Cyber Risk. Are You Protected?

PRACTICAL INSIGHTS FROM HUNTINGTON

WannaCry and Spectre. Equifax and Yahoo. For every cybersecurity attack and data breach that becomes infamous enough to be known by a single word, there are hundreds more that never make the news. Cybercrime is happening every day at businesses of all sizes.

"Every CFO of a mid-sized company is also now a Chief Technology Officer, whether they like it or not," said Ben VanVlerah, commercial region manager at Huntington. "CFOs have to understand aspects of technology, including cyber risk*."

In this report, we share an overview of some of the most common cybersecurity threats, discuss how much cyberattacks are costing businesses, and help you begin to develop a plan to mitigate risk and help protect your company against loss when cyberattacks happen.

CYBERCRIME CONTINUES TO SKYROCKET.

According to the Ponemon Institute's *2019 Cost of Cybercrime Study* that evaluated responses from 355 companies in eleven countries, successful breaches have risen more than 11%, to an average of 145 per company each year*. That's a staggering 2.8 successful attacks every week.

145

Successful breaches have risen more than 11%, to an average of 145 per company each year*.

Source: Ponemon Institute, LLC and Accenture Security.

As reported in IBM's *2019 X-Force Threat Intelligence Index*, the most popular ways organizations are being left open to attack is by phishing scams or social engineering, and through incorrect setup of business systems, servers, cloud environments, or overlooking best password practices. These attacks are often facilitated by inadvertent threat actors, who are insiders within your company who unknowingly compromise the environment§.

Nearly one-third—29 percent—of attacks analyzed by IBM involved compromises via phishing emails. Of those, 45 percent involved business email compromise (BEC) scams§, also known as "CEO fraud" or whaling attacks. These attacks use social engineering techniques to impersonate the identity of a trusted coworker or vendor via email. They ultimately attempt to trick an unsuspecting employee into making a fraudulent wire transfer or sharing sensitive data.

BUSINESSES NEED BETTER PREPARATION.

Meanwhile, businesses across every industry are woefully underprepared to deal with these increasingly sophisticated attacks.

In a recent article from InsuranceBee, 54% of surveyed businesses have no plan in place to deal with a cyber attack¶.

"Imagine a scenario where you have to suddenly shutdown your systems for a week because of a cyberattack," said Jeff Blendick, senior managing director, institutional banking, at Huntington. "What is your plan from a treasury management perspective? How would you pay your most important vendors? What would you do to make sure your employees get paid? How will you recover business operations#?"

One suspected reason for the disconnect between risk and response is business leaders often have what psychologists call "optimism bias." This is the tendency to underestimate the likelihood that their company will experience adverse events, even when others are clearly seeing negative impacts[¥].

54%

of surveyed businesses have no plan in place to deal with a cyber attack[¶].

Source: InsuranceBee

Ultimately, many small business owners feel they are not a target. According to data from Jungle Disk, small business owners are reporting that they don't feel "on the radar" or at risk of malicious attacks because hackers only care about "the big guys," not the small mom and pop shops[¥].

However, this assumption may not be well-founded. Verizon reports in a recent study that 43 percent of breaches involved small business victims[≠]. And regardless of company size, Jungle Disk data reveals that 43 percent of companies with a major data loss go out of business[¥].

People are going to retain their optimism, regardless of the facts on cybersecurity, the likelihood of being hacked, the ways they can be hacked, or the lasting influences an attack can have on their business[Ł].

Even businesses who have a formal plan to deal with a cyber attack, need to help protect their business by increasing spending on security-related hardware, software, and services. An encouraging sign is that worldwide spending on these tools will be $106.6 billion in 2019, an increase of 10.7% over 2018[Ł]. As threats continue to rise, a correlation in spending from businesses is to be expected.

What does cyber risk look like?

Add Texas to the growing list of states hit by cyberattacks. On a single morning in August of 2019, more than 20 cities were hit by a coordinated ransomware attack. According to the Texas Department of Information Resources (DIR), most of the attacks were made against small local governments[¥].

Cybersecurity experts from numerous state and federal agencies responded to the attacks, including the DIR, the Department of Homeland Security, the F.B.I. and the Federal Emergency Management Agency.

With an emergency response plan in already place, it was activated within hours the attack. Teams were dispatched to the most critically impacted sites to eradicate the malware and assess the impact on systems. It took a full week for business-critical services to be restored.

The identity of the attacker(s) has not been revealed, and it remains unclear the amount of ransom demanded and whether ransom was paid.

Tips for Helping to Protect Your Business

WHAT YOU CAN DO TODAY TO HELP PREVENT ATTACKS:

1. Backup your data and update and patch systems
2. Make sure your security solutions are up to date
3. Review and exercise your incident response plan
4. Pay attention to ransomware events and apply lessons learned

WHAT YOU CAN DO TO RECOVER IF IMPACTED:

1. Isolate the infected systems and phase your return to operations
2. Review the connections of any business relationships that touch your network
3. Apply business impact assessment findings to prioritize recovery

WHAT YOU CAN DO TO HELP SECURE YOUR ENVIRONMENT IN THE FUTURE:

1. Segment your networks
2. Develop containment strategies
3. Review disaster recovery procedures and validate goals with executives

Source: The Cybersecurity and Infrastructure Security Agency (CISA)[π].

As well, companies often ignore employee training, which many experts say can be the best defense for the money.

"It often comes down to human error," said William Carlin, insurance product specialist at Huntington Insurance, Inc. "All it takes is one employee to click on a link or mistakenly get duped into making a wire transfer. With one mistake, criminals can get through prevention measures no matter how good they are[Ω]."

43%

of breaches analyzed involved small business victims[≠].

Source: Verizon.

COSTLY IMPACTS OF CYBERCRIME.

Without a sound plan or adequate safeguards to thwart attacks, companies can experience massive losses. The *2019 Cost of Cybercrime Study* found that in those surveyed, the total average cost of cybercrime attacks for an organization totals $13 million per year[‡].

German insurance and investment provider Allianz estimates the aggregate total of annual losses associated with cybercrime in the United States at $108 billion[††]. That's almost as much as the estimated $125 billion in damage caused by Hurricane Harvey—the second-most costly hurricane in U.S. history according to NOAA National Centers for Environmental Information[‡‡].

"Businesses may not realize that even the cost of a forensic investigation can cost six figures," said Ashley Bauer, marketing manager at Huntington Insurance, Inc[§§].

While the cost of cybercrime varies across industries and company size, smaller companies often pay the ultimate price when they are forced to close operations due to financial hardship or damaged reputation.

CFOs MUST ENGAGE.

As risk-management leaders within an organization, CFOs and Treasurers must work with their boards of directors, IT business unit leaders and financial institutions to protect corporate data and systems without handcuffing the technologies that improve speed, efficiency and connectivity of their operation.

Your Business Can Be Affected

Avoid unnecessary costs by seeing the impacts it can have on your business, big or small.

An accounting employee at a large automotive business fell for a business email compromise (BEC) scam. The employee was fooled into making a large external fund transfer, which ultimately cost the company over $35 million dollars.

The president of a mid-size energy firm was persuaded by the supposed CEO of an overseas parent company to wire $200K to a foreign bank account. The president was tricked into it by the method of deepfake audio, a technology that can reproduce someone's voice.

An employee at a small machinery business downloaded ransomware onto the network of a public entity. Hackers used the employee credentials to gain access to systems and used their ransomware to encrypt many systems throughout the business. This ransomware incident cost the business over $12K.

"Cybersecurity should be viewed in conjunction with an overall business continuity strategy, and your financial institution should be helping your business operate and be successful," said Don Boian, cybersecurity outreach director at Huntington[¶¶].

Huntington serves both as a strategic resource to help businesses approach risk and as a provider of secure financial management solutions. For example, Huntington offers a **suite of treasury management products** designed to help guard against both paper and electronic payments fraud.

In addition, **Cyber Liability Insurance** is offered through Huntington Insurance, Inc. By offering insurance coverage in addition to standard financial services, Huntington offers a more comprehensive and convenient way to help businesses protect themselves against the negative impacts of cyber risk.

$108 billion

Estimated annual losses associated with cybercrime in the United States[†].

Source: Allianz Global Corporate & Specialty

"There is no one-size-fits-all cyber policy," said Carlin. "Some have better business interruption coverage, others have good third-party liability coverage. We get into those details to help clients find the match for their needs. Sometimes that means several different policies[Ω]."

For businesses that need to upgrade technology or replace aging IT infrastructure that is vulnerable to attack, Huntington has a variety of financing options.

"I think that soon companies will realize that a cyberattack is going to happen," said Bauer. "We can't outspend the criminals to entirely prevent it. It's best to be resilient when it happens. Contain it. Respond to it. Move on. So it's not a detrimental or catastrophic event. It just becomes another cost of doing business[§§]."

Huntington recommends conducting a risk assessment to determine what products and services would benefit your company.

Talk to a local Huntington banker about helping to manage and mitigate the impact of cybercrimes on your company.

About Huntington

Huntington Bancshares Incorporated is a regional bank holding company headquartered in Columbus, Ohio, with $108 billion of assets and a network of 868 full-service branches, including 12 Private Client Group offices, and 1,687 ATMs across seven Midwestern states. Founded in 1866, The Huntington National Bank and its affiliates provide consumer, small business, commercial, treasury management, wealth management, brokerage, trust, and insurance services. Huntington also provides vehicle finance, equipment finance, national settlement, and capital market services that extend beyond its core states.

Visit huntington.com for more information.

† *Ben VanVlerah interview. August, 2017.*

‡ *The Cost of Cybercrime. Ponemon Institute, LLC and Accenture Security. March 6, 2019.*

§ *2019 X-Force Intelligence Index. IBM. 2019.*

¶ *Cybercrime Survey Reveals SMB Owners are Unaware and Unprepared. InsuranceBee. 2019.*

Jeff Blendick interview. January 24, 2020.

¥ *Watts, Beth. Data Breach Optimism Bias: The Importance of Being Vigilant. Jungle Disk. February 23, 2018.*

¥ *Update on Texas Local Government Ransomware Attack. Texas Department of Information Resources. September 5, 2019.*

≠ *2019 Data Breach Investigations Report. Verizon. 2019.*

Ł *Barker, Jessica. The Human Nature of Cybersecurity. EDUCAUSE Review. May 20 , 2019.*

Ł *New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services. IDC. October 16, 2019.*

π *CISA Insights – Ransomware Outbreak. The Cybersecurity and Infrastructure Security Agency. August 21, 2019.*

Ω *William Carlin interview. October 4, 2019.*

†† *A Guide to Cyber Risk. Allianz Global Corporate & Specialty. 2019.*

‡‡ *Weather Disasters and Costs. Office for Coastal Management: National Oceanic and Atmospheric Administration. August 12, 2019.*

§§ *Ashley Bauer interview. January 16, 2018.*

¶¶ *Don Boian interview. September 24, 2018.*