May 9, 2025

CISO Liability and Personal Accountability Cybersecurity Failure

Jackie Cooney, Todd Renner, and Allison Raley
Arnall Golden Gregory LLP

Privacy+ Security Forum

Introduction – The New Era of Cyber Accountability

Privacy+ Security Forum

- Overview of the shifting cybersecurity governance landscape
- Increasing regulatory scrutiny on executive roles in cyber risk management
- Emergence of personal liability for CISOs and senior leadership
- Purpose: Understand regulatory trends, legal risks, and mitigation best practices

Key Drivers of Increased CISO Liability

- Surge in data breaches and ransomware incidents
- SEC and DOJ prioritization of individual accountability
- Expanding fiduciary expectations under governance standards
- Heightened expectations from public, investors, and boards

Privacy+ Security Forum

Regulatory Landscape: SEC, DOJ, and FTC Approach

Privacy+ Security Forum

- SEC (2023): Mandatory disclosures on cyber incidents and governance
- SEC Example: SolarWinds CISO charged for misleading disclosures
- DOJ: Emphasis on individual culpability in enforcement
- FTC: Views weak cybersecurity as unfair practice

Case Study: SEC v. SolarWinds and CISO Tim Brown

Privacy+ Security Forum

- Allegations: Fraud and internal control failures
- Key issue: Internal vs. public statements on risk posture
- Implication: Liability for disclosure gaps, not just breaches
- Lesson: Cyber governance is a material disclosure issue

Legal Theories of Liability

- Securities Fraud: Misstatements in SEC filings
- Negligence / Duty of Care: Failure to meet reasonable standard
- Breach of Fiduciary Duty: Especially for executive dual roles
- Criminal Liability: Willful concealment or obstruction

Privacy+ Security Forum

Executive and Organizational Risk Mitigation

- Governance Structure: Clear roles and escalation paths
- Board Reporting: Regular, documented updates
- Risk Assessments: Threat modeling and audits
- Insurance Review: D&O policies for cyber liability

Privacy+ Security Forum

Beyond the Point in Time

Privacy+ Security Forum

Timeline	Hidden Costs	Examples
Days, weeks, months	Employee Productivity losses	Can you measure payroll? Did you measure during the pandemic?
6 months - 1 year	Notification to Customers/Employees	Crisis Communication costs
Months	Helpdesk/Support/3rd Party	The calls do not slow down for a while
Periodic	Industry Certificaiton review and recertify	SOC2/HITRUST/CRA/etc…
Years	Consulting Charges (Investigaitons, Forensics)	3rd Party/Independent Review
Years	Loss to the Organization	Hard to measure (personnel, reputation, etc...)
Years	Costs of Recovery	Currently ~$4.5 Million
Years	Adminstrative Costs & Efforts	Legal, Re-Supply
Years	Material Determination and review	Legal and Regulatory connections
~10 years	Legal & Regulatory Proceedings	Years!! Experts, Litigation, Class, International
20 years	Legal & Regulatory Penalties	Years!! Monitorships, Chief Trust Officer
Indefinite	Insurance Costs	They will likely not go down
Indefinite	Remediation/CapEx/Restoration	Years of rebuilding
Immediate	Loss to Customers	Lack of trust, lost orders, website outage
Unknown	Loss of Future Business	Also hard to measure… how do you get your customers back? Suppliers? Vendors?
Unknown	Support to Law Enforcement	Who is allowed to speak to LE?
Unknown	Contractual Obligations and concerns	Will you be able to conduct work with critical partners? How long will you out of touch?

Preparing and Recovering from the Inevitable – Build Secure

Privacy+ Security Forum

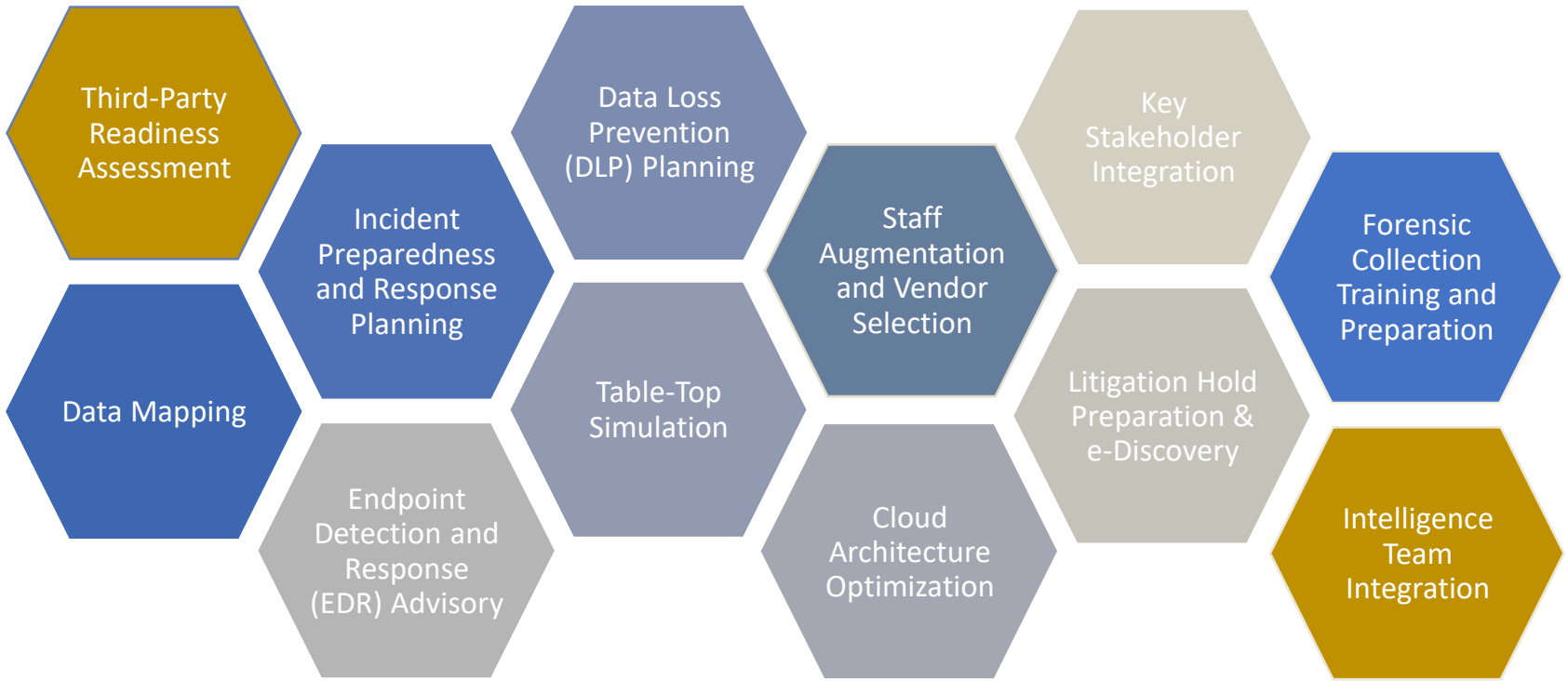
Counsel and Partners can help organizations define their cybersecurity strategy and build or enhance their cybersecurity and cyber risk management programs, giving clear visibility into both current and future operating states for key stakeholders and highlighting the risk-informed drivers for change.

Enhance Cybersecurity Defenses	The cyber threat landscape is constantly evolving, requiring a continuous process of review and improvement to ensure defenses are capable of efficiently responding to the most relevant threats.
Rebuild Reputation & Trust	Implementing comprehensive privacy and security measures showcases a strong commitment to protecting personal and sensitive data, which significantly impacts employees, customers, stakeholders, and regulators.
Increase Efficiency & Reduce Downtime	Designing organizational processes in alignment with cybersecurity frameworks eliminates the need to retroactively implement security measures and focus on growing your business. A strong cybersecurity program will reduce downtime, helping your organization recover faster and minimize financial losses.
Improve Cybersecurity Oversight	Regulators can view the board as directly responsible for the oversight of cybersecurity risk. Board members who understand the value of cybersecurity can ensure adequate measures are In place to mitigate cybersecurity risks.
Optimize Investments	According to IBM's Cost of Data Breach Report, about 50% of organizations increase security investments after a data breach. We work with clients to assess gaps and provide strategic roadmaps to maximize the return on investments.

Strategic Cybersecurity Transformation

Privacy+ Security Forum

Risk profiles for each organization are unique and can be addressed by a myriad of services and offerings. The steps below can help with your Executive and Organizational Risk Mitigation.



Transformation Planning → *Implementation*

Personal Risk Management for CISOs

- Document diligence in decisions
- Join internal disclosure committees
- Engage in incident response planning
- Consult legal counsel on cyber strategy
- Review indemnification and employment terms

Privacy+ Security Forum

Conclusion: Preparing for the Inevitable

Privacy+ Security Forum

- Cyber failures are inevitable, but liability can be managed
- CISOs must be legally fluent and board-ready
- Transparent governance reduces risk exposure
- Cyber risk = enterprise risk; accountability is the norm

Questions?

Thank you

www.agg.com

allison.raley@agg.com

jacqueline.cooney@agg.com

Todd.Renner@fticonsulting.com

Privacy+ Security Forum