WHEN IT COMES TO NEW TECH, OLD TECH IS YOUR BIGGEST RISK

Trending Topics summarizes news, information and perspective on matters affecting businesses and business leaders today. This insight is being provided to keep you up to date on the latest developments and trends influencing these topics. These views do not necessarily represent the views and opinions of PNC. For additional research on these topics, please consult the sources cited in this article.

Over the last decade, Americans have become used to the idea of cybersecurity breaches as billions of user records leak to malicious hackers in often highly publicized incidents. While some hacks succeed due to poor security practices, others could have been easily avoided with a few basic steps.

For example, the widely publicized Equifax breach leaked sensitive information of more than 145 million Americans, and it could have been avoided with a recommended software update.[1] Avoiding expensive and embarrassing security incidents is often easier than executives realize. Follow along to learn about the most common sources of cyberattacks and what your business can do to keep attackers at bay.

MOST ATTACKS START WITH AN EMAIL

90% of cybersecurity breaches start with a link in a bad email, according to a study from cybersecurity company PhishMe (since renamed Cofense).[2] With an estimated 235.6 billion emails sent per day, and 121 per office worker per day, it's no shock that an occasional malicious message gets through even the most stringent spam filters.[2,3]

In addition to malware, emails are a major source of other types of fraud. The 2018 AFP Payments Fraud and Control Survey found that 78% of companies were a target of payments fraud.[4] Putting strong accounts payable systems in place is another opportunity to improve cybersecurity.

Employees are a key resource for any business, and they can act as an additional line of defense against digital intruders trying to get your company's valuable data.

AGING SOFTWARE REQUIRES UPDATES

On your home computer and smartphone, you likely see regular notices for software updates that fix bugs and security issues. Dismissing a similar notice led to the Equifax breach that leaked names, addresses, Social Security numbers and other sensitive data from 145 million Americans.

While there are often other benefits of updates, the most important is digital security. As security software provider Norton explains on its website, suggested updates include a "multitude of revisions to your computer, such as adding new features, removing outdated features, updating drivers, delivering bug fixes, and most importantly, fixing security holes that have been discovered."[5]

In the case of Equifax, a vendor provided an update to its software that would have prevented the breach two months before it happened. Updating a complex database, web and other corporate systems takes more work than the single click and restart of a PC or smartphone update, but recent history teaches that these updates are too important to ignore.

In some cases, your business may be running software so old that the vendor no longer supports it. This is a common story with Windows XP, where many large companies relied on the aging operating system that saw support end in 2014. Even with years of notice, plenty of companies scrambled to upgrade and avoid security issues. And according to a 2017 survey, more than half of companies still work with Windows XP despite this risk.[6]

You don't have to be an early adopter, but it's best to upgrade from legacy software to newer systems that offer better security. When you upgrade, you'll probably also notice feature and performance improvements, offering a win-win scenario when you upgrade.

PNC

When your business puts the right focus on training, security updates and forward-looking upgrades, you can feel more confident that your company is better prepared to stand up to even the worst cyberthreats.

STAY ON THE CUTTING EDGE OF DIGITAL SECURITY

Cloud-based software offers a unique security feature that hosted software solutions do not: security and updates are handled for you. Online applications from SaaS (software as a solution) providers generally do not require clients to get involved with security details. However, they also require handing over control of your data to a third party, a risk many companies are not willing to take.

If your business hosts its own platforms, the burden of security updates and patches falls on your information technology security team. Past breaches show the importance of keeping your systems updated and investing in the latest innovations in cybersecurity.

In addition to working exclusively with trusted, security-minded vendors, it is also important to add the latest security suites to your business computing systems. From employee laptops and desktops to data centers and servers, you will get the best results if you invest in the latest and most powerful security applications. Drawing on machine learning and artificial intelligence, your business can add solutions that work to analyze threats and keep you one step ahead.

AVOID THE HEADLINES WITH ROCK SOLID SECURITY

No matter the industry, your customers and employees expect you to keep their information safe, and your business has an obligation to do so. Nonetheless, companies like Target, Home Depot, Yahoo, LinkedIn, and many others have landed in the headlines, damaging reputations and harming consumer trust.

When your business puts the right focus on training, security updates and forward-looking upgrades, you can feel more confident that your company is better prepared to stand up to even the worst cyberthreats.

The Cyber Security Resource Guide from PNC offers simple opportunities to educate employees about the risks of email fraud, including training and a fake email campaign to test employee alertness and awareness regarding incoming threats.

To discuss these topics in more detail, please contact your PNC Relationship Manager or visit pnc.com/ideas.

1 "Failure to Patch Two-Month-Old Bug Led to Massive Equifax Breach" by Dan Goodin, Ars Technica, September, 13, 2017. Available at: arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

2 "Enterprise Phishing Susceptibility and Resiliency Report" by Confense. Available at: cofense.com/enterprise-phishing-susceptibility-report/

3 "Email Statistics Report, 2014-2018" by The Radicati Group, Inc. Available at: radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf

4 "Cyber-Security Resource Guide" by PNC. Available at: pnc.com/content/dam/pnc-ideas/articles/Cyber-Security-Collateral.pdf

5 "5 Reasons Why General Software Updates and Patches are Important" by Steve Symanovich, Symantec Corporation. Available at: us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html

6 "Windows 10 Adoption Surges, Yes Businesses Still Hang on to Windows XP and Vista" by Peter Tsai, Spiceworks, April 3, 2017. Available at: community.spiceworks.com/networking/articles/2628-windows-10-adoptionsurges-yet-businesses-still-hang-on-to-windows-xp-and-vista

CIB ENT PDF 0119-0135-1089402

PNC