MELAND | BUDWICK

11 Cybersecurity Experts Share Tips for Preventing and Minimizing Data Breaches

https://mbdev.aplussdv.com/2019/08/09/11-cybersecurity-experts-share-tips-for-preventing-and-minimizing-data-breaches/

Julie Bawden-Davis

As a business owner, you no doubt have a list of major concerns for your company. Hopefully cybersecurity is at the top. The increasing incidence of data breaches and the resulting costs make cybersecurity a pressing concern for just about any business.

“The monetization of cybercrime has created an epidemic of data attacks,” says Chris Hoose, president of Choose Networks, an IT consulting firm for small businesses. “We hear about the large data breaches like MyFitnessPal, Facebook, Marriott and Equifax, but the most impactful ones are happening to small and medium-sized businesses every day.”

According to Hoose, it’s difficult for small to mid-sized businesses to survive a data breach.

“The cost of remediation, the hit to a company’s reputation and the fines levied through regulation often make closing the doors the only option,” he says.

A 2018 study performed for IBM Security by Ponemon Institute found that the average total cost of a data breach is $3.86 million. The Cost of a Data Breach Study: Global Overview involved interviews with more than 2,200 IT, data protection and compliance professionals from 477 companies that had experienced a data breach over the prior 12 months.

The study, conducted during 2017, found that “data breaches continue to be costlier and result in more consumer records being lost or stolen, year after year.”

Not every data breach is that costly—but any loss is a negative for your company.

“The financial consequences of a data leak depend on multiple variables, including the time taken to detect the leak, the qualifications of your incident response team and the type and amount of information stolen,” says Dennis Turpitka, founder and CEO of Apriorit, a software development company that provides engineering services to technology companies.

Data Breaches Can Happen to Any Company

“Even with the number of breaches growing at an alarming rate, many small-business owners think no one is interested in their data and it won’t happen to them. Cybercriminals are taking advantage of that mindset,” says Hoose.

“Significant cyberattacks may make headlines, but anyone in business is in the crosshairs of hackers and cybercriminals. Attacks on smaller businesses happen much more frequently and sometimes with more devastating effects,” says Chris Essex, senior vice-president of Global Sales for AppRiver, which offers cloud-based cybersecurity solutions.

“Any type of organization can be the victim of a cyberattack,” adds Daniel Eliot, director of education and strategic initiatives at the National Cyber Security Alliance, which drives awareness of cybersecurity issues. “Data breaches occur in municipal governments, high schools, colleges and all types of businesses.”

Technology Contributing to Cybersecurity Attacks

New technology is moving at dizzying speed, notes cybersecurity expert J. Eduardo Campos, president and managing partner of business consulting firm Embedded-Knowledge.

“We are in the midst of the Fourth Industrial Revolution (4IR), enabled by a wave of cutting-edge technologies, such as 5G,” says Campos. “This next generation of wireless technologies will enable sensors and mobile devices to operate even faster. This has led to living in a world where data breaches are increasing daily.”

Companies operating on outdated software or software that is no longer supported are leaving the door to the vault wide open with an invitation to enter.

—Daniel Eliot, director of education and strategic initiatives, National Cyber Security

Alliance

Businesses and governments are facing unprecedented cybersecurity challenges to keep their data protected, believes Uzi Scheffer, CEO of SOSA, a global innovation platform that connects corporations, governments and cities to technologies. “Thanks to the rise of cloud computing and IoT (devices connected to the internet), we’re now connected on extraordinary levels.”

It’s estimated that there will be more than 41 billion devices connected to the internet by 2025. “This means an immense amount of data that requires protection,” says Scheffer.

“All of this means that as marketing and systems automation make conducting business more convenient for consumers and businesses, it makes life easier for hackers,” adds Colin Bastable, CEO, Lucy Security, which offers cybersecurity services.

Understand Your Cybersecurity Risks and Obligations

Just because your information is stored in the cloud, doesn’t mean it’s not at risk.

“The cloud means ‘someone else’s computer,’ ” says Bastable. “If you’re not in control of the data, you have risk. If you have sensitive data, you are a point of attack.”

The attacks themselves have become much more sophisticated and far- reaching, notes Deepak Patel, vice president of product marketing at PerimeterX, a cybersecurity company.

“It is important for companies to understand that ATO attacks can use data from more than one data breach, which makes their attempts more successful,” Patel says.

In addition to protecting your company’s reputation and livelihood, it’s your duty to protect client and customer data, believes Van Nguyen, CTO of Convincely, a platform that optimizes website use.

“Every company is obligated to protect the data that customers entrusted them to keep safe,” he says.

Cybersecurity Measures to Help Prevent Data Breaches

While no business is ever completely safe from data breaches, there are steps you can take to help make your company less of a target.

1. **Insist on cybersecurity protocol.**

Ensure that employees change passwords regularly. Use two-factor or multi- factor authentication, and forbid employees from connecting foreign hardware—either cloud or hardwired—to a network connected system.

“Once you educate employees about best practices, it’s important that you require compliance at all times,” says Jerry Haffey, CEO of Ambrosia

Treatment Centers, a drug and alcohol treatment facility. “My company is responsible for safeguarding patient medical history and payment information. Adhering to cybersecurity protocol is enforced.”

2. **Consider the human link.**

“Most hacking losses stem from social engineering attacks that target employees,” says Bastable. “Train your staff to spot phishing attacks and to never click on questionable links.”

IT solutions don’t address human risk, agrees trade secrets and IP attorney Eric Ostroff, a partner at Meland Budwick, P.A. “Employees can be the target of social-engineering-based attacks, such as spear phishing. Create a culture of protection at your company that keeps data and IP security at the forefront of employees’ minds.”

Given that many cybersecurity breaches occur via emails, Eliot suggests not giving employee access to email until they’re trained to spot potential breaches and avoid them.

“Cybersecurity training should also continue throughout their careers,” he says.

3. **Seek the services of a skilled security professional**.

“Whether the person is in-house or a managed service provider, it’s essential that you get expert help,” says Essex. “A cybersecurity expert will ensure that all sensitive

data is in an encrypted format before emailing. An expert will also routinely perform risk assessment of your networks pre- and post-third-party integration and continually monitor for threats via email and web traffic."

A cybersecurity expert will also help you plan for the long-term, says Scheffer.

"Where most companies fail is in implementing a sustainable, long-term cybersecurity strategy that will evolve and modernize as technologies, approaches and practices advance," he says.

"By partnering with experienced cybersecurity service providers to analyze your business's 'cyber posture' on a periodic basis, you'll be able to continually monitor for threats, alert the appropriate teams of suspicious activities and respond in real-time to such events," says Scheffer.

4. **Look into cyber liability coverage.**

Cyber liability coverage will help with the monetary damages caused by a breach should one occur, which could help you keep your company doors open.

5. **Update software regularly.**

"Companies operating on outdated software or software that is no longer supported are leaving the door to the vault wide open with an invitation to enter," says Eliot. "It's a good idea to invest in updating your IT infrastructure, centralize system updates when appropriate, and teach employees to update their devices if they individually manage them."

6. **Understand the IoT Security Black Hole.**

"Perhaps the biggest security gap is located in the latest online frontier of mobile devices," says Scheffer.

"Devices are quickly becoming smarter. Many use relatively new combinations of communications protocols, coding language and IT infrastructures," Scheffer continues. "As a result, many cybersecurity companies have yet to identify all the loopholes created by these combinations. To make matters worse, IoT manufacturers are loosely monitored regarding even basic encryption for these

devices."

7. **Have a plan in place.**

"Ensure that you have a cybersecurity and data breach plan that identifies what sensitive assets you need to protect, how you plan to protect those assets, what measures you are taking to detect cyber incidents or breaches and what your plan is for responding and recovering from cyber incidents or breaches," advises Eliot.