COMCAST
BUSINESS

KEEPING DATA COVERED

CREATING A "BREACH-FREE" CLIMATE

COMCAST
BUSINESS

KEEPING DATA COVERED:

CREATING A "BREACH-FREE" CLIMATE

The best way to deal with cyber attacks: develop strategies to prevent them from claiming your data and reputation.

STEP 1 IS KEEPING CYBER ATTACKS AT BAY

The headlines are guaranteed to inspire fear and panic. Hackers accessed customer records, including personal data such as Social Security and credit card numbers. Or they infiltrated a system and held its data hostage until paid a ransom for the files. And then the victims of these cyber crimes suffer further losses—in reputation, in customer and vendor confidence, and perhaps even in their ability to remain in business.

Cybersecurity Ventures projects that "cyber crime" will cost the world $6 trillion annually by 2021. The company estimates that ransomware alone cost $5 billion globally

in 2017. What's driving this escalation in cyber threats? First, botnets and other technologies are making it easier than ever for hackers to launch mass attacks. And second, human error is making it possible for those attacks to succeed.

According to Mimecast, 91 percent of cyber attacks are launched via phishing emails. Which means your company is one unfortunate mouse click away from joining the ranks of the cyber compromised. Is your business strong enough to withstand key customers' loss of confidence? To rebound from a significant loss in revenue and reputation? Wouldn't it be more strategic to learn to avoid cyber attacks and protect and preserve the data and assets you've worked to build?

BREACH-PROOFING = EMPLOYEE-PROOFING

It sounds simplistic, but at the most basic level, cyber security depends on delivering one key message to your staff: "Don't touch that!"

And "that" encompasses a host of potential threats that look harmless. Looking harmless is part of hackers' strategy for infiltrating your system—whether they're targeting your business specifically or landing on your data randomly in the course of a mass attack. Outsmarting them starts with understanding how they think and then creating and enforcing policies that protect you from falling into their traps.

Do your employees use company-issued computers or devices to check their social media feeds during down times? All it takes is one click on a virus-infested link on Facebook, and suddenly cat videos aren't so adorable anymore. Online shopping can pose another risk. Even using apps to order lunch may expose your network to hackers.

If that doesn't concern you because you don't think your company has any data worth stealing, think again. Because small companies often take a more lax approach to cyber security systems and practices, they can be easy conduits for hackers whose ultimate target is a larger business—for example, your biggest client. In this scenario, your company is just being used to get to the real prize. But you'll suffer

collateral damage just the same.

Links in emails are the most common source of cyber trouble at businesses. Hackers have become adept at mimicking the look of emails your company receives every day from financial institutions, retailers, business partners, airlines,

your insurance company—and if they can get just one person on your staff to click on a link, you're in trouble.

"Socially engineered email hacks work on unsuspecting employees who haven't been trained to spot and react to them," says Steve Morgan, founder and editor-in-chief at Cybersecurity Ventures. His coverage of the Business Email Compromise scam details how the outfit "has been tricking finance and administrative employees into not only clicking on emails they shouldn't, but actually wire

THE HIT LIST: GUARD AGAINST THESE BREACH SOURCES

Technology makes it easy for hackers to launch a cyber attack. Don't make it easy for them to count your company among their victims. Which of these threats is most likely to exploit human error in your operations?

- ***Spear phishing*. The email looks legitimate. But it's not. Learn what your bank, vendors, suppliers, and other institutions do and don't communicate by email and what information they'll never ask you to provide via email. Keep an eye out for subtle differences in email addresses or URLs and telltale bad grammar in the email texts. And make sure your staff knows how to spot these fakes.**

- ***Lax password policies*. Strong passwords are at least 12 characters long and include a mix of lower- and upper-case letters, numbers, and special characters. Require everyone in your company to meet those standards.**

- ***Outdated operating and security systems*. The older your systems, the more susceptible they are to attacks. Check these Microsoft life cycle lists of products for which support ended in 2017 or will end in 2018, and make sure you install system and security updates promptly.**

- ***Failure to limit access*. Does one password grant all employees access to all your company's data? Creating layers of protection and separate passwords for sensitive areas of information can limit the damage in the event of a breach.**

- ***Homegrown viruses*. Even if your internal security is pristine, you can suffer a breach by importing infected documents created by employees on their home devices. Establish and enforce security policies that limit staff members to working on company-provided devices or that require employees to duplicate your security practices at home.**

- ***Personnel changes*. When employees leave the firm—and particularly when they've been terminated or have accepted an offer from a competitor—make sure they're no longer able to access your data. You may even want to update passwords and security procedures when employees move to new departments. (See Failure to limit access above.)**

transferring funds to cybercriminals—without realizing it."

Fake customer support representatives (CSRs) have persuaded employees to reveal their login credentials on the pretext of helping them reset their passwords. Scammers have even posed as IRS agents as a ruse for getting access to information. And in many of these cases, they don't even have to break into the system, because unwitting employees give them what they want.

PREVENTING–AND ACTING ON–BREACHES

Employee education, then, is a key to protecting your company's and customers' data.

"Every organization should train their employees on security awareness," Morgan says. "And every organization should have a simulated phishing program. This is the process of simulating phishing attacks on employees, regularly, to confirm that the employees are able to recognize the threats and respond to them properly."

He urges business owners to recognize that training is not a one-shot deal. "We're talking about behavioral training, and that is not something that changes after one class or watching one video." To optimize cyber safety, your business needs to reinforce those lessons and update them to integrate the latest scams.

ARE YOU PASSWORD-PROTECTION SAVVY?

Your anniversary. Your dog's name. The title of your favorite movie. What do they have in common? When used as passwords, they're as good as invitations to get hacked.

Of course, the more passwords you need, and the more complicated they are, the more likely you are to forget them. That's where password managers come in. They allow you to create passwords that are complex enough to foil hackers but give you access to a (password-protected, of course) list so you don't have to remember them.

PCMag.com's Best Password Managers of 2018 include:

- **Zoho Vault**
- **Dashlane**
- **Sticky Password Premium**
- **Keeper Password Manager & Digital Vault**
- **Password Boss Premium V2.0**
- **LastPass Premium**
- **LogMeOnce Password Management Suite Ultimate 5.2**
- **AgileBits 1Password 6**
- **RoboForm 8 Everywhere**
- **True Key by Intel Security**

The article also includes advice about creating passwords that protect data security.

Another essential is developing and maintaining good data storage and backup practices. Without them, the time and financial costs of data restoration are compounded and may pose secondary threats to your business by delaying your resumption of normal operations.

You also need what Morgan calls a cyber resiliency plan, because the last thing you want in the aftermath of a breach is to trust in your ability to improvise productively. As with the simulated phishing scenarios, he urges companies to run breach fire drills "to practice incident and breach response. The steps are going to be different for each organization depending on variables."

MAKE PROTECTION AN ORGANIZATIONAL PRIORITY

Cyber security isn't something business owners or management can handle on their own. Make sure your employees understand what is expected of them in the event of a breach. A climate of confidence is essential here, because without that, you risk employee hesitation about reporting breaches immediately. Make your entire staff aware of their role in dealing swiftly with actual or suspected breaches so the company is in the best position to minimize damage and initiate its response-and-recovery plan.

It can be helpful, too, to understand what corporate reputation management involves in the event of a breach. That knowledge can be integrated into your cyber security plans and give you a deeper understanding of how prevention can help avoid the need for a cure.

Start with your insurance coverage, says Mike Paul, president of Reputation Doctor LLC. "If this happened today, would you be covered? To be able to protect yourself, and to have an attorney who is backed by the insurance company who can go into court to protect you if you've had a breach and someone is suing you, is extremely important."

Next, do a risk assessment to determine how much you need to invest in cyber security—and understand that this investment isn't really optional. "You can't say today that you didn't know," he says. "That will come up in any lawsuit that is brought against

you. You do not have the right to say, 'I didn't know. I was naïve.' That's not how it works."

Neither will it be helpful in the event of a breach to throw one person under the bus, announce that the employee was fired, and say that it won't happen again. "That's not going to increase trust in your business, because what we want to hear is that the business is responsible," Paul says.

Any response will have to be tailored to the circumstances of the particular breach, but there are some commonalities, and they relate to trust and transparency. People's first question, Paul says, will be how big the breach is. They expect an honest answer, even if the answer is that the company doesn't have full details yet and is still investigating. In the aftermath of a breach, when people's trust has been compromised, they're worried, and you're in crisis mode, it's essential to communicate that you have (or are in the process of getting) a handle on the issue. Simply stating that a thorough investigation is underway and that you'll have more information soon can buy you a few hours to get things under control.

As the business owner, you'll be focused on the impact on your company, and it's valuable to have on the response team someone who can think beyond that insider perspective.

Another key message point is the distinction between data that was breached and data that is being used. "If it's true that 'to date, we have no information that any of the data has been used in a destructive way to individual customers,'" Paul says. "then you need to say it. The best way to help rebuild trust is to utilize the facts that are readily available and in your control as quickly and fully as possible."

He encourages companies to bring on board someone outside the organization who can adopt the mindset of stakeholders who have been (or fear they have been) damaged by the breach. As the business owner, you'll be focused on the impact on your company, and it's valuable to have on the response team someone who can think beyond that insider perspective.

DATA SECURITY RESOURCES

It's a challenge to keep track of constantly evolving cyber threats. These resources can help you protect your data and reputation.

Spear phishing. Bot nets. Ransomware. Cyber crime is so insidious that we've had to invent a new vocabulary to describe it. And you didn't get into business to spend half your waking hours learning these terms and monitoring hackers. But to protect your business, you do need to stay on top of these trends and know how to protect yourself from cyber threats. These online resources can give you the information you need to optimize your company's security systems, policies, and practices.

HARVARD BUSINESS REVIEW

- **The Biggest Cybersecurity Threats Are Inside Your Company reviews human errors that often expose companies to attacks and offers a plan for protecting your data assets.**
- **While "the root cause of most security breaches can be traced to human actions, or lack thereof," the author of Which of Your Employees Are Most Likely to Expose Your Company to a Cyberattack?" adds this note of caution: "the bigger mistake is to believe that cyber security can be attained simply by correcting bad behavior."**
- **"To prepare for and prevent the cyber attacks of the future, firms need to balance technological deterrents and tripwires with agile, human-centered defenses." With that in mind, the authors argue that The Best Cybersecurity Investment You Can Make Is Better Training.**

CYBERSECURITY VENTURES

The company's Cybersecurity Research page includes links to a variety of its reports, including:

- **Ransomware Damage Report**
- **Mobile Security Report**
- **Cyberinsurance Report**
- **Password Report**
- **Security Awareness Training Report**
- **Official 2017 Annual Cybercrime Report**
- **The Complexity Crisis in Cybersecurity: Simplify or Die!**
- **Cybersecurity 500 List**

The website also maintains a list of links to free IT security tools.

In addition, Cybersecurity Ventures' Steve Morgan contributes regularly to CSOonline.com, where he published his Great big list of cybersecurity resources. They include lists of data threats, cyber warfare definitions, and more than 400 cyber and information security-related definitions.

PCMAG.COM

In 10 Cybersecurity Steps Your Small Business Should Take Right Now, you'll hear from ADP, ESET, Microsoft, and NIST experts who review "everyday challenges, risks, and proactive cyber security measures businesses can take." The article is adapted from a National Business Week panel discussion.

How Businesses Are Applying AI to Cybersecurity explains how "automated incident response, behavioral analytics, and predictive machine learning can enhance your security."

Of course, the best way to manage a breach is to take steps to ensure that you don't have to deal with one. But by creating a plan for optimizing cyber security awareness within your company and for dealing with crises should they arise, you strengthen the foundation of trust on which your business relationships and operations depend.

COMING UP:
BUILDING AN IRON SAFETY NET: IMPLEMENTING A HOLISTIC SECURITY SOLUTION

Upgrading your network security creates an opportunity to review your company's systems to ensure not only that they are optimally protected against cyber crime and data breaches, but also that they operate in the most effective and productive manner. Implementation can be accomplished in tandem with upgrading enterprise-wide systems and therefore promoting better flow within and among departments in the organization.