Why You Should Consider Cyber Insurance for Your Company (INFOGRAPHIC)

Brian Wallace, Founder & President, NowSourcing

Is your business ready to face a successful ransomware attack and come out alive on the other end? Most small to midsize businesses are not. In fact, 45% of SMBS report that their cyber security is ineffective. They could easily be overtaken by ransomware.

In the past year, 66% of SMBS have fallen prey to at least one cyber attack, with ransomware being the most common method of attack. Just one successful ransomware attack can mean the loss of copious amounts of money in ransom, extortion, and recovery efforts. It can mean the loss of privacy as personal information may be publicized. It can mean the loss of productivity as systems shut down, and it could mean the loss of reputation as the majority of customers stop doing business with a company that has experienced a data breach. All of this combined means the loss of the entire business within 6 months of attack for 60% of companies who fall victim to ransomware.

Since the beginning of the COVID pandemic in 2020, ransomware attacks have risen by 50%. That means that, every 10 seconds, a person, device, or business is hit by a ransomware attack. The rise in these attacks comes largely from the 70% of the American workforce that began working from home last year. With the sudden surge in use of personal devices and personal networks, rather than company devices and networks, cyber security has taken a huge hit. As IT departments are left blind to the dangers and threats against personal devices and networks, cyber criminals have had a field day with the flimsy security suddenly facing most companies.

The cost of these attacks is also taking a sharp upturn. Just a few years ago, in 2019, damages due to cyber attacks amounted to 4 billion dollars, but by 2028, it’s expected to reach 28 billion dollars. In 2015, damages due to ransomware cost 24 million dollars, but just 5 years later, in 2020, that amount was at 170 billion.

Most SMBS are not prepared to survive these attacks. Security measures don’t meet the demand. “Strong” passwords, password authentication apps, and two factor authentication methods can all be easily hacked, leaving SMBS vulnerable to attack and failure.

Cyber insurance is one way that SMBS can help protect themselves. It doesn’t keep the attack from happening, but it’s a cushion that could help these businesses pull through to live another day.

CYBERINSURANCE AND WHY IT MATTERS

In 2020, daily ransomware attacks increased by 50%

CYBERATTACKS ARE ON THE RISE

$ 4.4 million
Largest attack on a U.S. energy system

$ 11 million
Largest reported ransom payment

$ 50 million
Largest reported ransom demand

THE COST OF CYBERCRIME

Cybercrime is comparable the third largest economy on Earth

DAMAGES DUE TO CYBERCRIME

- 2019 - $4 billion
- 2020 - $7 billion
- 2025 - $28 billion

Ransomware is most common method of attack

DAMAGES DUE TO RANSOMWARE

- 2015 — $24 million
- 2016 — $209 million
- 2020 — $170 billion

Sources:
global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031

WHY ARE ATTACKS INCREASING?

EXPANDING ATTACK OPPORTUNITIES

IN 2020, A PERSON, BUSINESS, OR DEVICE WAS ATTACKED BY RANSOMWARE EVERY 10 SECONDS

More Users
By 2023, 5.3 billion people worldwide will have access to the internet

More Devices
By 2023, there will be 3.6 connected devices for every person on Earth

More Data
By 2022, world data will more than triple — half of that data will be stored in the cloud

THE ROLE OF WORK FROM HOME

70% OF AMERICANS WORKED FROM HOME IN 2020

With more people working online, risk increased exponentially

- Data is often shared across multiple apps and cloud services
- IT departments are blind to security weaknesses at home
- Remote workers are more likely to use personal devices

Sources:
global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031

BUSINESSES ARE UNPREPARED FOR THESE ATTACKS

45% OF SMALL TO MIDSIZE BUSINESSES (SMBS) SAY THEIR CYBERSECURITY IS INEFFECTIVE. IN THE PAST YEAR...

66% of SMBs fell victim to at least one cyberattack

60% go out of business within 6 months after a data breach or hack

SECURITY "BEST PRACTICES" FALL SHORT

Many common protection tools can be hacked

- Two factor authentication
- "Strong" passwords
- Password manager apps

If a single cyberattack is successful, you can lose everything

- Money: Paid for ransom, extortion, or recovery efforts
- Privacy: Personal information may be publicized
- Productivity: Halted operations when systems shut down
- Reputation: Loss of trust after a breach is announced

Sources:
hackerpocalypse-cybercrime-report-2016

IS CYBERINSURANCE THE SOLUTION?

IS CYBERINSURANCE WORTH THE COST?

SMBs CYBERINSURANCE POLICIES USUALLY COVER UP TO $1 MILLION IN DAMAGES

COVERAGE INCLUDES

- **Profit losses** — Including reputation damage or halted operations
- **Liabilities** — Including contract penalties and media fines
- **Lawsuits** — including class-actions and regulatory investigations

COVERAGE DOES NOT INCLUDE

- **Physical property** — Replacement of damaged or "bricked" devices
- **Future loss of profits** — Long term losses after a cyberattack
- **Intellectual property** — Loss of company value after data is leaked

By 2028, spending on cybersecurity services will grow to

$193 BILLION

with SMBs putting 5-20% of their IT budget toward preventing an attack

Sources:
pennyriletechnologies.com/how-much-do-smbs-really-spend-on-cyber-security
prnewswire.com/news-releases/cyber-security-services-market-size-worth-192-70-billion-by-2028-grand-view-research-inc-301267353.html

RANSOM PAYMENTS MAY NOT BE COVERED

IN THE FIRST HALF OF 2020, 41% OF CYBERINSURACE CLAIMS RELATED TO RANSOMWARE ATTACKS

BUT, MANY INSURERS HAVE STOPPED COVERING THE COSTS OF RANSOMS — INSTEAD LIMITING COVERAGE TO OTHER DAMAGES

Rising demands make coverage unaffordable

From 2020 to 2021, the cost to recover from ransomware increased 243% — the highest reported paid ransom was over $3 million

Ransom payments may be prosecuted

In the U.S., making payments to officially sanctioned individuals and jurisdictions is illegal — including ransom demands

Sources:
secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
threatpost.com/cyber-insurance-ransomware-payments/160580

About the Author: *Brian Wallace is the Founder and President of NowSourcing, an industry leading infographic design agency in Louisville, KY and Cincinnati, OH which works with companies ranging from startups to Fortune 500s. Brian runs #LinkedInLocal events, hosts the Next Action Podcast, and has been named a Google Small Business Adviser for 2016-present. Follow Brian Wallace on LinkedIn as well as Twitter.*