

Five Measures for Effective Cybersecurity After COVID-19

Around the world, the coronavirus pandemic has had powerful effects on industries of all types. Businesses were forced to adapt quickly to protect their customers and their employees. Because COVID-19 required stringent social distancing and self-quarantine restrictions, many businesses shifted to online work environments to remain in operation. Other companies focused on e-commerce, allowing them to continue delivering the goods and services consumers needed. Cybersecurity, then, became ever more important, as remote employee access and online shopping took center stage in many business operations. As an effective risk-management strategy, business owners must leverage the protection of cyber liability insurance plans and industry best practices to keep their networks and their sensitive data safe.

Challenges and Risks During the COVID-19 Pandemic

As businesses revamped their operations, moving to remote work environments for their employees, challenges and risks for cybersecurity professionals and business leaders grew rapidly. Some of the challenges include:

- Access to critical business networks via personal computing devices and on less-secure home networks.
- Employees unfamiliar with cybersecurity practices, making them vulnerable to social engineering hacks and similar cyber criminality.
- Targeted attacks by criminals on already-strained networks, particularly critical services such as healthcare and banking operations.
- A change in perceptions about anomalous network behaviors. Prior to the pandemic, these behaviors were seen as evidence of criminals attempting to breach computer security. Now, with so many people working from home, anomalous behaviors are the norm rather than the exception, making actual criminal activity harder to spot.
- Flaws in security on popular productivity software products, including video conferencing platforms like Zoom.

Most importantly, business leaders may not be fully aware of the cyber risks their companies face in the dramatic upheaval of the pandemic and its aftermath. While cyber liability insurance is designed to protect against many risks associated with network breaches and data loss, it is critical that leadership understands these risks and makes efforts to manage them effectively.

The 5 Measures: Cybersecurity Now and Post-Pandemic

In response to the unprecedented cyber risks exacerbated by the pandemic, the World Economic Forum (WEF) published a report entitled "Cybersecurity Leadership Principles: Lessons Learnt During the COVID-19 Pandemic to Prepare for the New Normal." The report's aim is to shape adequate responses to growing cyber threats, and contains five measures that will shape the future of cybersecurity. The five measures are:

- 1. Fostering a culture of cyber resilience:** As risks grow and wane, resilience is the key to continued data safety. Implementing proactive risk management practices and developing strategies to recover from cyber attacks are among the recommendations of the WEF.
- 2. Focusing on protection of critical assets and services:** It is impossible for businesses to protect every aspect of an operation. Instead, identifying and prioritizing those assets and services that are critical for business continuity while maintaining compliance with privacy and data security regulations is the better course of action.
- 3. Balancing risk-informed decisions within the pandemic and in the future:** Implementation of new systems and practices always come with new risks. Leaders must balance those risks and may have to make difficult decisions as they adapt to the "new normal." Maintaining flexibility by continual reassessment of existing and emerging risks will help balance risk exposures.
- 4. Updating and practicing response plans, including those designed for business continuity:** While many companies have created business continuity and data breach response plans, these are not static documents. Risks evolve, and even the best plan is useless without testing its capabilities. By updating and practicing the plans, deficiencies can be uncovered and remedied before an actual response is needed.

5. Strengthening collaboration throughout the business ecosystem: Establishing and building partnerships between public and private entities regarding cybersecurity is the key to continued success. Sharing information between partners in a transparent manner is the goal of this collaborative effort. By leveraging the power of collaboration, business leaders can more quickly identify emerging threats and take the steps needed to manage or eliminate those threats before they can cause an embarrassing and expensive data breach.

Summary

The future is uncertain, but what is certain is that cyber criminality will continue to threaten the business world. In addition to protecting assets and systems with robust cyber liability insurance plans, insurance agents must provide their clients with the information and practices designed to manage risks going forward. The COVID-10 pandemic has been a challenging time, but it has also provided an important learning experience for industries around the world. These lessons will shape the direction of cybersecurity response for years to come.

Sources

Blauner, Charles and Georges de Moura. "5 Principles for Effective Cybersecurity Leadership in a Post-COVID World." World Economic Forum, May 26, 2020, <https://www.weforum.org/agenda/2020/05/principles-for-effective-cybersecurity-leadership-covid-19-coronavirus-pandemic-cyberattacks-cyber-risk-security-cloud-technology/>.

"Cyber Liabilities in the Financial Sector," U.S. Risk, LLC, February 24, 2020, <https://www.usrisk.com/2020/02/cyber-liabilities-in-the-financial-sector/>.

De Moura, Georges, et al. "Cybersecurity Leadership Principles: Lessons Learnt During the COVID-19 Pandemic to Prepare for the New Normal." World Economic Forum, May 22, 2020, http://www3.weforum.org/docs/WEF_Cybersecurity_leadership_principles_for_the_Covid_19_pandemic_2020.pdf.

About U.S. Risk

U.S. Risk, LLC is a wholesale broker and specialty lines underwriting manager providing a wide range of specialty insurance products and services. Headquartered in Dallas, Texas and operating 16 domestic and international branches, U.S. Risk and its affiliates can help you access a world of new markets and products. For more information, contact us today.

Toll-free: (800) 232-5830 | Visit us at [usrisk.com](https://www.usrisk.com)