LINKSQUARES

How to Avoid Cybersecurity Issues and Manage Risks

Speakers

Andy Lunsford

CEO, Co-Founder & GC
BreachRx

Robb McCune

VP, IT & Security
LinkSquares

Cybersecurity: the evolution.

The practice of protecting computer systems, networks, and data from theft, damage, disruption, and any unauthorized access.

- Key Components of Cybersecurity:
  - Information Security
  - Network Security
  - Application Security
  - Endpoint Security
  - Cloud Security
  - Physical Security
  - Identity Management
  - Disaster Recovery & Business Continuity
  - Educational Awareness

Cybersecurity risks your company is facing

- Phishing
- Misdirected Emails
- Corporate Account Takeover (CATO)
- Hybrid work environment/ cloud security
- Malware
- Ransomware
- Third-Party Risks
  Supply Chain

Cybersecurity Readiness

- Understand data value at stake.
- Assess your risk profile thoroughly.
- Benchmark against industry standards.
- Know local cybersecurity regulations.
- Review incident response processes.
- Identify cybersecurity leaders in team.
- Locate cybersecurity policy documents.
- Clarify insurance and reporting obligations.

Incident Response Program Maturity Model

Program Maturity	0 - Denial **No incident response plan**	1 - Reactive **Generic incident response template**	2 - Managed **Detailed incident response plans**	3 - Systematic **Routine updating and implementation of IR plans**	4 - Proactive **Dynamically updated IR Program**
Org. Maturity	No full-time privacy or security team	Dedicated team responsibilities	Detailed incident response team + duties	Detailed workflows + annual tabletop	IR team integrated + Regular exercises
Regulation & Contract Maturity	Little to no in-house knowledge of applicable privacy and cybersecurity regulations	Some tracking of regulations + obligations	Active tracking of regulations + obligations	Centralized management of global regulations + contracts	Proactive integration of regulations + contracts into incident response workflows
Tech. Maturity	No system in place	Manual processes + spreadsheets	Spreadsheets + basic ticketing system	Basic system + manual exercises	Automated processes + exercises

Teams to involve in the process

01 Information technology (IT)

02 Compliance

03 Legal - what is your role?

- Negotiating security terms in your contracts
- Responding to breaches
- Managing risk
- Knowing and complying with regulations
- Staying up to date on new rules, laws and regulations
- Creating a team of responders

Tabletop Exercise Prep

How to go about setting one up? How you get the most out of them?

- Single points of failure
    - Shrinking vendors for risk, but then fewer points of failure
    - Actually doing it, prove it, not just checking the box

1. **Identify:** Legal teams play an essential role in identifying the legal and regulatory requirements related to cybersecurity that the organization must comply with. They also help identify the potential legal risks associated with different types of data the organization handles.
2. **Protect:** The legal team can help devise policies and procedures to protect sensitive data, ensuring they are in line with relevant laws and regulations. They may also be involved in negotiating and reviewing contracts with third-party service providers to ensure appropriate cybersecurity measures are in place.
3. **Detect:** While the detection of cybersecurity incidents is typically a technical function, the legal team needs to understand the process to provide appropriate legal advice when an incident occurs.
4. **Respond:** When a cybersecurity incident occurs, the legal team becomes crucial. They will guide the response in terms of disclosure obligations, communication with affected parties, and managing legal implications.
5. **Recover:** Post-incident, the legal team can advise on the recovery process, including any legal requirements for notifying customers, regulators, or other stakeholders. They can also assist in implementing changes to policies and procedures to prevent future incidents.

What’s next?

Upcoming laws

Network & Information Security Directive (NIS2)

Digital Operational Resilience Act (DORA) - EU

EU AI Act

New York Department of Financial Services (NYDFS)

New State Privacy Laws - MD, MN, NJ, RI, KY, NE, NH

2025 Outlook

Cyber Incident Reporting for Critical Infrastructure (CIRCIA)

SEC Cybersecurity Rules Enforcement

State AI Laws (US)

Cyber Resiliency Focused Laws (US + Worldwide)

AI

Everything is unfolding as we speak

ISO 42001

EU AI Act

LINKSQUARES

Thank you!

More questions?

Please reach out to:
webinars@linksquares.com