Cybersecurity in the Age of Digital Transformation

Forum and Panel Discussion Key Takeaways

Would your business still be able to open tomorrow if your network's security was breached today?

On November 21, 2019, Cowan Insurance Group—in partnership with eSentire—presented Cybersecurity in the Age of Digital Transformation, to explore this question. Moderated by Greg Vanier, Senior Vice President, Crisis and Reputation Risk, Edelman, the forum featured an expert panel discussion that helped attendees gain the latest insight into cybersecurity and learn how they could manage and mitigate risk to their business.

Addressing the current threat landscape and trends, the panellists provided their observations as seen through their lens of expertise on topics relating to cyber risk trends, strategies, as well as pre-breach and incident response planning.

After a wide ranging and informative discussion, we asked our experts to share their key takeaway points.

Imran Ahmad, LL.M. DESS LL.B.
Partner, Blake, Cassels & Graydon LLP

Five things your organization can do to improve its cybersecurity posture:

1. Build a data inventory; to start, ask yourself:

- What data is critical to our business?
- How is it kept?
- Where is it kept?

2. Have a practical Cyber Incident Response Plan ("CIRP")

3. Incorporate contractual language

4. Have a Data Retention Policy, and be sure to implement it

5. Conduct cyber due diligence on vendors

Mark Hubbard, B.Sc. CISO
Thinktum

There are three top things an organization should be thinking about as it relates to cyber:

1. Moving security discussions from the backroom to the boardroom

2. Shifting the security view from a technical requirement to a strategic priority

3. Incorporating security and privacy awareness as a part of your culture from the board through your levels of management and employees, extending awareness to their personal lives.

From there, the rest of the pieces fall into place. It's not easy, but the roadblocks begin to diminish with organizational commitment. To develop a holistic cybersecurity strategy from the ground up, break your approach down into small and manageable steps, recognizing your accomplishments and progress.

There are some critical actions you need to take to determine your exposure and focus areas:

- Develop awareness throughout the organization
- Perform a maturity assessment
- Review your environment, practices, and policies, and identify gaps
- Run a vulnerability scan; prioritize vulnerabilities and create a tactical plan for critical issues
- Make sure you have a complete asset inventory
- Review your backup plan, and develop an incident response plan and a business continuity plan

Remember: every step you take is an improvement on what you had before.

Eldon Sprickerhoff, CISSP CISA
Founder and Chief Innovation Officer, eSentire Inc.

Increased cybercrime and security gaps in cloud services and providers are two top concerns for cybersecurity experts today. With a large profit margin, and the ability to now purchase what formerly needed coding expertise to create, no one is immune to attacks. Criminals can send ransomware to any email address and receive a payout, or compromise legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Cloud service providers have introduced gaps to the business model of security by using a 'shared security' model. Before implementing a cloud service in your organization, do your due diligence to consider issues related to:

- Backups
- Retention
- Broad access
- Incident Response Handling
- Forensics
- Responsibility for data held within

Remember, backups are essential, but ensuring a high-fidelity restore process—within a timeline acceptable to the business function—is critical and needs to happen regularly.

David Black, BCom. CIP CCIC
Commercial Account Executive, Vice President, Commercial, Cowan Insurance Group

The global cyber insurance market is expected to triple to $17 billion by 2023. Today's insurance market is very competitive, with easy access and competitive pricing. Now is an excellent time to purchase cyber insurance; these market conditions aren't expected to last over the medium term.

- There has been a significant increase in extortion demand claims (ransomware)
- New segments, such as municipalities and not-for-profit, are being targeted by criminals

When securing insurance, look for a reliable provider network with a range of coverage offerings and claims adjustment; be wary of newcomers.

Best practices for managing cybersecurity risk include:

- Understanding your environment and inherent risks (i.e. selling products online poses more risk than selling through traditional distribution channels)
- Knowing the assets you are trying to protect and understanding that legacy systems are a potential attack vector
- Being cognizant of the data you are required to protect, why you have it, and what you are going to do with it
- Creating a risk plan and standard process that includes patch management process, intrusion detection, firewalls, and virus protection to protect assets
- Ensuring that insurance is part of your incident response plan in terms of reporting a loss and transferring risk
- Reviewing indemnity agreements with all IT vendors and cloud service providers
- Training employees to understand threats such as phishing and spear-phishing

Insurance without an incident response plan and best practices is not sustainable nor practical. Insurance programs are very affordable with broad coverage grants, allowing you to plan and budget for continuous improvement in your business.