Where's the Urgency in Your Cybersecurity Strategy?

Cybercrime is rising exponentially. And, taking a cold, hard, continual look at your organization's capabilities is becoming a mission-critical imperative.

When high-profile cyberattacks make headlines, like 2017's breach of the Maersk Group, which shut down Port of Tacoma terminals, Dr. Barbara Endicott-Popovsky, a University of Washington[1] cybersecurity expert, fires up a world map showing the frequency of cyber crime strikes. The graphics she draws from are based on daunting 2017 FBI statistics such as: 4,000 ransomware attacks daily; over 1,120 data breaches exposing 171 million records; and rising financial losses worldwide expected to top $6 trillion by 2021. [2]

"The days of fixing this with a firewall or IT patch are over. This is an arms race," says Endicott-Popovsky, executive director at the University's Center for Information Assurance and Cybersecurity (CIAC). "If you are not awake at night worrying about this, you should be."

Reports from the World Economic Forum[3] illustrate the magnitude of tackling cybercrime. Organizational vulnerability can arise from unintentional mistakes by employees, undetected pathways via networks, the cloud, applications, hardware processing chips, or software. But the battle between business and hackers is asymmetric. Whether the break-in occurs via phishing, ransomware, DDos-attacks, bots, malicious code, or encrypted viruses, these incidents are automated, AI-enabled threats operating 24/7 that only need to succeed once. Yet economic competition in new markets requires enterprises to share platforms and tools with partners, vendors, and customers in a hyperconnected, digital world.

Small companies are not immune. Last year, Congress reported 61 percent of small businesses were attacked online, requiring operations to shut down for three to 14 days to evaluate the damage to IT assets and infrastructure.[4] Analysts say organizations of all sizes must think beyond assets and databases to consider potential impacts such as:

- Manufacturing and other operational delays
- Potential threat to public health and safety
- Financial losses from paying ransom
- Stolen proprietary information
- Legal consequence, liability exposure

• Reputation or brand damage

Fighting Back Requires a Significant Shift
The best way to approach cybersecurity, say researchers, is for C-suite leaders to shift from a task-based approach to an ongoing, resilient stance. The entire corporate culture must be trained and prepared to detect, mitigate, respond, and recover from cybercrime. Being effective will require action that cut across department silos, involving employee awareness training, legal examination of vendors and third-party contracts, and compliance with fast-changing international rules on digital privacy and data breaches.

The *Harvard Business Review* taps the board of directors as leaders best positioned to integrate cybersecurity into every aspect of a firm's business strategy.[5] The CEO or department head may view additional security measures as added costs that slow growth and performance. But it is the board's role to advise their CEOs on risk and liability. "Companies routinely insure against black swan events such as fire, flood, earthquakes, and hurricanes," says CIAC's Endicott-Popovsky. "And cybercrime is rising at an exponential rate."

Staying Ahead Of The Risks
Not surprisingly, an astonishing 87 percent of board directors and C-level executives lack confidence in their company's cybersecurity posture.[6] One solution is for companies to hire Chief Information Security Officers and CERTs (computer emergency response teams). But few organizational leaders are briefed on these issues, or approach it from the board's perspective of tackling risk and liability. To best handle that, experts recommend boards obtain an objective, third-party assessment.

Just as financial oversight requires verified audits, security experts should undertake a specialized check-up called capability assessments. These comprehensive standards on IT governance, originally developed by the CMMI Institute, ISACA, ISO, and Carnegie Mellon University, have been adopted by the U.S. Department of Defense, federal contractors, Big Four auditors such as Gartner and Deloitte, and many others.

Today, any organization can obtain a capability assessment in light of:
• Regulatory requirements of business sector
• Technology usage
• Threat incident probability
• Ongoing mitigation plans
• Response protocols
• Employee documentation, awareness training, and practice drills for worst-case scenarios
• Loss tolerance (financial, operational, or reputational)

Taken as a whole, these benchmarks are ranked by low- to high-maturity, with five possible stages or ratings. These reports offer board members a roadmap, flagging a need for additional investment or confirming that operations are aligned with strategic objectives.

What's crucial is to get these metrics into the board's hands, pronto. "Everyone sees these executives testifying in Congress after being hit by a cyber event," says CIAC's Dr. Endicott-Popovsky. "No one wants the board that's asleep when the big hack finally hits."

##

Sources:

1) https://www.uwb.edu/ciac/community/faculty-and-staff/executive-director

2) Forrester Research, 2017
https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

3) World Economic Forum – Future of Digital Economy and Society System Initiative: Advancing Cyber Resilience - PDF

4) Testimony before Senate and House Committees
https://www.hsgac.senate.gov/hearings/cyber-threats-facing-america-an-overview-of-the-cybersecurity-threat-landscape
and
https://smallbusiness.house.gov/uploadedfiles/11-15-17_sage_testimony.pdf

5) CMMI Cybersecurity Capability Assessment Analysts Deck V6 – PowerPoint deck

Source in document: ISACA State of Cyber Security Report 2017 E&Y Report