Are You Protected Against Cyber Theft?

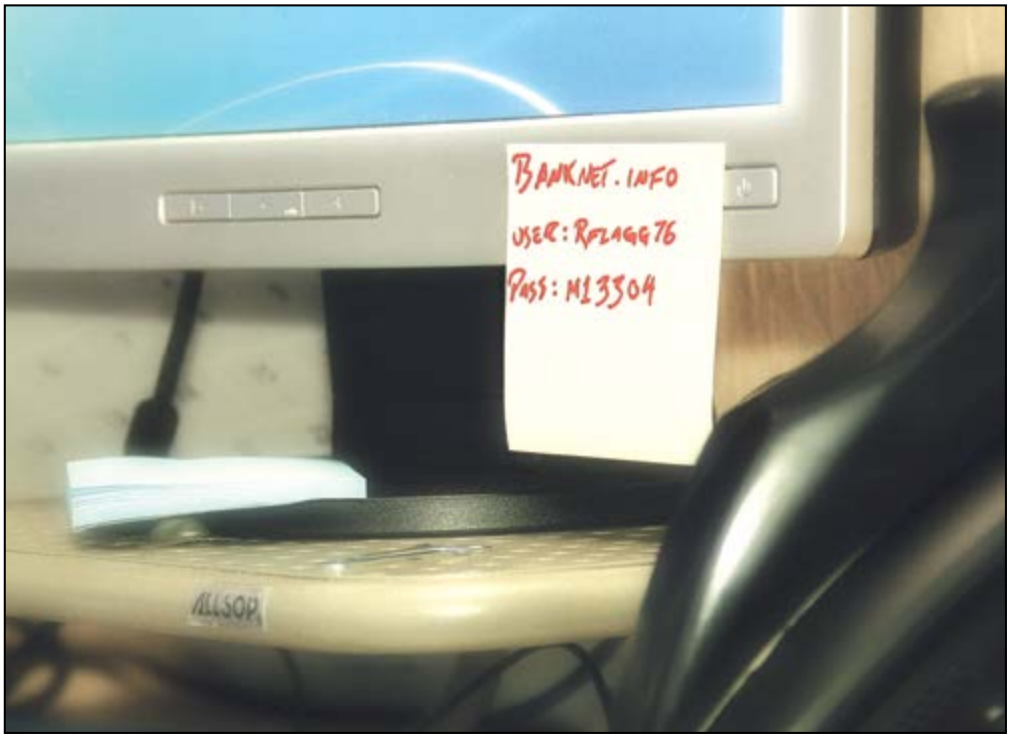
If the Answer Is 'No,' the Consequences Could Be Costly

By MICHAEL LEVIN

When it comes to cyber security and data breaches, no system is infallible. Some of the largest companies in the world have been victims of data breaches. Recently, the Swansea, Mass. Police Department contracted the CrytoLocker computer virus, and paid ransom to gain access to their files.

While large breaches like those at Target, Neiman Marcus, and Yahoo! receive great media attention, smaller breaches occur daily without much fanfare. A common misconception is that malicious hackers target only large companies. However, small and mid-sized companies are often perceived — for good reasons — as easier targets due to their limited IT resources.

What is the incentive for criminals to steal data? There is a large black market for stolen identities. Some estimates put the value of stolen personal identifiable information (PII) and personal health information (PHI) at $5-$10 per record, depending on the information. Malicious hackers who gain access to computer systems have the potential to modify accounts-payable data and change bank routing numbers.



Human Error

Another common misconception is that most breaches result from a hacker sitting behind a computer in some foreign country. Malicious hacker activity has and will continue to occur; however, some studies estimate that approximately 50% to 60% of breaches result from simple human and system errors.

For example, unencrypted laptops and smartphones that are lost or stolen pose a large threat, as do data backups brought home by an employee for off-site storage. Lost or weak passwords continue to be an issue as well. It's fairly common to see a sticky note on an employee's computer monitor with their username and password to access the enterprise software system (hopefully not the controller).

In addition, people often mistakenly send e-mails to someone other than the intended recipient. How many times have you replied to an e-mail that started with, "I think you meant to send this to another person?" If the e-mail contains PII or PHI, this may be a breach.

Not understanding the technology in your office can also result in a breach. Affinity Health Plan Inc. settled with the U.S. Department of Health and Human Services (HHS) for $1.2 million when it returned leased photocopiers with 344,579 personal health-information records on the copier's hard drives (yes, modern copiers have hard drives that store data).

Human error breaches are not limited to digital data. Improper disposal of documents that contained PII or PHI has led to breaches. The list of exposures on the human-error side alone is limited only by one's imagination.

While large breaches like those at Target, Neiman Marcus, and Yahoo! receive great media attention, smaller breaches occur daily without much fanfare.

Cyber Risk Management

Implementing preventative measures, best practices, and a strong backup solution help reduce, but not eliminate, the risk. An incidence-response plan that details responsibilities and vendors is crucial to quickly address a breach and to avoid panic buying. Many state laws have time deadlines for certain actions. The clock is ticking once a breach has been identified. A written policy and plan detailing security measures will be of assistance should you be interviewed by the Office of Civil Rights, HHS, or the state attorney general.

Potential Cost of a Cyber Incident

Expenses from a data breach or a cyber incident vary and can be quite high. Beyond

the intangible cost associated with the loss of consumer confidence, organizations may face lawsuits, regulatory expenses, regulatory-defense costs, notification costs, and business-interruption losses.

In order to limit the damage, organizations often hire public-relations firms, outsource call centers, provide credit monitoring for at least a year (required by law in some states), and provide identity-fraud insurance.

Forensic specialists may be required to identify and remediate the source of a breach that results from an organization's computer systems. Again, the clock is ticking. Not finding and resolving all the issues with a system creates further exposure down the road.

As discussed earlier, part of a comprehensive cyber risk-management program is to have a good backup solution and to monitor it regularly to ensure that data is consistently backed up. Without a solid backup strategy, organizations may incur data-restoration and computer-program-restoration expenses — assuming the data and programs can be restored.

Cyber-liability Insurance

It is important to understand that a general-liability insurance policy typically does not respond to cyber exposures. Available cyber-liability insurance coverages include network and information-security liability, security-breach remediation and notification, hacker damage, crisis-management expenses, business interruption, cyber extortion, media, data restoration, and computer fraud.

Today's cyber-insurance policies are flexible so that you can choose coverages based on your unique needs, exposures, and risk tolerance.

Today's cyber-insurance policies are flexible so that you can choose coverages based on your unique needs, exposures, and risk tolerance. Developing a meaningful cyber-insurance program requires an understanding of an organization's IT systems, data-security best practices, and level of employee education.

In Summary

Whether or not they realize it, most organizations, no matter the size, have some sort of cyber-security or data-breach exposure. If you store personal identifiable information or personal health information, your risks increase exponentially. And these risks are here to stay.

There are far too many cyber-security exposures to be covered in a single article. It is important to work with an insurance agent who is capable of understanding your exposures and who can match insurance coverages and carriers to meet your unique needs. A properly structured cyber-liability insurance policy can be an important element to an organization's overall cyber-risk-management program and long-term sustainability. ■

Michael Levin is an account executive at the Dowd Insurance Agency, a full-service agency providing personal, commercial, and financial-planning needs, with six offices in Western Mass.; (413) 538-7444; mlevin@dowd.com