LIMBA
LONG ISLAND METRO BUSINESS ACTION
NEWSLETTER

Cybersecurity in the 21st Century: Defense is the Best Offense

BY: Robert W. Doyle, Jr.,
Partner, Lewis Johs Avallone Aviles, LLP
(Associate Robert J. Yenchman assisted in the preparation of this article)

Pick up a newspaper, turn on the nightly news, or just browse the internet and chances are good that you will learn about another "massive data breach" affecting the lives of many. The common misconception that "I won't be hacked" or "it'll be obvious if I am hacked" are simply wrong. Cyber data breaches only take minutes to occur and often go undetected by the victimized individual or company for days, weeks and even months. According to data breach investigation report prepared by Verizon, 58% of malware attack victims are categorized as small businesses, which are costing them a lot of hard-earned cash. Statistics indicate that in 2017, average malware-related costs for small and medium-sized businesses included $1,027,053 due to damage or theft of IT assets, and $1,207,965 due to disruption to normal business operations. It is imperative to become aware of the potential dangers that arise when the issues of cybersecurity are not properly addressed.

Cyberattacks and data breaches take many forms. It may be as simple as an unsuspecting employee opening an email which initiates a series of events that allows for the extraction of company information. That kind of attack is most commonly achieved through the introduction of malware, which is a broad term used to describe software that is used to inflict harm on a system. Within the genre of malware is ransomware, which attackers use to lock up a target computer and then demand a fee in exchange for the captured data's release. Another form of attack is known as a "phishing" scam, which is aimed at manipulating an unsuspecting individual to divulge sensitive or personal information. That information is then used either to gain access to even more information or as the predicate to identity theft.

Defense is the best offense. Becoming aware of your cyber-vulnerabilities is critically important. An assessment begins by asking the following questions:

- What kind of information do we possess?
- Do we possess information that has appeal to others?
- Where is that information stored?
- Who can access that information?
- Are we protecting personal, employee, proprietary and/or client information from those seeking to use it against us?
- How are we protecting that information?
- Do we classify data based on its sensitivity?
- Do we have a plan in place to respond in the event of a cyberattack?

The answers to the assessment will assist in developing a security strategy that is specific to your company's needs. The strategy, however, will require some essential items. The first essential item is employee training, which should highlight the dangers a successful attack may pose. This "shock and awe" approach in educating employees will make it easier to enforce any security regulations you put it place. It will also make employees more vigilant and facilitate proper habits when they work on your company's data systems. The second essential item is protecting your company's network and devices by implementing passwords that need to be routinely changed. Protection also can be achieved through anti-virus software and various firewalls aimed at preventing unauthorized users access to your private network. When using such methods, it is important to keep the software regularly updated, as hackers have become adept at exploiting software that is not kept current. A thirdessential item as part of any security strategy should be data backup. The backup should be performed on a periodic basis and will allow for the retrieval of information should a data breach occur.

In today's fast-paced environment, it is critical to be one step ahead of those who wish to expose our potential weaknesses. The Federal Trade Commission offers a website, www.ftc.gov/datasecurity, which is an excellent resource that allows one to educate themselves about cybersecurity and the real-life dangers that a lapse will pose. Likewise, the Department of Homeland Security offers a well named website, www.dhs.gov/how-do-i/protect-myself-cyber-attacks, which is another great educational resource.

Navigating the world of cybersecurity can be complex, which is why Lewis Johs Avallone Aviles, LLP created a Cybersecurity Crisis and Risk Management Team. The team, comprised of experienced attorneys and experts, works to protect companies both before and after a data breach by developing cost-effective strategies to address privacy, data security and information management issues. We help clients develop and implement security programs, as well as incident analysis and response programs that reduce the strategic and financial risk of data loss.

Robert W. Doyle, Jr. is a partner at Lewis Johs Avallone Aviles, LLP and a former president of the Nassau Suffolk Trial Lawyers Association.
Robert J. Yenchman, an associate at the firm, assisted in the preparation of this article.