GETTY IMAGES

THE BUSINESS OF CYBER SECURITY

MBJ: How big is the cyber risk facing small businesses these days? What are some of the potential consequences of a major cybersecurity breach at my business?
Dan Weddle: The cyber risk facing small businesses today is greater than it has ever been. Threat actors aren't just focused on large corporate and government targets — it's a numbers game. By attacking businesses of all sizes, hackers have the chance for larger payouts. Hackers are also aware that small businesses are likely less secure and have minimal resources to mitigate an attack, making them more likely to pay a ransom demand.

The two biggest consequences of cybersecurity attacks for businesses are destruction of data and disabling of systems. This is usually due to ransomware. The other is a data breach that exposes sensitive client or personnel data. Both are typically accomplished through phishing schemes.

Melody McAnally: Forty-three percent of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves, according to the Ponemon Institute. For small business owners, this means it is no longer a matter of if security threats will arise but when.

Hiscox, an insurance carrier, estimates each data breach costs a small business $200,000 on average, and the National Cyber Security Alliance reported 60% go out of business within six months of being victimized.

What are some of the types of cyberattacks that could affect a business?
Weddle: The most common type of attack is email phishing. Hackers are skilled at making emails look legitimate and attaching documents or links that direct you to malicious content. Unfortunately, this is often one of the most difficult attacks to prevent, as it requires security systems and continuous end-user training.

Ransomware attacks are also common. They are usually deployed from a phishing attack and utilize malicious code to encrypt files and demand a ransom. Vishing is similar to phishing but uses a phone call and social engineering to convince a user to provide the hacker with access to a device or credentials.

Hackers also use unpatched systems and software to gain network access and introduce malware. Denial of service attacks are also common.

McAnally: Phishing email attacks are the main type of cyberattacks facing all businesses. Phishing increased by 52% in 2018 with nearly one-third of all data breaches in 2018 involving phishing, according to Verizon's 2019 Data Breach Investigations Report.

Popular phishing emails pose as Microsoft and Amazon, asking the user to click a link to change one's username and password and state an urgent purpose. If employees receive an email requesting they change their username and password, they should contact their business's IT helpdesk, as it is probably a scam.

What are some of the key components of a plan to reduce the chances of being hit by a cyberattack?
McAnally: The National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce Cybersecurity Framework provides the most comprehensive plan to reduce cyberattacks:

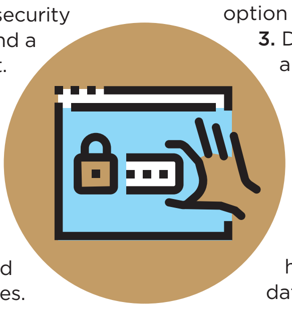
1. Identify: Create an inventory all of your equipment, software, and data, including smart phones, tablets, and point of sale devices.
2. Protect: Control who logs on to your network, particularly administrator access and third-party vendors' access. Encrypt sensitive data at rest and in transit (email). Conduct regular backups of data. Update security software patches regularly. Train everyone about cybersecurity risks, particularly phishing emails.
3. Detect: Monitor your network for unauthorized access and software. Investigate any unusual activities on your network or by employees, such as large data exports.
4. Respond: Have a data breach response plan.
5. Recover: After an attack, repair and restore your network and equipment.

Weddle: The most important thing for a business to do is to educate their employees continuously.

Teaching users what to look for in phishing attacks is crucial in minimizing the risks of email-borne attacks.

Businesses also need to have a solid backup and disaster recovery strategy. It is critical to understand your businesses needs around recovery points and recovery times to ensure that you have a backup solution that can meet those requirements. Your backup solution should also provide segregated storage of your backups, preferably in the cloud.

Some other things your business can implement include email security filtering, two-factor authentication, DNS security filtering, web content filtering, and a smart endpoint protection agent.



Businesses should also consider implementing a comprehensive "security stack." This includes several things:

- A Security Appliance, commonly referred to as a firewall, with regular rule reviews.
- Regular patching of devices and systems to minimize vulnerabilities.
- DNS-based content filtering to block malicious sites and IP addresses.
- Email security filtering to help remove threats before they make it to a user's inbox.
- Web content filtering to restrict users from sites that are known to carry malware and other malicious content.
- Endpoint protection for servers and end-user devices to stop or mitigate damage from viruses and malware.
- A comprehensive backup and disaster recovery solution to allow businesses to recover when all other measures fail.
- Multifactor authentication enabled on every system that supports it.
- Security awareness training for end users on a regular basis. It should include routine email phishing tests designed to help users identify and mitigate potential malicious attacks.
- Documented policies and procedures that provide a clear definition of the security responsibilities of users and a well-defined path of action in the event of an attack.
- An annual review (at the least) of these items for configuration and accuracy.

Which types of companies/partners can help me reduce the likelihood for a cyberattack?
Weddle: Your cybersecurity partner should be able to provide a comprehensive security solution that provides tools for your infrastructure, data transmission, and endpoints. Additionally, you need a partner who can train users and provide valuable insights to help you make educated decisions.

ProTech is focused on providing all these things for our clients and would love to help every business improve their security.

McAnally: The U.S. Department of Homeland Security's (DHS) Cyber Resilience Review (CRR) is a non-technical assessment to evaluate operational resilience and cybersecurity practices. You can complete the assessment yourself or request an on-site assessment by DHS cybersecurity professionals.

DHS also offers free cyber hygiene vulnerability scanning for small businesses. This service can help secure your internet-facing systems from weak configuration and known vulnerabilities. You'll also receive weekly reports.

What types of questions should business owners or managers ask when assessing their cyber risk or choosing a third-party partner to help them improve their cybersecurity?
Weddle:
1. Are all my systems patched?
2. Do we have a reliable backup and disaster recovery solution in place?
3. Is our backup data stored locally or in the cloud?
4. Are my firewall policies up to date?
5. Do we have a robust antivirus and anti-malware solution on every endpoint?
6. Are we meeting all compliance and regulatory requirements?
7. Is my security partner experienced in managing and supporting different solutions?
8. Does my security partner follow best-in-class security measures?

McAnally: Many small businesses outsource their IT to third-party vendors. Be sure to do your due diligence by asking the following:
1. Do you use multifactor authentication, which is the gold standard of IT security?
2. Can you provide regular assessment and reporting of your backup data, including the option for off-site data backup?
3. Do you run the latest versions of all software and operating systems, since hackers frequently target software vulnerability and security flaws?
4. Do you conduct regular cybersecurity training for my employees?
5. How securely do you handle your sensitive business data and what data security measures do you have in place to avoid cyberattacks?

What are some of the legal ramifications companies face when it comes to protecting their customers' secure information against cyber threats?
McAnally: All businesses have a legal obligation to use reasonable data security measures to protect sensitive individual information. There is no federal data security law, which means there is a patchwork set of different state laws on what is considered

reasonable data security.

Data breach class action lawsuits continue to increase — and negligence is the leading legal theory asserted in these lawsuits. If your business has suffered a data breach, legal discovery often uncovers some action a business could have taken to protect its sensitive data.

Other common lawsuit claims are violations of state consumer protection laws, breach of contract, and invasion of privacy. A cyber insurance survey found that the average cost for an insurance-covered legal defense was $434,354 and an insurance-covered legal settlement was $880,893.

Weddle: Many states are now requiring companies to quickly disclose data breaches. And in many cases, companies may have to provide ongoing credit monitoring and other services to individuals whose data was compromised. If it can easily be shown that your company didn't do its due diligence in protecting sensitive data, like PHI (Protected Health Information) or PII (Personally Identifiable Information), then there is always the potential for a lawsuit.

We know one of the biggest threats for businesses is their employees. How can companies better educate their workers to avoid cyber threats?

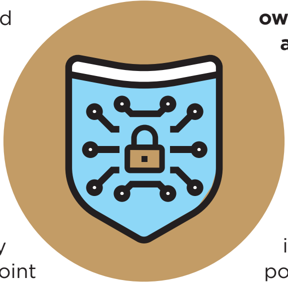
Weddle: Ongoing training for employees is crucial to ensuring that your business is protected. Quality training will include what to look for and how to respond.

Routinely testing users with phishing tests is an extremely effective way of not only educating users but also understanding which of your users are most likely to compromise your systems. In most cases, companies will see their "click rate" reduced from more than 20% down to sub 5% in the first few months of running these types of tests and education programs. This will also quickly identify habitual "clickers" and provide the opportunity to have direct conversations with them concerning this behavior and the threat it presents to the company.

McAnally: Knowledge is key. Regular and mandatory employee training of cyber risks is the best way to educate about cyber threats and should happen more than once a year. It's also important to document employee training and communicate frequently with employees about recent phishing scams you are experiencing.

What are some of best practices to help monitor for and identify breaches? What are the key components to include in a breach/incident response plan?

McAnally: Monitoring and logging access to your network is the best way to identify breaches. The key components of a data breach/incident response plan are to: (i) notify customers and employees who may be at risk; (ii) keep business operations up and running; (iii) report attacks to law enforcement; (iv) investigate and stop the attack; and (v) plan for inadvertent attacks (like weather emergencies) that may put your data at risk.



Weddle: There are a number of solutions that can help to continuously monitor for security events and help identify breaches. Many of today's endpoint security solutions are able to quickly detect and stop ransomware and malware infections before they progress very far. Other advanced systems can continually monitor traffic and utilize machine learning to identify anomalous activity outside your business's normal utilizations. Understanding the types of data your business maintains and its criticality will help you determine how extensive a system you require.

When building an incident response plan, you need to have clearly defined actions for end users when a data breach is detected. In the case of ransomware, this may include having the end user immediately turn off their machine, unplug it from the network and notify IT support. It should also include the recovery plan to restore lost files and systems.

What is the outlook like for cybersecurity moving forward?

Weddle: Cybersecurity is a constantly evolving game of cat and mouse between cybersecurity solutions and cyber criminals. With the rapid progression of machine learning, the ability for AI to "understand" normal traffic and usage patterns on networks and devices will begin to make it more difficult for malicious activity to go unnoticed and without response. Pairing that with increased end-user awareness of threats will be key to the future of cybersecurity.

McAnally: Businesses continue to face more cyberattacks than ever, and the cybersecurity risks will only increase. Ransomware-type attacks are on the rise, and most businesses have no choice but to pay the ransom to get access to their data to stay in business. Plan and prepare for cyberattacks now.

Is there anything that business owners/executives need to know about technology/cybersecurity that we haven't covered?

McAnally: It's important to note that most commercial general liability policies will not provide insurance coverage for cyberattacks. Cyber insurance policies are more important than ever to prepare for cyberattacks and are becoming more affordable. Talk with your insurance broker to inquire about cyber insurance coverage for your business.

Weddle: Business leaders need to realize that it is no longer a question of if but when. Preparedness is critical. Leaders also need to understand that a breach will not only impact them financially but it also impacts their credibility with clients. Having a robust plan in place and performing regular testing will help minimize loss.

BUTLER | SNOW

MELODY MCANALLY

Melody is Co-Team Leader of Butler Snow's Data Security and Privacy Team and regularly advises businesses on data security, data breach response, cyber-risk management and privacy issues. She has also written and presented on a variety of topics relating to data security and privacy.

PROTECH SERVICES GROUP
INNOVATION APPLIED

DAN WEDDLE

Dan is a University of Memphis graduate with more than 25 years in the information technology industry. He joined Pro-Tech in 2005 as President and took over the position of CEO in 2019. Dan has held management positions with major corporations across a wide variety of IT disciplines providing him a unique perspective for leading the largest technology company in Memphis.