Cybersecurity. Why It's More Essential Than Ever.

Cybercrime is happening every day at businesses of all sizes. It's an unavoidable reality of doing business. Yet, many businesses do not have a formal plan to help protect their data and networks. This lack of preparedness can be critical, if not catastrophic, because cybercrime continues to rise.

RISING RATES

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

COMMON CURRENT THREATS

According to IBM's *2019 X-Force Threat Intelligence Index*,‡ people inside of organizations will continue to jeopardize cybersecurity in 2019. IBM refers to them as inadvertent insiders.

Inadvertent insiders are people within your business who unwittingly compromise the organization by falling for phishing scams or social engineering. They can also create compromise through improper configuration of systems, servers, and cloud environments, and by not following password best practices.

145

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

Source: Ponemon Institute and Accenture†

In its analysis, IBM determined that 29% of reported attacks involved compromises via phishing emails and 45% of those were business email compromise (BEC) scams. These attacks use social engineering techniques to impersonate the identity of a CEO or high-ranking employee via email. These emails are sent to those who control bank accounts with instructions to make fraudulent wire transfers. At last count, the FBI reports that BEC fraud has cost organizations across the globe more than $12.5 billion.§

In a disturbing trend, the IBM research found that misconfigured cloud servers contributed to the exposure of more than 990 million records in 2018. It's why a majority of IT and security professionals noted misconfigured systems as a serious cloud security risk because they help give attackers access to a diverse range of sensitive data including email addresses, user names, passwords, credit card and health data, and national identification numbers.

According to the IBM study, spam and malware continued to be prevalent in 2018, spreading malicious links and attachments to users all over the world. Clicking on these links opens the doors to a business's sensitive data.

PREPARATION REQUIRED

Across every industry, many businesses are dangerously unprepared to deal with attacks that are growing in sophistication and number. In fact, a 2017 survey by IBM and Ponemon of 2,400 security and IT professionals found that 75% of respondents said they did not have a formal cybersecurity incident response plan across their organization.‖

Even businesses that have a plan are likely underfunding it. According to a 2017 article in the *Harvard Business Review*, firms typically allocate just 5% of their overall IT spend to security.# And something as simple as employee training is often overlooked, which many security specialists consider the best defense.

"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."¶

COSTLY DAMAGE

The Ponemon Institute's *Ninth Annual Cost of Cybercrime Study* found that, in those surveyed, the total average annual cost of cybercrime attacks for an organization in 2018 was $13 million.†

75%

Of respondents said they did not have a formal cybersecurity incident response plan across their organization.

Source: Hacked: How Business is Fighting Back Against the Explosion in Cybercrime‡

The Center for Strategic and International Studies (CSIS) and McAfee estimated the 2017 cost of cybercrime in North America at between $140 billion and $175 billion.Ω For smaller businesses, the consequences can be catastrophic, when they are forced to close due to financial hardship or damaged reputation.

A CRITICAL PRIORITY

Business owners should work with IT staff or consultants and financial institutions to help protect data and systems without hindering the technologies that advance their operation.

"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, director of cybersecurity outreach for Huntington.¶

"I think that soon companies will realize that a cyberattack is going to happen," said Ashley Bauer, marketing manager at Huntington Insurance, Inc. "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."¶

For a deeper analysis of cyber risk, download our white paper and talk with a Huntington banker about helping to mitigate the impact of cybercrimes on your business.

$13 Million

The total average annual cost of cybercrime attacks for an organization in 2018.

Source: Ponemon Institute and Accenture†

About Huntington

Huntington Bancshares Incorporated is a regional bank holding company headquartered in Columbus, Ohio, with $109 billion of assets and a network of 950 branches and 1,770 ATMs across eight 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 auto dealer, equipment finance, national settlement, and capital market services that extend beyond its core states. Visit huntington.com for more information.

---

† *The Cost of Cybercrime. Ponemon Institute LLC and Accenture. 6 March 2019.*

‡ *2019 IBM X-Force Threat Intelligence Index Report. IBM. February 2019.*

§ *Business E-Mail Compromise: The 12 Billion Dollar Scam. Federal Bureau of Investigation. 12 July 2018.*

‖ *Roberts, Jeff John and Lashinsky, Adam. Hacked: How Business Is Fighting Back Against the Explosion in Cybercrime. June 2017.*

Vintz, Steve. CFOs Don't Worry Enough About Cyber Risk. Harvard Business Review. 1 December 2017.

¶ *"Practical Insights: Cyber Risk." Huntington National Bank. May 2018.*

Ω *Economic Impact of Cybercrime—No Slowing Down. The Center for Strategic and International Studies (CSIS) and McAfee. February 2018.*
