CONNER STRONG & BUCKELEW

The other side of cyber breaches: How to protect yourself from physical damages and business interruptions caused by a cyberattack

BY EDWARD J. COONEY, MBA AND JOSEPH P. HRUBASH

On June 27, 2017, Russian hackers made their way[1] into the internal systems of a multinational life sciences company.

Once inside, they were able to disrupt the company's business operations on an unprecedented scale. The destructive virus known as NotPetya quickly spread across their computer systems, encrypting hard drives and causing machines to malfunction. The company's email system was shut down and 70,000 their employees were barred from touching their work computers.

This company's global drug research, sales and manufacturing was impacted for nearly a full work week. While the final financial consequences of the breach are still being tallied, early estimates indicate the hack and subsequent business interruptions cost the company in excess of $310 million[2].

This is far from an isolated incident – FedEx lost $300 million due to business interruptions in 2017 when its systems were compromised by hackers, and shipping company Maersk also reported $200 million in losses thanks to a similar situation. Hackers are also disrupting electrical[3] grids, gas providers, and other public utility systems that are increasing their reliance on internet-connected devices but lacking in cybersecurity standards.

When most business leaders think of cyberattacks, they tend to focus on the sensitive customer data that will end up in the hands of criminals. However, cyber crooks are increasingly utilizing tactics that target the manipulation or complete shutdown of machinery and systems used to make everything from automobiles to clean water.

Many organizations fail to prepare for the potential physical damage these breaches can cause to their machinery and inventory, as well as the business interruptions that could lead to significant financial loss. When a cyber breach is the root cause of an incident, there are typically some gaps in coverage, or even outright exclusions, in standard business interruption or property insurance policies that could leave companies fully on the hook for any resulting damages.

Thankfully there are a number of preventative steps businesses can take that can deter a cyber breach from happening in the first place and mitigate the damage should one occur. Here are just a few strategies to consider implementing today:

1. **Antivirus software and strong firewalls**
   A firewall is your network's first line of defense against a cyberattack. Firewalls can also block malicious code from entering your network and log specific attempts to breach the system. Antivirus software serves as a detection service to flag any unwanted code. Together, antivirus software and firewalls serve as the foundation for your cybersecurity defense.

2. **Employee training and strong passwords**

A significant portion of cyber breaches are caused by internal employees inadvertently providing access to hackers. Research from the Ponemon Institute and IBM Security found that 28% of breaches worldwide were caused by some form of human error in 2017. Employee training to recognize phishing emails and other malicious attempts to hack the system is imperative. Weak passwords also provide an easy entry point for hackers. Requiring employees to use strong passwords that include a combination of capital letters, symbols and numbers, as well as forcing employees to update those passwords on a monthly basis is another vital step in breach prevention.

3. **Backing up data and software, off the network, at least once a week**

Certain ransomware attacks are capable of holding an organization's internal systems hostage until a ransom is paid. An Indiana hospital paid hackers[4] $55,000 earlier this year to regain control of their software after hackers remotely took control. By backing up their software and data offline, companies can keep their operations running and limit business interruptions during these attacks. However, one backup isn't enough. While daily backups are ideal, businesses need to consistently back up their systems and data at least once a week.

4. **Performing security audits for all network-connected devices**

Every network-connected device serves as a potential entry point for hackers. Late last year a hacker broke into more than 150,000 HP printers just to raise awareness[5] about how susceptible these devices are to a breach. Businesses must conduct a comprehensive review of all network-connected devices to lock all windows and doors by disconnecting any devices that don't need to be connected to the internet and adding protections to those that do.

5. **Swift security patching**

Scanning for cybersecurity deficiencies and then making the patches necessary to address them may seem like a no brainer, but organizations across the globe still fail to properly take care of these shortages in a timely manner, if it all. Credit monitoring firm Equifax failed to spot and address a patchable security deficit that eventually led to its massive data breach last year. Continuous scans and a team dedicated to addressing these security shortfalls are a must.

6. **Robust and rehearsed response plans**

The hope is that by taking these preventative steps, you won't have to worry about being hacked. But in the event that you are the victim of a cyber-attack, drafting and maintaining a response plan is a critical component. Too many organizations are caught flat footed in the event of a cyber breach. Response plans must include backup policies for continuing operations offline while systems are down. Depending on the business, this could take many forms, but any plan that keeps operations running will go a long way in limiting business interruptions. Considering hackers are constantly utilizing new tactics, its imperative businesses constantly update their plans in response to new developments.

7. **Securing the right insurance coverage**

Most companies have some mix of property and business interruption insurance coverage. But many business owners may be surprised to find gaps in coverage or even outright exclusions in these policies for damages caused by cyberattacks. A full-fledged review of existing insurance policies to identify these coverage liabilities is the first step to remedying this issue. There are a few insurance products available which address this common cyber gap in property insurance policies. But without securing that specialty coverage companies may need to make additional adjustments to make sure they're at least partially covered.

NO ONE IS SAFE

Cyberattacks impact every industry, geography, and profession across the globe. These threats are only becoming more sophisticated as hackers develop new malicious techniques and strategies. The potential damages of such an event are extreme, and the next great hack could come in a form we've never seen before.

Implementing a full sweep of preventative measures is even more important for companies with internet connected devices and machines that are directly involved in manufacturing a product. Once compromised, these malfunctioning machines can lead to batches of defective products and months of business delays. Cybercriminals know no bounds when it comes to the type of businesses they target. It can happen to you too.

Sources:

[1] https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP

[2] https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/

[3] https://www.forbes.com/sites/constancedouris/2018/01/16/as-cyber-threats-to-the-electric-grid-rise-utilities-regulators-seek-solutions/#718a99b7343e

[4] https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/

[5] https://gizmodo.com/hacker-claims-he-hacked-150-000-printers-to-raise-aware-1792067012

Edward J. Cooney, MBA

Conner Strong & Buckelew

Vice President, Account Executive/Underwriting Manager

P: 973-659-6424 | ecooney@connerstrong.com

Joseph P. Hrubash

PERMA Risk Management Services

Senior Vice President, Account Executive

P: 973-659-6577 | jhrubash@permainc.com