NORTON ROSE FULBRIGHT

The Role of the GC: Managing Enterprise-Wide Cybersecurity Risk

July 27, 2022

Norton Rose Fulbright US LLP

Our Panel

Will Daugherty

Norton Rose Fulbright
Head of Cybersecurity – United States
Houston
+1 713 651 5684
will.daugherty@nortonrosefulbright.com

Neha Parekh

Procure Technologies
VP, Associate General Counsel,
Global Data Protection & Privacy

Grant Duffy

Southwest Airlines
Director – Privacy & Compliance

Is cybersecurity a risk that general counsels have a role in managing?

- **Survey says…..**
  - A 2022 ACC survey revealed that on a scale of 1-10, CLO's ranked Cybersecurity, on average, as the issue with highest level of importance to their business

Cybersecurity Incident Response

- Incident response was the typical area of cybersecurity that most Legal/Privacy team were initially involved, and for good reason
- For significant incidents, GC's are expanding their roles during incident response, recognizing the legal risks and multi-disciplinary approach required
- Incident preparation has become a large focus for GC's to manage cyber risk

Establish and update Enterprise and Info Sec Incident Response Plans	Develop Ransomware Incident Response Playbook / Decision Tree	Conduct tabletop exercises to build muscle memory and enhance the IRP	Drill and test other problem areas – recovery, asset identification, password resets, deployment of EDR	Legal integrated into SOC alerting processes/immediate engagement of counsel

Evolution of general counsel's role

Expanded from Cybersecurity Incident Response, to other domains, including:

- Cybersecurity Compliance
- Information Governance
- Privacy Compliance
- Board Oversight of Cybersecurity Risks
- Third-Party Risk Management / Customer Questionnaires

Cybersecurity compliance

Areas in-house counsel should be focused on, include:

- **Mapping the regulatory landscape** applicable to the organization
- Overseeing **Cybersecurity Risk Assessment** and **Penetration Tests**
- Reviewing and updating **Information Security Policies and Procedures**
- Conduct **regulatory readiness assessment** to better position the organization to quickly and comprehensively respond to requests by regulators in the first few days or weeks of an incident
- **Prepare for future regulatory rules** imposing short reporting requirements (e.g., proposed SEC Cyber rules for RIAs and Public Companies) and robust cybersecurity policies and procedures

But what are the practical challenges for managing cybersecurity compliance?

Also available as part of the eCourse
Hooked on CLE: December 2022

First appeared as part of the conference materials for the
2022 Essential Cybersecurity Law session
"The Role of the GC: Managing Enterprise-Wide Cybersecurity Risk"