2017 BURR Alert

The Top Eight Things You Should Be Doing to Protect Your Business from Cyber Threats

By David D. Dowd III and Elizabeth B. Shirley July 2017

Cyber threats take many forms. The wide-spread WannaCry ransomware attack in May of 2017 highlighted how computer files could be held hostage in return for payment, while the Dyn denial of service in October of 2016 highlighted how websites like Airbnb and Twitter could be made inaccessible. This article sets out what your business can do to prevent a cyber attack.

1) Identify the types of cyber attacks to which your business is most likely vulnerable. By doing so, you can invest in measures that will be most relevant to your business. For instance, businesses that host websites must preempt denial of service attacks, while those that hold private customer information must prevent unauthorized access to their data. Of course, many businesses will likely be vulnerable to a variety of cyber attacks.

2) Develop a framework to prevent, investigate and respond to the cyber attacks to which your business is most vulnerable. In 2014, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) issued, and continues to update, a voluntary Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). In addition to their own independent initiatives, businesses should periodically consult the Framework to keep abreast of cybersecurity best practices in order to assess their security status relative to others.

3) Invest in the latest computer security and protection measures. Businesses should strive to use the most up-to-date software and avail themselves of periodic releases of software updates. Cyber attack methods constantly evolve, and older versions of software are more vulnerable to newer and more complex threats. For example, victims of the WannaCry ransomware attack were mainly those organizations that ran older versions of Windows operating software. Businesses should also consider regularly backing up data and insulating that data from their computer network, segmenting their computer network, and monitoring network activity.

4) Implement employee vigilance and training measures. Perpetrators of cyber attacks often employ phishing scams by sending emails with attached malware to individuals who then promptly download the attachments and infect their employers' computer networks. Businesses should train employees to identify suspicious emails in order to guard against phishing schemes. Given that malicious emails are often sent by seemingly familiar senders, businesses should teach employees how to spot subtle clues that indicate dangerous emails. For instance, employers should instruct employees to check whether the domain name of the originating account is a "near-miss" from what would be expected. For example, an employee recognizing "dot com" and "dot co" could be the difference in avoiding hefty losses.

5) Test your cyber security measures and monitor their effectiveness. To test whether employees take instructed precautions against phishing attacks, businesses should send their employees emails from a "near-miss" domain and tally how many employees fall for them. Of course,

even after enhancing computer security systems and increasing employee awareness of network defenses, businesses may nonetheless succumb to a cyber attack, but at least the chances of doing so may be reduced.

6) Obtain effective cyber attack insurance coverage. Businesses should compare their potential damages in the event of a cyber attack to the coverage provided in their existing insurance policies and seek out supplementary insurance for any uncovered damages or liabilities that may arise in the event of a cyber attack. For instance, since courts are divided as to whether computer systems constitute "tangible property" for purposes of an insurance claim, businesses should consider consulting their insurance companies, brokers, or legal counsel to obtain insurance that covers the types of damages that arise in cyber attacks.

7) Adopt an effective legal strategy for your business that preempts and limits liability. As many businesses hold confidential information, any data breach or unauthorized disclosure could make such businesses liable to a host of federal and state law claims, as well as possible class-action suits. Thus, the establishment of an effective legal strategy in place that preempts and limits liability is essential.

8) Employ traditional security measures for your business at locations that could be vulnerable to physical disruption of your cyber capabilities. Businesses should account for some of the more traditional ways in which perpetrators can disrupt their computer networks. To prevent someone from unplugging the power source to a computer network or server, you could consider employing security guards at such locations and installing CCTV cameras.

To discuss this further, please contact:

David D. Dowd III in Birmingham at ddowd@burr.com or 205-458-5293
Elizabeth B. Shirley in Birmingham at bshirley@burr.com or 205-458-5186
or the Chair of our Cybersecurity group, India E. Vincent in Birmingham at ivincent@burr.com or 205-458-5284