Navigating the Labyrinth
A Guide to Cybersecurity Legal Risk for Executives and Directors
Beth Burgin Waller, Esq.
Chair, Cybersecurity & Data Privacy Practice
Understand the Lay of the Land

Step 1: Before a CISO can be expected engage the Board on cyber risk, he or she needs to understand the board room landscape.
Basic Board Duties

- Each director has a duty to act with the best interests of the corporation and the shareholders in executing their director role.

- This is called a “fiduciary duty.”

- Directors have a duty to inform themselves of “all material information reasonably available to them” prior to making a decision. This includes cyber risk.
The Board’s Basic Structure

- Often cybersecurity issues are first tackled in committee, with the audit committee often leading the charge on cybersecurity issues.

- Each committee reports to the Board.

- Board is ultimately responsible to the shareholders, employees, and public.
CISOs Belong at the Board Table

Step 2: A CISO’s concerns should not be delivered by anyone other than the CISO to the Board.
A CISO’s Own Fiduciary Duties

- A CISO – by title – is a Chief Information Security Officer.

- Officers, like Boards of Directors, have fiduciary duties to the Corporation.

- Those duties include the duty of good faith, duty of care, and duty of loyalty.
A Few Duties

- **Duty of good faith** → must act in the best interest of the company.

- **Duty of care** → must display care in performance of the work assigned to them. Not extraordinary care, but care that a person of ordinary prudence would take.

- **Duty of loyalty** → must make decisions without personal economic conflict.
The Dreaded Disclosures

Step 3: Publicly traded companies have a duty to disclose cyber risk under SEC guidance
In 2018, the U.S. Securities and Exchange Commission (SEC) came forward with “Interpretive Guidance” on timely disclosure of material cyber incidents and risks.

Disclosures become a delicate balance of cyber risk disclosure without laying out a roadmap of vulnerabilities.

Public filings need to include discussions of cyber risk and CISOs need to be involved in that drafting process.
Duties Hidden in Privacy Regulations

Step 4: Privacy laws are layering in security requirements
Hidden Dangers in Privacy Regs

- California Consumer Privacy Act (effective in 2020) has a hidden security provision:
  - The CCPA specifies that people can sue "as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."
  - E.U.’s General Data Protection Regulation
Invoke Attorney Client Privilege

Step 5: If you are about to say something extremely dangerous to the Company, call the lawyers in first.
Attorney Client Privilege

- CISOs should not be shy about asking to bring in-house counsel in on conversations about major cyber risks or incidents.

- Copy in-house counsel on communications and for major issues, bring in outside counsel, even into the Board room.

Invoke privilege by looping in lawyers before disclosing the risk.
Delivering the Bad News

Step 6: Be thoughtful about the language you use as it could be reflected in meeting minutes and come back to haunt you later.
Every communication without privilege invoked could be evidence in a later lawsuit.

4.2 Topic Area 1: Information Security Management and Culture Subtopic Area Results
For the Information Security Management and Culture Subtopic Area, there is a significant lack of policy and procedure. However, there is minor to moderate level of implementation and acceptance, with a minimal level of verification.
Exhibit A: Your Last Assessment

Step 7: Assessments, pen tests, and all the gnarly documentation you generate could become evidence.
Can be useful tools and dangerous litigation weapons.

### Assessments Will be Discovered and Analyzed

<table>
<thead>
<tr>
<th>Topic Area ID</th>
<th>Security Program Topic Areas</th>
<th>Policy</th>
<th>Procedures</th>
<th>Implemented</th>
<th>Tested</th>
<th>Integrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Security Management and Culture</td>
<td>1%</td>
<td>3%</td>
<td>29%</td>
<td>7%</td>
<td>29%</td>
</tr>
<tr>
<td>2</td>
<td>Information Security Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Security Awareness, Training, and Education</td>
<td>4%</td>
<td>2%</td>
<td>27%</td>
<td>2%</td>
<td>25%</td>
</tr>
<tr>
<td>4</td>
<td>Budget and Resources</td>
<td>2%</td>
<td>13%</td>
<td></td>
<td></td>
<td>13%</td>
</tr>
<tr>
<td>5</td>
<td>Life Cycle Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Incident and Emergency Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Security Controls</td>
<td>8%</td>
<td>8%</td>
<td>64%</td>
<td>16%</td>
<td>64%</td>
</tr>
</tbody>
</table>
The Types of Claims You Face: Breach of Contract

Step 7: Understand the Risk of Signing Agreements with Customers or Vendors.
A few sources of a potential breach of contract claim:

- Master Services Agreements
- Nondisclosure Agreements (did you violate the requirement to keep client/customer data confidential in the event of a breach?)
- Information Security Agreements
- Data Protection Addendums
- User Agreements
- Even privacy policies with public/customers

Every agreement you sign could be utilized later.

Incredibly important to negotiate and limit risk, especially through ISA.
“Appropriate physical, technical and organizational security measures as are appropriate to the risks…” After a breach, will you be said to meet this standard?

Are you prepared to give over your security audit documents to your Customer?

Do you have cyber insurance in place to protect against the claim?

Every agreement you sign with a representation or warranty related to security could be used as a basis for a later lawsuit in the event of an incident or breach.
The Types of Claims You Face: Negligence

Step 8: Understand the “duty of care.”
Negligence is the failure to exercise reasonable care which results in an injury or damage to another.

In the cybersecurity context, negligence is a constantly evolving concept.

What is reasonable care?
California Consumer Privacy Act, going into effect in 2020 is not helpful on this topic for security professionals as we’ve discussed.

California staking out statutorily “the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.”

Increasingly, duties will be codified.
The Types of Claims You Face: Fraud

Step 9: Misstatements in the security context.
- Fraud is not just a single term under the law.
  - Constructive fraud
  - Fraud in the inducement
  - Material Fraud

In the security context, every statement you make about your security measures could be utilized later in a fraud action.
Understand the Harm

Step 10: The relief that can be sought can be more than a few dollars.
Compensatory damages vs. special damages.

Understand the damages you exclude in a contract with a customer or a vendor.

Limitation of liability terms (coupled with the representations and warranties you make or they make) are the most important terms in any contract.

- Watch out for “fees paid” provisions and exclusions for “loss of data.”
Beth Burgin Waller
Chair of the Cybersecurity & Data Privacy Practice

bwaller@woodsrogers.com
Direct: (804) 343-5039