BURR FORMAN LLP

# Burr Alert: The Top Eight Things You Should Be Doing to Protect Your Business from Cyber Threats

Articles / Publications
07.24.2017

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


RELATED PROFESSIONALS

David D. Dowd, III, CIPP/US

Elizabeth B. Shirley, CIPP/US, CIPM

India E. Vincent, CIPP/US, CIPM

# Burr Alert: The Top Eight Things You Should Be Doing to Protect Your Business from Cyber Threats

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.

Download the full article, "Burr Alert: The Top Eight Things You Should Be Doing to Protect Your Business from Cyber Threats" written by David Dowd III and Elizabeth Shirley.

For further information please contact David Dowd, Elizabeth Shirley or India Vincent - Cybersecurity Chair.