The Coming Cyber Crime War

What Every Business Gets Wrong about Cyber Threats

By Adam Puharic – President, Puharic and Associates

E-mail: Adam@puharicassociates.com

A drastically underreported business event in late March of 2021 may have signaled "the opening trumpets" to a cyber war and crime spree growing in threat to all businesses. According to Bloomberg News, CNA Financial Corp., among the largest insurance companies in the U.S., paid $40 million to regain control of its network after a ransomware attack. The irony of a modern, nationwide insurance company and significant provider of cyber liability insurance falling prey to hack, encryption and ransom cannot be overstated.

In December of 2020, SolarWinds, a system management software provider used by the IT industry to facilitate remote access was hacked. This is very significant because this was an instance where cyber criminals evolved their strategy from robbing individual banks to "stealing the keys" for entire industries. In January of 2022, Okta, an authentication company used by thousands of organizations around the world, revealed how a cyber attacker had access to one of its employees' laptops -- though they deny a breach occurred.

But this will not impact your business, will it? You cannot possibly need more information on cyber security, can you? You have done all the right things: You have a reputable IT services provider monitoring your systems 24 hours a day. You've purchased higher limits for your cyber liability insurance policy. You change your password every other day. What else can you do?

Many business owners and leaders have become exhausted discussing the topic of cyber security, which a few short years ago was on the periphery of prominent issues facing their businesses. Then came the pandemic, the work-from-home transformation, the global supply chain disruption, and the geo-political dangers of 2022. Your business has transformed beneath your feet, changing the operations from a service or product delivery company, into a technology company that facilitates goods and services.

So yes, regretfully you may be approaching cyber security wrong. By compartmentalizing cyber responsibilities, ignoring the transformation of business operations, and denying cyber security's rightful position as the key strategic risk you face, you may be falling into a complacent trap that could prove fatal to the growth, integrity, and sustainability of your business.

Specifically, there are five things every business owner needs to know right now about their cyber vulnerability:

1. **Your core business model has changed, and your operations are no longer extricable from technology.**

When you began, you could describe your operations in a single sentence using the model: "we provide X goods or services to our customers." After the government forced work-from-home lockdown of 2020 and 2021, in many cases without a conscious understanding of the change, many businesses now use more sophisticated technologies that employ multiple software and hardware methodologies to provide goods or services to their increasingly remote and hybrid customer base. In most cases, without willful planning, the technology component changed from a force multiplier and convenience tool to a mission-critical and core business function. Take a moment and contemplate your operations without the technology changes of the last two years?

With the preceding revelation in mind, it is time to revisit your strategic business plan. Where have you placed technology in the matrix of company priorities? How often do you revisit these priorities? Does this emphasis on technology translate up, down and sideways to every level of employee? Do you embrace technology as a partner in your business and provide the resources worthy of its status?

2. You must break the silo approach to insurance and IT services. Now! They must go hand-in-hand to protect your most valuable asset – your business.

If you currently carry cyber liability insurance, you might be familiar with the various insurance carrier questionnaires that are used to understand your company risk and develop pricing. You may even be forward-thinking enough to share the questionnaire with your current IT services partner. But now is the time to bring those teams together. Schedule a three-way meeting. Review the questionnaires of not only your current carrier, but the questions asked by every carrier your insurance professional has access to. Demand your insurance provider expand their market reach and professional education on the topic. Review the key critical questions with your IT services provider and develop a timeline to "get to yes," that is, a plan to be 100% compliant with the latest insurance carrier mandates.

The simple truth that is sometimes overlooked is that the cyber insurance questionnaire is developed in response to the claims the carrier has witnessed or become wary of. The insurance carrier is tipping their hat and showing their cards about the core areas of cyber vulnerability. Your insurance agent has this knowledge but might not be aware of the power this knowledge can provide if put in the hands of the IT vendor you hired to protect your technology and data. Better yet, consider partnering with an insurance professional who has developed an integrated solution that pairs insurance with an IT services provider in a collaborative, sharing and communicating environment.

3. Every employee must take a proactive role in learning to prevent and identify hacking attempts as they have become that last line of defense, a human firewall, for your business.

The time has come to implement regular, company-wide awareness training designed to empower employees at every level of the company to fight and win in this new cyber war. Employee training should focus on:

- How to create passwords that can't be hacked.
- Business password managers.
- How to identify fraudulent, spoofed (fake) email.
- How to best protect against ransomware.
- What is Zero Trust and why it is effective.

This is no longer a luxury affordable only to the larger employers. Every business that has been transformed by the technology revolution and hybrid work environment must engage with an IT services firm capable of training efficiently and effectively.

4. You must implement new technologies **NOW**.

Fourth, cyber liability insurance carriers are demanding that clients move towards some common and emerging technology strategies:

- Multi-factor authentication (MFA) access to email and to remotely access your company files.
- A 3-2-1 backup solution (3 different backups on 2 different kinds of media, with at least 1 offline).
- Cybersecurity and phishing training as per above.
- Least privileged access to files (especially PII and PHI).
- Data encryption on mobile devices and backups.
- Zero-trust security. Zero Trust is a shift of network defenses toward a more comprehensive IT security model that allows organizations to restrict access controls to networks, applications, and environment without sacrificing performance and user experience. "Never trust, always verify."
- Endpoint detection and response (EDR).

5. You must recognize that ignorance is no longer an option.

Finally, and most importantly, you, the business leader, need to embrace cyber security as a mission-critical center of knowledge. It is your responsibility to read the latest, meet regularly with your IT professionals and Cyber insurance providers, and force cooperation among multiple vendors. You must engage in a program of regular training among team members to identify and respond appropriately to cyber threats. You must provide strategic thinking and break patterns of operations to create a "hardened target" that cyber criminals will pass by for easier and more vulnerable victims. You must build system redundancy and game-plan for hacking incidents and company response. The cyber war is now, and you can no longer afford to remain a bystander!

Puharic and Associates, Inc. is a professional risk management and insurance firm in Manasquan NJ. Puharic focuses on concierge-style risk management to provide 360-degree protection for business owners by combining all insurance coverages under one roof. By creating a 3-dimensional risk profile of the business owners' risks, from cyber to employee benefits to personal risks, Puharic and Associates helps business owners grow by creating a step-by-step plan for their protection that evolves with them.
For more information, please visit www.puharicassociates.com