Cybersecurity – The #1 Risk Business Leaders Can't Afford to Ignore

AUGUST 13, 2021 | ARTICLES

The risk of cybercrime to businesses of all sizes is very real, with significant costs, and can no longer be ignored. Planning ahead is essential to ensuring business continuity. Cybersecurity Ventures, a leading researcher and online resource for the global cyber economy projects global cybercrime costs to increase by 15% per year, reaching $10.5 trillion annually by 2025. And according to global cybersecurity leader Trend Micro Inc., in their Cyber Risk Index Report, an annual survey of 2,800 IT managers and practitioners from the US, Europe, and Asia/Pacific, 26% of global corporations fell victim to 7 or more cyberattacks in the past year, and over 80% of these expect such attacks to be "somewhat" or "very likely" to succeed.

Coronavirus Drives Pivot in Cybersecurity Response

Since COVID-19, the demand for enhanced cybersecurity across industries has increased exponentially, with specific needs to address the new realities of a world in pandemic mode. As companies shut down and employees worked from home in unprecedented numbers, chief information security officers (CISO's) had to create secure connections for this extensive new remote workforce. Also, the surge in online commerce required significant systems upgrades. CISO's had to reallocate budgets to cover COVID-related costs, putting planned security improvements on hold and possibly exacerbating already identified risks and existing threats.

Identifying Vulnerabilities, Understanding Consequences Essential to Cyber Defense

The first step in defending against cybercrime is understanding risks and identifying where your systems are susceptible. According to Trend Micro's Cyber Risk Index, top cyber threats include:

- Ransomware (malware that cryptically blocks access unless a ransom is paid)
- Social engineering/phishing (techniques to trick people into providing personal data)
- Clickjacking (concealed hyperlinks trick people into unintended actions revealing personal data and allowing control of one's computer)
- Fileless attacks (tools built into software that allow attack and leave no code, file, or traceable footprint)
- Botnets (unsuspecting network of computers infected by malware and controlled by a hacker)
- Man-in-the-middle attacks (attacker intercepts communications between users, able to "eavesdrop" or alter the communications)

Certain situations present particular vulnerabilities: In automated buildings, every system and device are unique yet connected, each with its own unique cyber risks; and connected devices are easy to infiltrate. Healthcare facilities are high-value targets, with hackers launching constant attacks; medical records are "best sellers", fetching up to $1,000 per record on the dark web (Forbes.com 1/8/2021).

When developing a cyber defense plan, organizations should also consider potential problems, which could include:

- Loss of confidential employee and customer data
- Access to intellectual property and financial information
- Customer churn/loss of existing customers
- Interruption of operations
- Damage to critical infrastructure
- Stolen or damaged equipment

Ransomware Makes for Expensive Holidays

Ransomware, the most common form of cybercrime, is expensive. It encrypts files, locks out users, potentially corrupts data, and can cost companies millions in ransom payouts. Attacks have tripled since 2013 (Economist.com 6/19/2021).

Companies should be particularly vigilant during holidays, when IT staff is reduced, systems are more vulnerable, and protective responses delayed (Fortune.com 7/6/2021). The recent Kaseya hack occurred over the July 4th weekend, affecting nearly 1,500 businesses, and last year's SolarWinds hack occurred just before Christmas, attacking over 100 private companies, think tanks, and branches of the US military.

Employee Training and Cybersecurity Policy

An essential component of a good cybersecurity plan is an up-to-date, readily available cybersecurity policy. All employees, from entry level to the C-suite, should understand the policy and be trained to recognize and avoid security risks. Mitch Berger, Managing Partner of IMSA Search Global Partners USA and IMSA Board Member, relates, "Many of our clients in the C-suite and HR departments have told us that cybersecurity is now a prominent part of employee onboarding, with hands-on training about online information sharing, passwords and security questions, two-factor authentication for account access, and what to look for in emails and other communications which would signal a cyber threat."

Prevention is the Best Policy

The effects of any cyberattack can be catastrophic, resulting in business disruption, harm to company or brand image, customer loss, data theft, and in some rare cases, loss of life. The costs can be catastrophic as well. Experts recommend companies get ahead of the problem, addressing vulnerabilities before cyberattacks occur, by implementing the following preventive measures:

- Identify and assess risk areas across applications, devices, and people
- Implement the ability to automate responses to abnormal activity
- Adapt systems to remotely resolve issues
- Create policies and action plans for quick and effective response in the face of an attack
- Empower CISO's with appropriate budgetary and human resources to provide proper planning, training, and continual monitoring and upgrading of systems

In today's business environment, where online and digital are the way business gets done, cybersecurity is a top priority. And in the words of Benjamin Franklin, "An ounce of prevention is worth a pound of cure."