Investing in cybersecurity prevention - July 2018

applya® Corporation

According to the Identity Theft Resource Center, as of July 2017, over 700 companies were breached, nearly matching the total of all breaches in 2016. A data breach occurs when an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is put at risk.

IBM's Data Breach Study reports that on average, the cost per record stolen in the United States is $221, and that the average time to just identify a malicious attack is 229 days. How will that affect your company? If you run a business that processes only 10 unique records per day and your company is breached, and it takes you the 229 days to detect the attack, your total exposure is over $500,000. The potential damage can be catastrophic for you.

"Cyber threats pose one of the gravest national security dangers the United States faces," stated former United States President Barack Obama. "When our nation's intellectual property is stolen, it harms our economy, and when a victim experiences online theft, fraud, or abuse, it puts all of us at risk."

As illustrated in this interactive graphic of the world's biggest data breaches in the last ten years, the size and severity of attacks has steadily increased. Yet spending on security training for application developers has failed to grow accordingly.

Cybersecurity is a one-way war; hackers attack relentlessly while businesses can only attempt to defend their assets. Thus, the only way to reduce risk is to make hackers jump through as many hoops as possible before reaching the valuable information. This is what is known as reducing the hacker's ROI, so that the hacker moves on to a more lucrative target than you.

Now is more critical than ever to view your cybersecurity investment similar to how you would justify insurance. The premiums paid – cybersecurity investments – reduce the expenses to a fraction of what they would be without coverage.

How can you prevent an attack when you don't know what you are looking for?

Hackers prey on human error by stimulating strong emotions to create gaps in security. Per the same IBM report, human error comprised 23 percent of all data breaches. To establish a baseline for cybersecurity awareness, the Department of Homeland Security offers free posters and other promotional material that should be placed around the office. We also recommend quality and regular cybersecurity awareness training for your employees.

Rather than outsource IT security to external firms and their experts, everyone in a company's IT team must be up-trained in security practices to build cyber resiliency across the organization. There simply is no substitute for internal training, planning and being prepared for a cyber threat.

Cybersecurity and elearning

A meaningful security culture requires consistent reinforcement of cybersecurity awareness and best practices. Hackers use cutting-edge technology and their methods are volatile. If employees are only trained once a year at your company, they may be unaware of new threats and may not be up to speed on new defense practices. Employees should be regularly trained on the basics of security, especially Password Security and Email Security.

Check out courses available from Enterprise Risk Management through OpenSesame on cybersecurity topics to maximize the protection of your business today. OpenSesame's elearning course catalog help managers and developers understand cybersecurity threats and create an opportunity to begin a dialogue within your company on the importance of secure data.

- Syntrio is a leading elearning course publisher with the objective to provide clients with a cost-effective, turn-key online learning solution comprised of their proprietary courseware and hosted learning management systems. Start with their "Cyber Security Basics" course, particularly for those not in IT positions.
- Cyber Attacks and Security Breaches Today from WatchIT: This 6 course track was designed specifically to provide a starting point for executives, technologists, sales and consultants to begin to develop the tools necessary to combat cybersecurity threats.

Remember, you don't have to be a Fortune 500 company to fall prey to hackers. They pick on individual consumers all the way up to corporate giants. It's only a matter of time before the cyber pirates turn their eyes upon your industry with greedy intent.

OpenSesame helps companies like yours develop the world's most productive and admired workforces with the most comprehensive catalog of elearning courses from the world's top publishers.