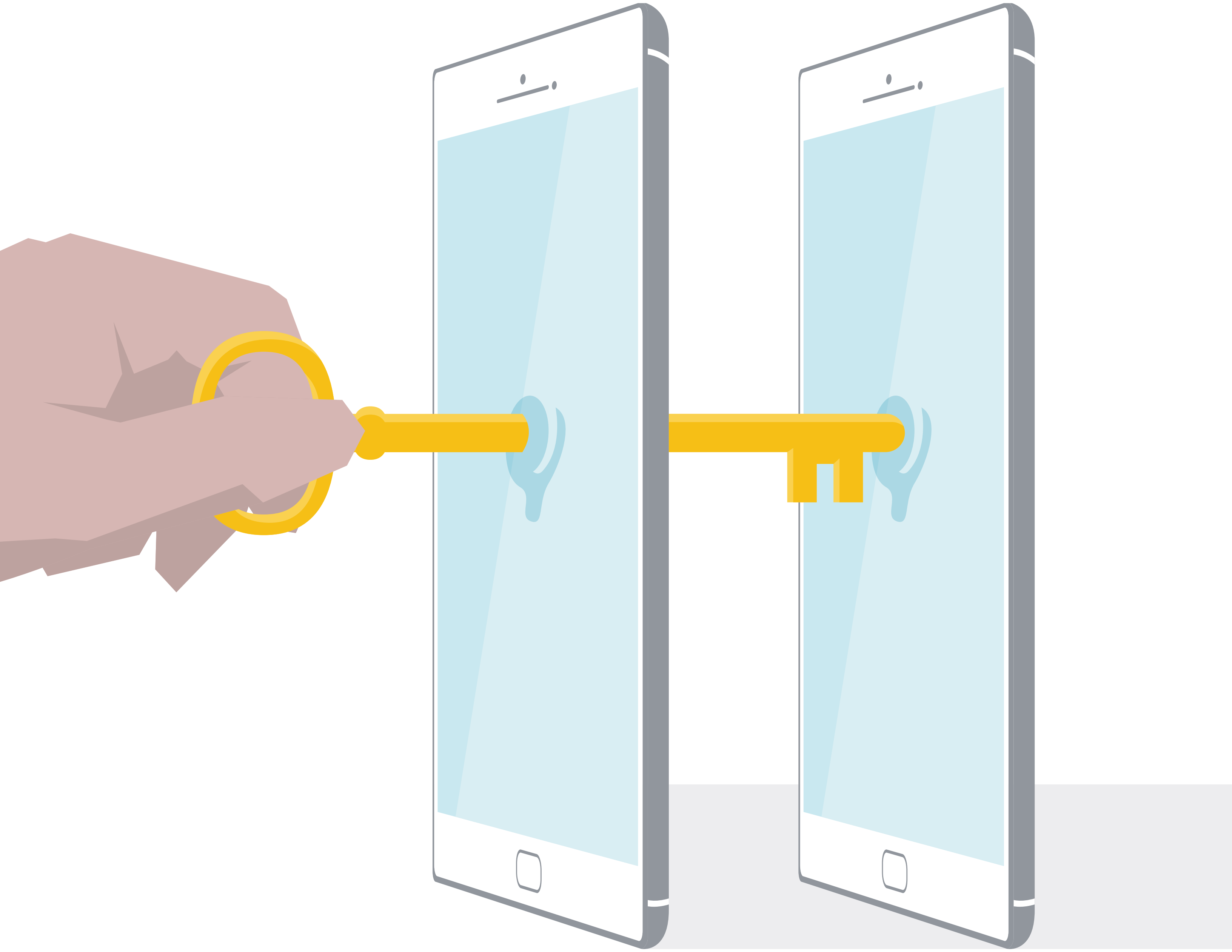
A GUIDE TO BUILDING STRONG CYBERSECURITY DEFENSES

COMCAST **BUSINESS**
BUILT FOR BUSINESS

TABLE OF CONTENTS

Hackers don't discriminate by size.

Cyberattacks on small and midsize businesses (SMB) are a common occurrence. While smaller organizations often lull themselves into thinking cybercriminals aren't interested in them, reality is quite different. It's true the biggest headline-grabbing hacks typically involve large companies, but anyone could be a target. Hackers don't discriminate by size.



More than half (55 percent) of companies with fewer than 1,000 employees have experienced a cyberattack, and **43 percent** of all attacks target small businesses. These statistics make it clear all businesses need a solid cybersecurity strategy. Be it **ransomware**, DDoS (distributed denial of service), phishing or some other threat, there is no shortage of cyber threats targeted at small businesses. Any business that neglects its cybersecurity responsibilities is taking a huge risk. And because businesses are more and more connected with each other, the risk extends to the company's customers, partners and suppliers.

> **Any business that neglects its cybersecurity responsibilities is taking a huge risk.**

The seriousness of the threat, however, isn't always fully understood by small businesses. For instance, only **2 percent** of small business owners in a CNBC/ Survey Monkey poll in April 2017 cited cyber threats as the most critical issue they face. Understandably, small businesses have other concerns, but overlooking cybersecurity could be a costly mistake.

SECURITY FOOTPRINT

Unified Communications (UC) provides easy access to tools and apps from multiple devices. Screen sharing, web and audio conferencing, virtual workspaces, smart whiteboards, and team chat can be integrated with project management and workflow systems to make it easier for individuals and teams to meet remotely and collaborate with one another.

> **Overlooking cybersecurity could be a costly mistake.**

MULTIPLE THREATS

Hackers use a wide range of methods to target businesses, ransomware being the most common these days. Ransomware locks up computers and encrypts data. For owners to regain access to their data, they have to pay ransom to a hacker who then releases a decryption key. Because of its prevalence, ransomware is discussed in greater detail later in this document.

MALVERTISING

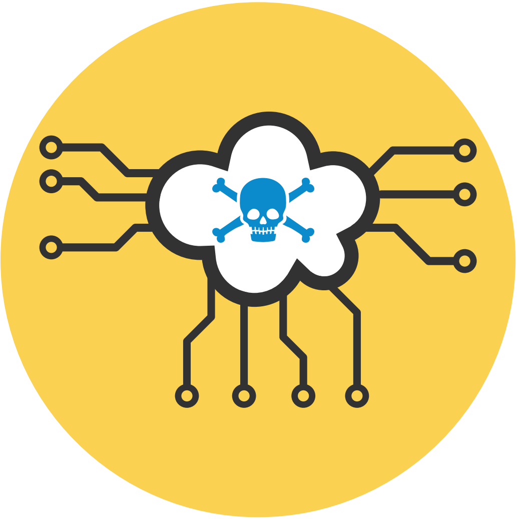
Short for "malware advertising," it consists of delivering malware to a network after a user clicks on an apparently legitimate ad. Identifying malvertising isn't easy because of the way it hides itself, but some advanced malware detection systems are getting better at it.

CLICKJACKING

Similar to malvertising, this practice involves hiding hyperlinks to compromised webpages in legitimate website links. Users then are asked to reveal personal data that hackers steal for nefarious purposes.

PHISHING

Often providing a gateway for ransomware infections, phishing typically works by goading users into clicking an email attachment or URL containing a virus. Phishing has become more and more sophisticated , as hackers target specific individuals with messages they can't resist.



DRIVE-BY DOWNLOADS

This dirty trick downloads malware into networks, often without users realizing what is happening. Sometimes users have to respond to a pop-up window for the download to occur but other times all you have to do is unwittingly visit a compromised website.

SOFTWARE VULNERABILITIES

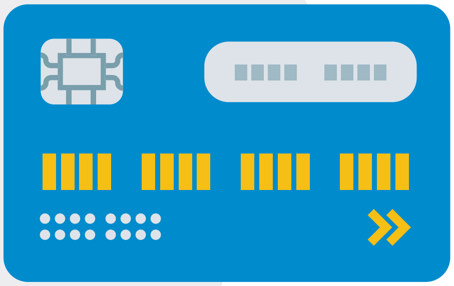
Hackers exploit vulnerabilities in popular web platforms such as Wordpress, tools such as Java and file formats such as HTML, PDF and CSV to deliver malware.

SOCIAL MEDIA DATA THEFT

Information that users share willingly on social media can be hijacked to break into networks and craft targeted phishing emails.

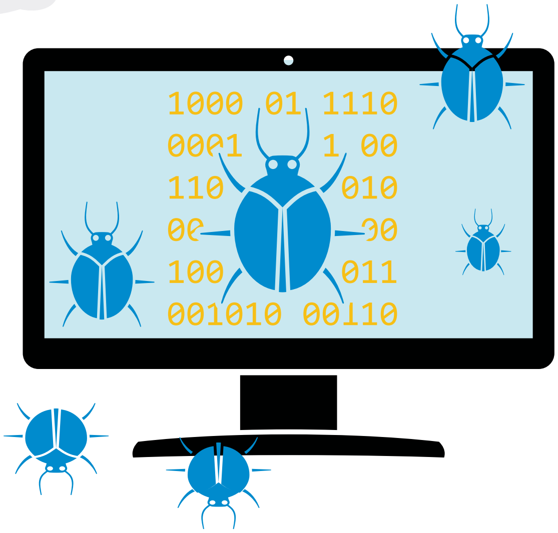
WHY YOU?

Why are cybercriminals interested in small businesses? After all, small and medium companies do not have the resources and deep pockets of enterprise companies.



VALUABLE DATA

Hackers target small businesses for several reasons. One is obvious: They know that even small companies traffic in data that carries a dollar value on the Dark Web – medical records, credit card information, Social Security numbers, bank account credentials or proprietary business information. Cybercriminals are always trying to come up with new ways to steal this data. They either use it themselves to get into bank accounts and make fraudulent purchases or sell it to other criminals who will use it.



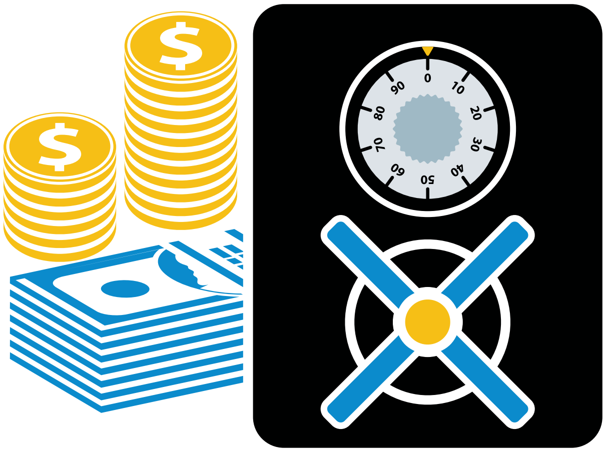
ARMY OF ROBOTS

Sometimes cyber hackers are interested only in using a company's computers, and conscripting them into an army of bots to perpetrate massive DDoS attacks. DDoS works by artificially generating enormous amounts of web traffic to disrupt service to a company or group of companies. The hijacked bots help generate the disruptive traffic.

> **As long as an attack method proves lucrative, hackers will keep using it.**

INTER-BUSINESS LINKS

Today's businesses are digitally connected to each other to complete transactions, manage supply chains and share information. Since larger companies presumably (although not necessarily) are tougher to penetrate, hackers target smaller partners as a way to get into the systems of large companies. This is what happened in the Target breach of 2014.



PROFIT - PURE & SIMPLE

When you think about it, cyber hackers target small businesses – or any other company — primarily for profit. Sure, some attacks are primarily about disruption, as is the case with DDoS, but usually the motive is to make money. This explains why ransomware is such a popular method of attack. It often succeeds, generating revenue for attackers. And as long as an attack method proves lucrative, hackers will keep using it.

SETTING A STRATEGY

Understanding the threats and what cybercriminals are after is essential to building strong cybersecurity defenses. If you know your enemies, you have a better chance to defeat them. In developing a cybersecurity strategy, here are some essential components:

EDUCATE USERS

Countless phishing and ransomware attacks have proven that unaware or careless users can be a company's biggest security risk. Businesses can turn users into the front line of defense by properly educating them on cyber threats.

IMPLEMENT ADVANCED TOOLS

Businesses need tools that deliver endpoint protection, secure the network through firewalls and other methods, and perform threat analysis to keep their data safe. Cloud-based platforms that address multiple security layers typically are the easiest, most affordable path to cybersecurity for small businesses.

> **If you know your enemies, you have a better chance to defeat them.**

INVEST IN EXPERTISE

It’s hard to have a full grasp of cybersecurity without expert help. For smaller companies, working with a managed security services provider (MSSP) is the best bet, though even businesses with in-house experts can benefit from tapping a provider.

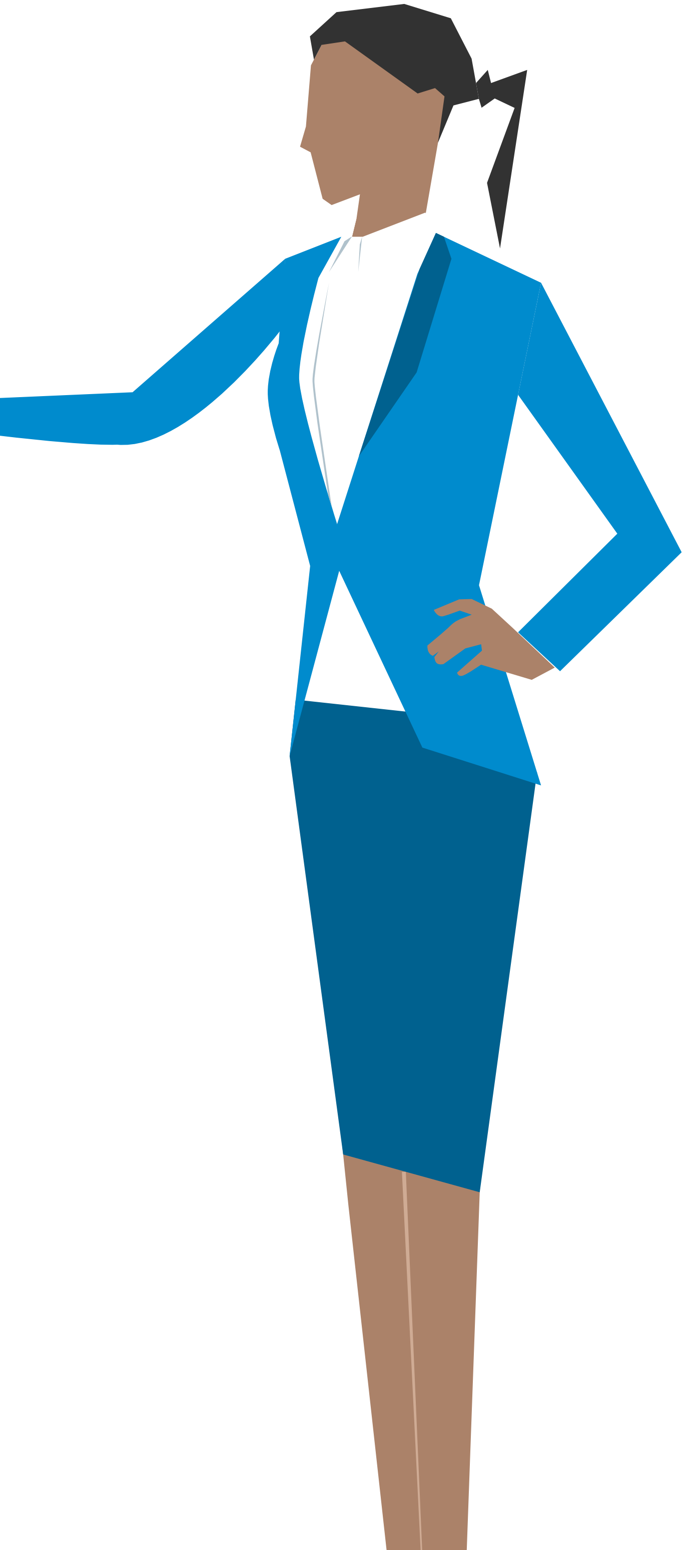
SECURE MOBILE DEVICES

As computing becomes more mobile and cloud-based, companies must include mobile devices in their security strategies or risk leaving a door open to cyberattackers.

HUMAN ELEMENT

When hackers succeed, it's often because they target unsuspecting users. They know users are busy, trusting or distracted, and as a result, let their guard down when a suspicious email lands in their inbox or they chance upon a sketchy-looking website. Most cybersecurity incidents involve some type of user activity, be it clicking an infected attachment, visiting a compromised website, making passwords too easy to crack, misconfiguring a system or even sharing a computing device.

Most cybersecurity incidents involve some type of user activity.



Activity resulting in cybersecurity breaches usually is not malicious. Often it's just careless. A recent survey of 1,000 IT professionals shows that careless workers cause more than half (54 percent) of cybersecurity incidents. Examples of such breaches in recent years include:

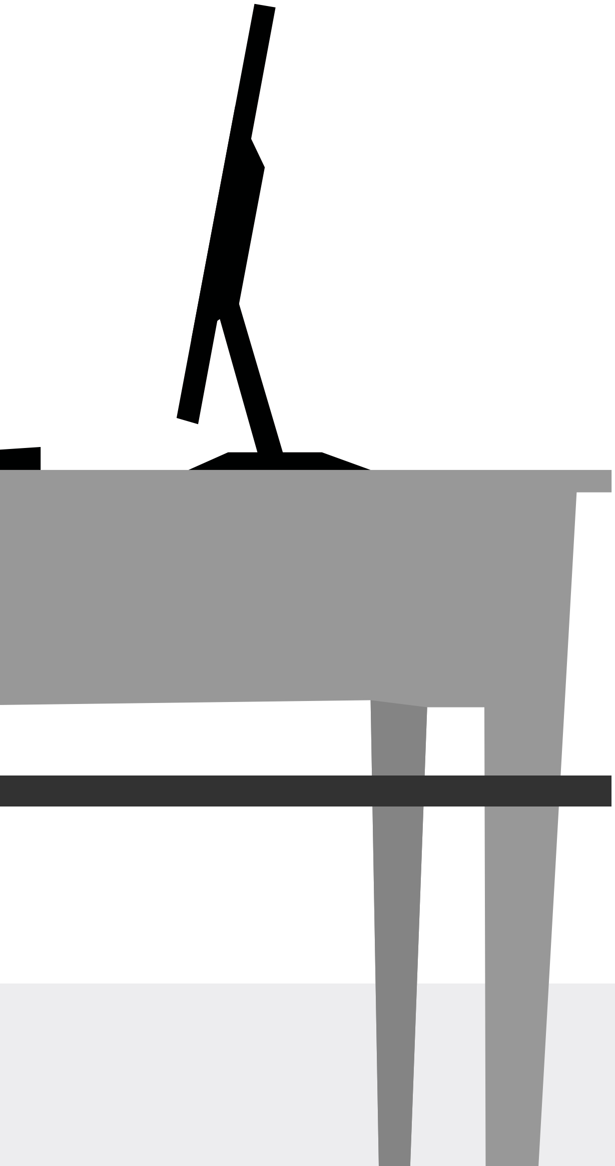
- Through social engineering, the credentials of an insurance company's administrator were stolen to break into a database containing employee and customer data such as names, addresses, Social Security numbers and income data.
- Hackers broke into a bank's servers after administrators forgot to implement two-step verification to access one of the bank's systems.
- Hackers used a third-party vendor's stolen username and password to break into a retailer's systems and steal millions of credit card numbers.

Such incidents are the reason users are often referred to as the "weakest link" in IT security. But they don't have to be. Instead, businesses can turn their employees into their first line of defense by educating them about cybersecurity threats, promoting safe computing practices and implementing well-crafted policies to protect data. A focus on the "human element" of cybersecurity is more than a good idea; it's an absolute necessity to help prevent cyberattacks. It takes only one bad decision by one user for a ransomware infection or some other malware attack to disrupt your operations for hours or days.

USER EDUCATION

Education is key to addressing the human element of cybersecurity. Raising user awareness of cyber dangers should be a priority for all businesses. Cybersecurity training is most effective as an ongoing effort ideally combining in-person sessions, online courses and awareness campaigns with email reminders and posters.

Raising user awareness of cyber dangers should be a priority for all businesses.



Topics to cover should include the following:

- Identify and avoid suspicious emails. This will help users avoid phishing attempts with URLs or attachments programmed to download malware into your network.
- Set and enforce strong password policies. Teach users to come up with strong passwords or passphrases, and enforce policies to change passwords frequently and prohibit password sharing.
- Set browsers to warn users when visiting a site that has been flagged as containing malware.
- Block downloads from suspicious or unsanctioned sources.
- Prohibit users from sharing company-owned laptops and mobile devices.
- Teach users not to access sensitive company data through public WiFi networks.

COMMON SENSE POLICIES

Technology alone cannot guarantee the security of a company's data. User education must be supported by common sense policies. If you train users and do nothing to enforce security rules, chances are users will fall back on bad habits that can lead to a breach.

Security policies are multidimensional. Password policies are a good start point, but businesses also need to address who gets access to which systems. Employees should be granted permissions only to those systems they need to do their jobs.

Businesses also need rules on whether employees are allowed to use their own mobile devices at work (BYOD). If so, those devices need to be monitored, secured with endpoint protection, encryption and — in case of loss or theft — wipe capability. Mobile devices also should be containerized to keep company data separate from personal files.

When employees leave the company, take immediate steps to disable access to company systems, make sure all company-owned devices are returned, disable the employee's email address, and change passwords to sensitive company assets for which the employee had privileges. All of these steps seem obvious but businesses often neglect them.

User education must be supported by common sense policies.

HOW TO FIGHT RANSOMWARE

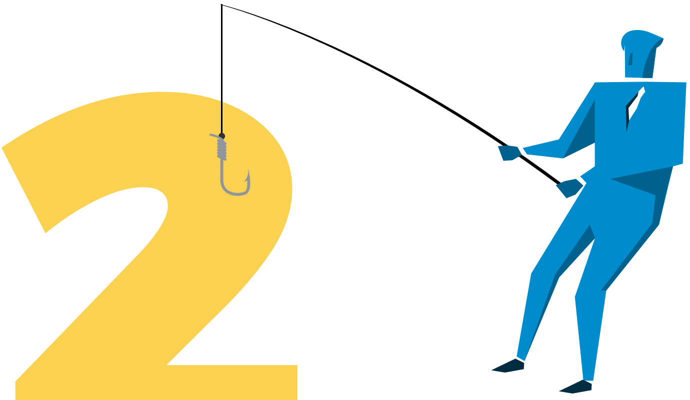
As already noted, ransomware is a major problem for businesses of all sizes. Ransomware attacks occur at an alarming rate — every **40 seconds** a company is hit. When the attack succeeds, a pop-up appears on a computer screen saying all data has been locked and access can be restored only if the user pays ransom.

The average ransom demand is over $1,000, though organizations have paid tens of thousands in some cases. Nearly half of ransomware attacks infect **20 computers** or more, so an attack on a small company could halt operations for days.

Ransomware is currently the number one cybersecurity concern for a reason – it's effective. Too many companies fail to plug their security holes, essentially issuing hackers an open invitation to attack. To avoid becoming another ransomware statistic, businesses need a solid cybersecurity strategy that includes the following elements:

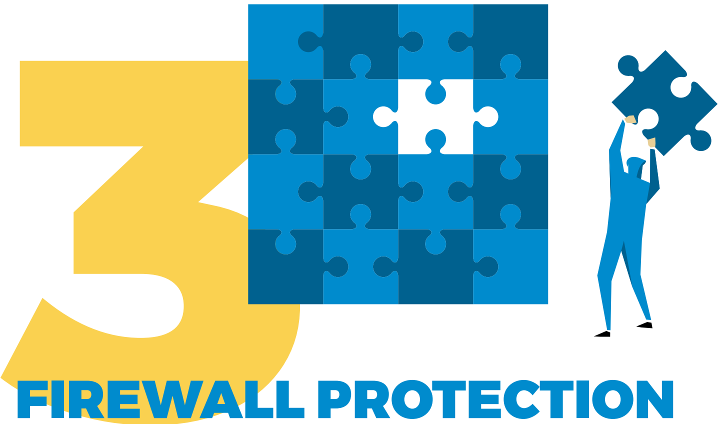
ENDPOINT SECURITY

Endpoint security is a more comprehensive version of the traditional antivirus tools that protect computers from malware. Traditional tools block only the malware they recognize, based on signatures that have been written into the AV software. The more sophisticated endpoint protection platforms scan and block malware, and use machine learning to identify zero-day threats and other previously unseen malware, including many ransomware variants.



ANTI-PHISHING TOOLS

Although hackers use other methods to deliver ransomware, phishing remains a favorite because it preys on user trust, curiosity and fear. Anti-phishing tools, such as email and spam filters, sift out malicious URLs and attachments to prevent users from unwittingly downloading malware.



FIREWALL PROTECTION

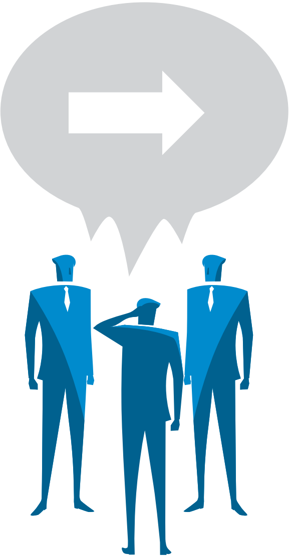
Firewalls block unauthorized content with controls such as access denial to IP addresses known to deliver ransomware. Even if a ransomware payload is delivered, a firewall can prevent it from communicating with the command and control server from which it would receive instructions to lock out data. This could stave off infection until the ransomware is detected and removed.

PATCH MANAGEMENT

The fast-spreading WannaCry and Petya ransomware attacks in 2017 exploited Microsoft's Windows Server Message Block (SMB) protocol. Fixing those vulnerabilities would have prevented infection, which is why patch management is critical to fighting ransomware and zero-day threats. Businesses need strict patching policies so users don't ignore software update prompts. Preferably, businesses would deploy automated patch management.

5 ACCESS CONTROLS

Limiting access to sensitive data to the least number of users possible helps prevent attacks. Employees should get access only to data they need to do their jobs, so access controls for files, directories and network share permissions should be configured with that in mind. This helps minimize leaks and makes it easier to identify its origins if one happens.



6 MACRO SCRIPTS

A common method of delivering ransomware is to hide it in macro programs that get into systems when users open or download a compromised file. Macros automate repetitive tasks with toolbar buttons and keyboard shortcuts in applications such as Microsoft Word and Excel. Disabling macros in the Office Preferences dialogue box can prevent these types of infections.

BACKUP AND RECOVERY

Regular data backups are key to fighting ransomware. An automated data backup and recovery solution is preferable because you don't have to rely on users to do it. If struck by ransomware, your business can simply restore its data to resume operations after the malware is removed.

USER AWARENESS TRAINING

The need for user education in cybersecurity cannot be overstated. Users need to learn about cyber dangers and how to avoid them. Training should be ongoing to cover new threats and remind users of safe computing practices. When it comes to security awareness, repetition is safety.

PREPARE AN INCIDENT RESPONSE PLAN

Prevention is critical to a cybersecurity strategy but you cannot ignore another critical component — incident response. Since no security measure is 100 percent foolproof, businesses must prepare for the eventuality of a breach.

Every business should have an incident response plan (IRP) outlining what steps to take and who is responsible for the response following a breach. As many as **75 percent** of companies have not prepared an IRP, according to the Ponemon Institute.

That's a problem because without an IRP, it's hard to minimize the damage of a breach if you're unclear on what actions to take. Some malware infections spread at lightning speed once a network has been breached, so reaction time is critical. As we saw in May 2017 with the **WannaCry** ransomware outbreak, infections can cross country borders and hop continents in a matter of hours.

Trying to come up with a response plan after an incident occurs is already too late. And remember, cybersecurity experts warn that for most businesses, a cyberattack isn't a matter of if but when.

An IRP should be tailored to each company's specific needs and circumstances, which means no two plans are alike. However, each plan should include these components:

BUILD A CROSS-FUNCTIONAL TEAM

Responding to a security breach involves more people than those in charge of IT and cybersecurity. Technical staff are usually the first to spring into action following an incident as they seek to identify the problem, assess damage and start remediation, but the response also includes non-technical aspects. In addition to employees, it may be necessary to notify customers and suppliers about the breach, so there is work to do for management and other teams such as marketing, PR, HR and legal.

CLARIFY RESPONSE ROLES

Once the team is in place, every member needs to know his or her role and responsibilities, and exactly what steps to take immediately after being notified of a breach. For instance, the first steps for technical staff will be to identify and isolate infected systems, and determine where the breach occurred and how far the infection has spread. Team members must be given the appropriate authority to act quickly such as taking a system offline.

DEFINE SECURITY INCIDENTS

The IRP must define what constitutes an incident, how to prioritize different types of incidents and what are the appropriate steps for each type. An unsuccessful hacker attack still may require some sort of response, such as updating threat intelligence tools, hardening certain systems and notifying management. The National Institute of Standards and Technology (NIST) provides guidelines on what constitutes incidents and how to prepare for them.

SPECIFY PROCEDURES

To remove any doubt as to how to proceed following an incident, the plan should be detailed and clear in its prescribed steps for recovery. It should include contingencies such as resuming operations from an alternative location, in case of damage to a building, and how to access remediation tools from remote sites and mobile tools if the breach occurs after hours or when response team members are away.

ANTICIPATE HACKERS' MOVES

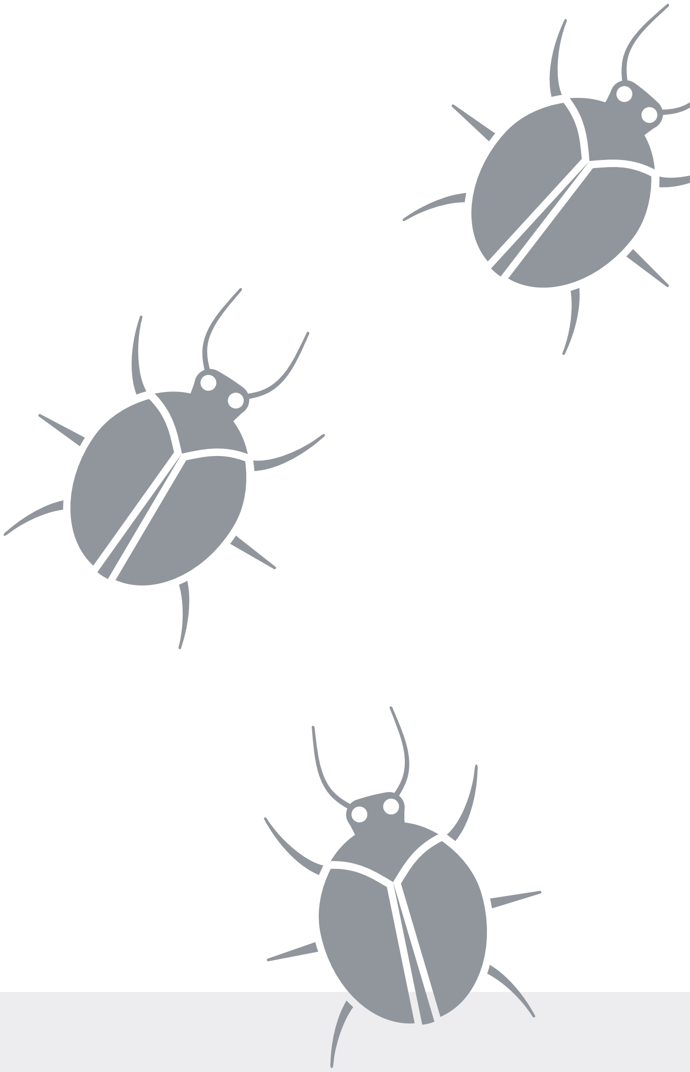
Most companies handle intellectual property and private data such as employee medical records and Social Security numbers, as well as private customer and partner information such as payment card credentials and bank account numbers. Hackers target these types of data because they can sell the information for a profit on the black market. A response plan should include an immediate check of the systems that house sensitive data to determine if they've been breached.

TEST THE PLAN

To ensure a response plan is effective, businesses should test it periodically, drilling all relevant parties with exercises and simulations. Testing is critical because it will reveal weaknesses and omissions you wouldn't want to discover after a breach already has occurred.

DOCUMENT AND COMMUNICATE

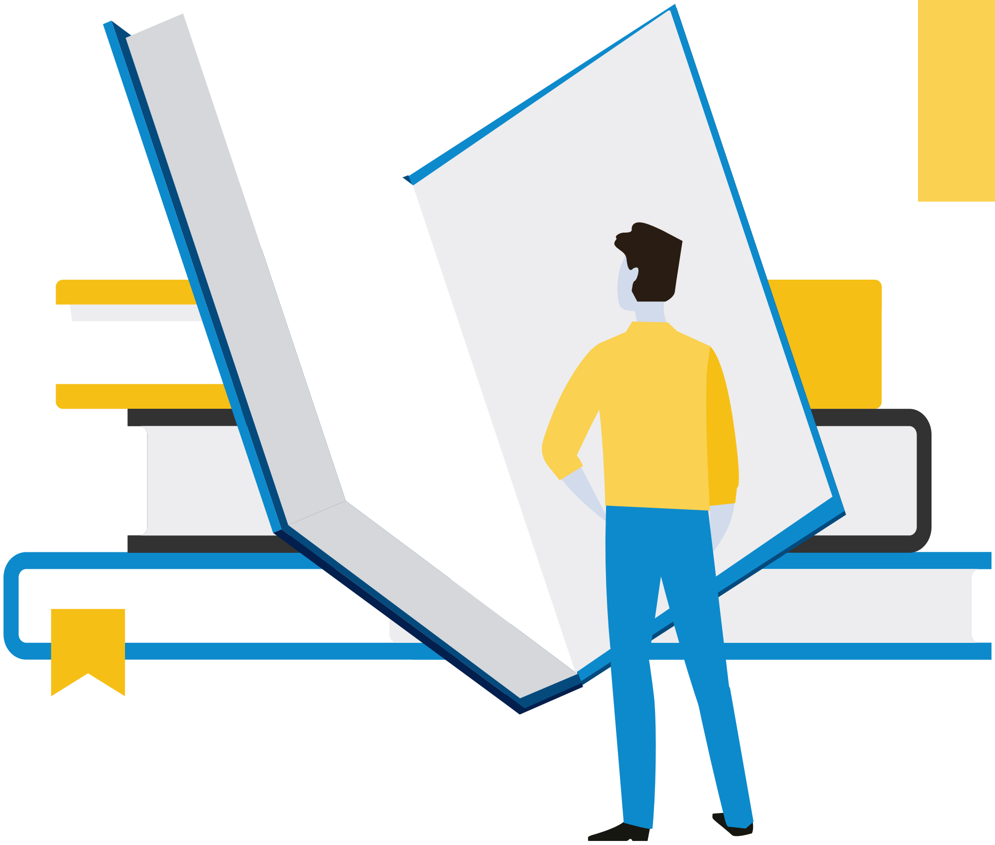
Without proper documentation, an IRP's effectiveness is limited. Every single action, process and procedure should be faithfully documented in clear language and shared with everyone involved in the response. All employees should receive a version of the plan, and required to read it and sign an acknowledgment of the plan.



FIVE KEY SMALL BUSINESS CYBERSECURITY TIPS

Large enterprises typically have the resources to protect their networks against the ever-evolving cyber threat landscape. But smaller businesses have tighter budgets and fewer resources. Hackers know that, which is one of the main reasons they target small businesses.

A cyberattack can have serious consequences. A 2017 VIPRE Security **study** found that 66 percent of IT managers at companies of up to 1,000 employees fear an attack can shut them down temporarily or for good. These are high stakes. With that in mind, here are five key security recommendations for small businesses:



EDUCATE USERS

No amount of technology can completely protect your network and data. User training and awareness, therefore, are crucial to building solid defenses.

2

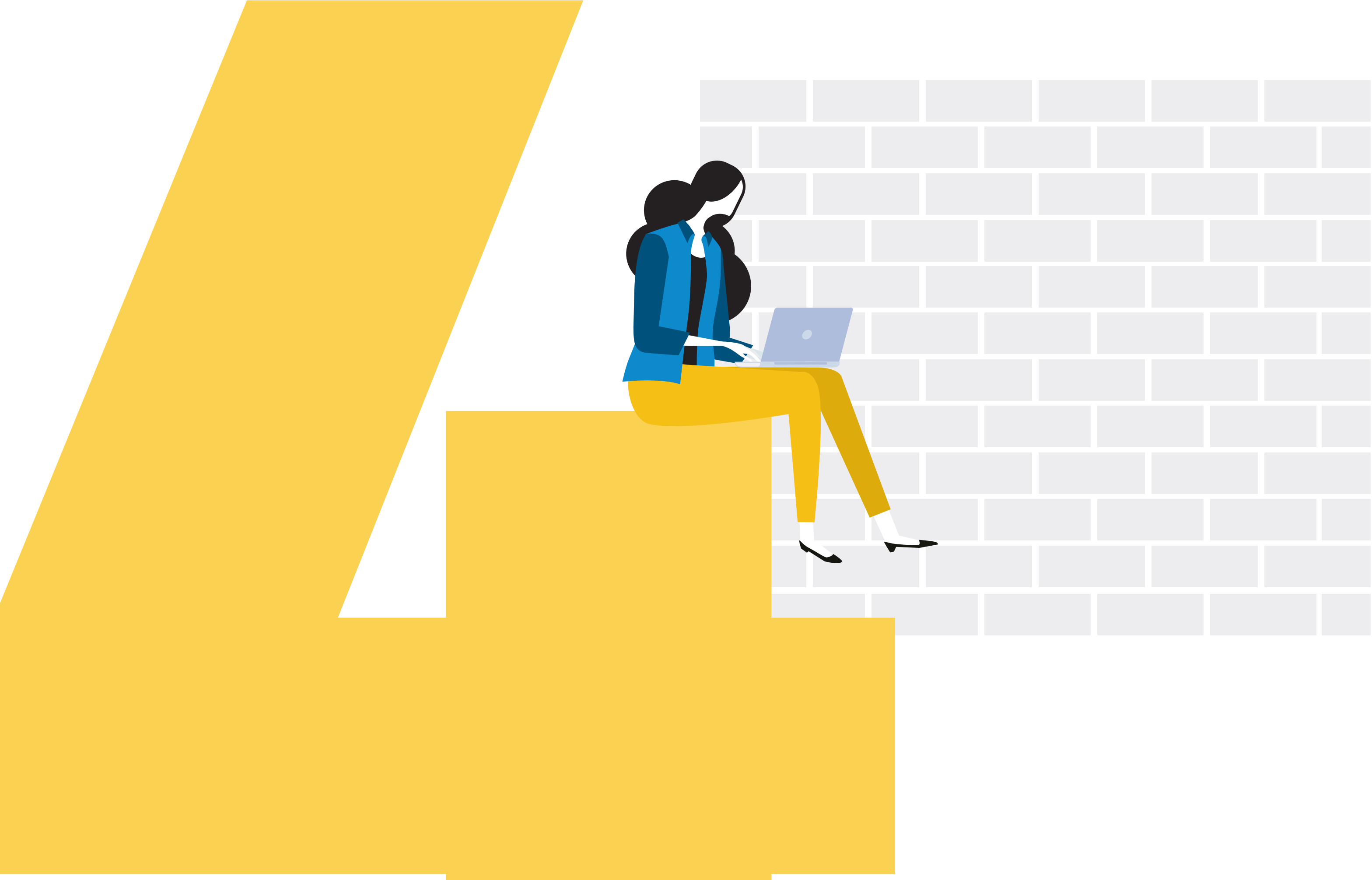
SECURE ENDPOINTS

From stationary workstations to laptops to mobile devices, all endpoints must be secured to help prevent a breach. Select an endpoint solution with advanced protection that can spot zero-day and other previously unknown threats.

3

APPLY SECURITY PATCHES

Left to users, many security patches will be ignored, creating vulnerabilities that hackers know how to exploit. Implement a strict patch management policy, preferably using an automated process to take users out of the equation.



DEPLOY FIREWALLS

Think of a firewall as a sentry that allows only authorized guests into a building. Firewalls let you choose which types of content to allow into your network, blocking unauthorized data while still allowing outbound communications.

5

ENFORCE PASSWORD POLICIES

Although users tend to resist them, passwords are necessary and should be changed regularly. Require users to use combinations with numbers, special characters and upper and lowercase letters to make passwords harder to crack.

CONCLUSION

In its most recent **State of Cybersecurity in SMB**, the Ponemon Institute reported the number of small businesses that experienced breaches "involving sensitive information about customers, target customers or employees" increased to 54 percent from 50 percent in one year, and ransomware attacks jumped to 52 percent from 2 percent. Nearly one third of companies that were breached did not know the root cause of the attacks.

This means they did lack the systems and practices to not only stop a breach but also figure out how it happens. Considering the relentless pace of cyberattacks, this is too risky. SMBs need strong, well-executed cybersecurity strategies.

With Business Internet from Comcast Business, you'll have access to the latest Internet security to protect your network against unwanted intruders. Learn more at ComcastBusiness.com

COMCAST BUSINESS

BUILT FOR BUSINESS