12 Cyber readiness strategies to reduce corporate risk

The alarming security statistics for 2021 are a call for companies and leaders worldwide to take risk management more seriously.


Philippe FUNK

LUXEMBOURG, LUXEMBOURG, LUXEMBOURG, November 23, 2021 /EINPresswire.com/ -- Cybersecurity statistics point to a gap between growing threat warnings and U.S. trends. Cybersecurity statistics are heuristics of value, but they also point to gaps in alerting threats and trends.

The alarming security statistics for 2021 are a call for companies and leaders worldwide to take risk management more seriously. Organizations need a cybersecurity strategy to protect infrastructure and customer data against growing cybersecurity threats. The challenge is to translate cybersecurity statistics into a functional, agile risk management strategy to defend ourselves.

> Imagination is more important than knowledge. For knowledge is limited, whereas imagination embraces the entire world, stimulating progress, giving birth to evolution."
>
> *Albert Einstein*

The CISA (Coal Mine and Combined Security Agency) developed Cyber Essentials - a guide for small businesses and local government officials to build an actionable understanding and implement organizational cybersecurity practices. In a webinar for the U.S. Chamber of Commerce on June 29, CISA leaders gave insights into the pillars of the Cyber Essential Plan and provided a starting point for greater resilience and building a corporate culture of cyber readiness. The Cyber Essential Plan leads cyber readiness to a holistic approach that goes beyond get-it-out-of-the-silos and addresses cybersecurity at a broader organizational level, considering the teamwork of an organization's cybersecurity practices.

The report includes a new cyber readiness model that measures a company's strength in six critical areas of cybersecurity: people, processes, and technology. The model should be interactive, allowing companies to compare their cyber maturity with their peers and draw on best practices in each area to develop cyber resilience, Hiscox says. The survey respondents' findings show that the model highlights several companies that lack "genuine cyber resilience," the report said.

The report highlighted the wide variety of financial costs incurred by cyberattacks, with smaller companies having the most significant losses relative to the company's size. The economic cybersecurity costs of breaches have increased significantly in recent years. Nearly 5% of the companies surveyed experienced a cyberattack and incurred costs of $300,000 or more.

According to Hiscox's 2019 Cyber Readiness Report, the average cost of a cyberattack has risen from $34,000 to $200,000 for a single incident. Forty-seven percent of small businesses have experienced cyberattacks against them in the past year, and 44 percent have experienced more than one. According to the Hiscox Cyber Readiness Report 2021, the proportion of companies targeted by cybercriminals has increased from 38% to 43% in the last year, and a quarter of attacked companies (28%) have experienced five or more attacks.

Malicious hackers know that most small organizations are not sufficiently prepared for security breaches on the network, making them popular targets for cyberattacks. Smaller companies must implement robust security strategies to protect sensitive information from the ubiquitous cyber threat.

As cybercriminals evolve their technology and attack strategies, organizations need to adapt their approach to cybersecurity and privacy. Businesses need to protect their workload, data, and applications in multiple areas, and this requires an integrated solution with automated system monitoring, vulnerability assessment, and endpoint protection to stop emerging threats. File backups can protect against digital interference by malicious actors.

As part of your cyber preparedness plan, you should use protocols to assess and monitor the security of your vendor networks and third-party vendors. Businesses need to plan and prepare to defend themselves against all threat scenarios because cybercriminals need to find every single vulnerability or gap in their defenses to carry out their evil plans.

For small businesses today, it doesn't matter where a cybersecurity incident happens. Making network security a priority for small businesses is a must as cyberattacks continue to increase.

In the face of security crises such as ransomware and phishing, which in most cases show that no one is invulnerable, it has become necessary to have a security team that can respond in real-time and wards off attacks. Cybercriminals exploit network vulnerabilities that companies may not be aware of, so developing an approach based on your specific risks is the key to combatting

devastating attacks. With multiple security crises occurring in 2020 and continuing to harm the unprepared, it is worth taking the time to evaluate and choose your best strategy and how to implement it.

As we move further into 2021, it is worth examining up-to-date statistics from many articles and blogs and their potential impact on cybersecurity for our rapidly changing digital landscape. I have divided cybersecurity statistics into several categories to exploit this information, including top sources for cybersecurity statistics, cybersecurity readiness status, types of cyber threats, and economic cybersecurity data risk. There are many other categories of cybersecurity that require more profound insights, including perspectives on the cloud, the Internet of Things, open-source, deep counterfeiting, lack of skilled cyber workers, and statistics on many other types of cyberattacks.

Essentially, cybersecurity values define an organization's general commitment to readiness and reduce the likelihood and severity of cybersecurity events. Different aspects of cybersecurity can be assessed for consistency, but displaying a cybersecurity thumbprint indicates values and willingness for cybersecurity. Moreover, the cyberculture must mature to absorb these values and create an attitude.

Invest in external moderators, fire drills, and tabletop exercises to test the company's response plan at a level that enables rigorous testing and disconnects from dynamic internal leadership when the organization wants to conduct internal drills to prepare for cyberattacks. Once an organization knows its role and responsibilities and manages potential problems, its response to a live cyber attack can be a considerable burden. Responding to this is not only the responsibility of your cybersecurity team, but every organization has a role to play.

The Ponemon survey found that 47% of organizations do not regularly assess the readiness of their response teams, meaning they test their plans for the first time at the worst possible time - amid a cyberattack.

Philippe FUNK
White Hat Hackers
email us here