TRENDING TOPICS

PREPARING YOUR COMPANY FOR CYBERSECURITY AND FRAUD PREVENTION

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.

Cyberbreaches can cause liability for businesses of all types if customer data is compromised. It's becoming increasingly important for companies to incorporate training and take precautions beyond just their IT department. Chief financial officers (CFOs) can and should take a lead role in ensuring their organization is prepared to combat cyber data theft and fraud.

This issue affects companies of all sizes and virtually all industries, from retailers to manufacturers. Professional services organizations like medical practices, law firms, consultants and a host of others face this issue as well.

Employee training and establishing a corporate culture of security can help reduce your organization's risk.

THE MAGNITUDE OF THE PROBLEM

According to the 2018 AFP Payments Fraud and Control Survey — Report of Survey Results for the year ended in 2017:[1]

- 78% of companies were the target of some sort of payment fraud.
- 74% of organizations surveyed were victims of check fraud.
- 77% of the organizations surveyed experienced some level of business email compromise.
- 54% of the business email issues targeted wires, 34% targeted checks.
- Nearly one-half of the respondents reported that incidents of attempted fraud increased in 2017 over those in 2016.

As you can see, this is a significant problem.

EMPHASIZE THE NEED TO PROTECT COMPANY DATA

Your company's biggest weapons against cyberfraud and related breaches are your employees. New hires must be educated as to best practices in cybersecurity from their date of hire throughout their initial training, and this emphasis must be updated via ongoing training and education.

In retailing, for example, there are countless electronic transactions both in a physical store environment and on your company's website. Employees in both areas of the business should be educated on the proper processes and procedures to protect customer data at all times.[2]

Manufacturer's data will increasingly be vulnerable to breaches and hacking due to the use of new technologies like the "internet of things" (IoT), robotics applications, blockchain and a host of other emerging technologies. Smaller manufacturers are especially at risk due to a lack of in-house expertise in many cases. Manufacturers need to take steps to protect this data, and a great starting point is emphasizing the importance of this to all employees.[3]

Some best practices for all types of companies in this area include:

Password protections and protocols

Emphasize the need for employees to select strong passwords. Using key life milestones like birthdays or your anniversary are easy for a hacker to figure out — likewise with favorite sports teams, etc. Establish protocols for changing passwords on a regular basis. Discourage employees from sharing their passwords as well.[1]

Decide what is important to protect
For a retailer, there is both physical inventory and intangible assets. The employees using and in charge of these areas must be properly trained in cybersecurity protocols. This reduces the likelihood of data or inventory theft via unauthorized access to systems triggering false transactions and shipments to bogus buyers.[2]

Unauthorized software on company systems
Regardless of your industry, employees putting unauthorized, personal software programs on your company systems can lead to major data breaches and cyberthreats. Many of these programs may not have the level of security with their online interfaces that the programs used for your business might.

Establish a strict policy prohibiting this practice to help reduce cyberthreats against your proprietary company and sensitive customer data.

Email protocols
Emails with suspicious links aren't just a problem at home, they are a major problem in the workplace. It takes one employee opening a suspicious email and clicking on the link in that message to infect your company's entire system across all functional areas.

Manufacturers routinely receive specifications from other partners along their supply chain. It's important to ensure that all employees are trained to recognize who is a legitimate customer and who is not. When in doubt, there should be a process to contact someone in IT or another appropriate group within your organization.

Some red flags to look for in emails include:[1]

- Inspect the email header and look for altered words and letters that don't look right.
- Know that "from" names can be altered to mask a bogus email account.
- Train employees to be suspicious of any message that requests secrecy or is labeled urgent.
- Be wary of email senders who indicate they can only be reached via email.
- Be suspicious of emails indicating that payments should be sent to account numbers or a new mailing address.

Instruct employees on how to verify whether these are legitimate emails and where to seek help in doing so within the organization.

SOCIAL MEDIA USAGE

Most employees use social media in their personal lives, and in addition, many companies have a robust social media presence whether on Twitter, Facebook or elsewhere.

Like anything else online, there are risks ranging from clicking on bogus and dangerous links to inadvertently sharing sensitive information.

Your company should have rules about the do's and don'ts of social media usage on company systems, including ongoing updates and training for your employees.

Regardless of the business your company is in, data and computer systems are an integral part of your daily operations, ranging from the most basic to the most complex areas of your business. Installing protocols and training your employees is essential to minimizing threats from a data breach.

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

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

2 "5 Cybersecurity Questions Retailers Must Ask to Protect their Businesses" by Jovi Umawing, Malwarebytes Labs, April 17, 2018. Available at: blog.malwarebytes.com/101/2018/04/5-cybersecurity-questions-retailers-must-ask-protect-businesses/

3 "Many Manufacturers Still Falling Short in Cybersecurity" by Craig Guillot, Chief Executive, June 2, 2018. Available at: chiefexecutive.net/many-manufacturers-still-falling-short-in-cybersecurity/

Other sources
"Facebook's Security Breach Shows Even Significant Security Investment Might Not Help" by Kate Fazzini, CNBC, September 28, 2018. Available at: cnbc.com/2018/09/28/facebooks-security-breach-shows-even-significant-security-investment-might-not-help.html

"Perspectives: The Next Big Cybersecurity Threats Facing Businesses" by Don Steinberg, Forbes, April 3, 2018. Available at: forbes.com/sites/kpmg/2018/04/03/perspectives-the-next-big-cybersecurity-threats-facing-businesses/#318ec7f741ba

"Cyber Security Training for Employees" by Travelers Insurance. Available at: travelers.com/resources/cyber-security/cyber-security-training-for-employees

CIB ENT PDF 0119-0135-1089402