Talking Cybersecurity to the Board

https://sans.org/security-awareness
Why Do I Care?

- The success of your program depends on leadership support. That support starts at the top.
- Board members are asking a lot of questions about cybersecurity and don’t like or don’t understand the answers.
- This == opportunity
The Board
What is a Board?

• Elected members responsible for overseeing the management of the corporation.
• Monitor the health, welfare and future of the organization. They are strategic.

*Noses In, Fingers Out*
Who is a Board Member

• Very smart, experts in their field.
• Experience founding / running large or similar organizations.
• Strong credentials and trust.
• Extremely busy, on multiple boards / committees.
They Are

- Business strategy and results oriented
- People and data focused
- Business, not technology oriented
- P&L obsessed for publicly traded companies
- Do not think in terms of quarters but years

Their native language is business!
They Are Not

• ATM Machines
• Human Resources
• Court of Appeals
• Cybersecurity / technology experts

*Their native language is not Cybersecurity*
They Know Risk, but not Cyber Risk

Vulnerabilities x Threats x Impact
“Security people don’t speak our language. In fact, at each briefing they seem to speak a different language.”

“The CISO is great at talking about ‘blood in the streets’ but very weak on strategy to avoid disasters.”

“We know bad things will happen – the CEO and CFO and VPs inform us of business problems frequently. **We want to have confidence that basic competence and strategies are in place to reduce bottom line impact.**”

“A big part of **being believable and building our trust** is showing us how we compare to competitors, other industries, some kind of standards or benchmarks.”
Speaking to the Board
Speaking to the Board
Know Your Board

• Identify who is on your board
• Research them on LinkedIn
• Talk to a Board Member or senior exec ahead of time to better understand what you are in for.
Do Your Homework

• First impressions last a long time, they remember.
• Research every board member on LinkedIn.
• Talk to a Board member or senior executive before the briefing
When Speaking – Two Things

• Are you presenting information?

OR

• Are you asking someone to make a decision?
What to Say

• Coach them on the basics. They are very smart, just do not understand your world.

• Focus on big picture. Think business benefits, not security features (you do know your mission statement, right?).

• Use maturity models / frameworks. How do you compare to others?
# Benchmarking Models / Frameworks

## Basic CIS Controls

<table>
<thead>
<tr>
<th></th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inventory and Control of Hardware Assets</td>
</tr>
<tr>
<td>2</td>
<td>Inventory and Control of Software Assets</td>
</tr>
<tr>
<td>3</td>
<td>Continuous Vulnerability Management</td>
</tr>
<tr>
<td>4</td>
<td>Controlled Use of Administrative Privileges</td>
</tr>
<tr>
<td>5</td>
<td>Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
</tr>
<tr>
<td>6</td>
<td>Maintenance, Monitoring and Analysis of Audit Logs</td>
</tr>
</tbody>
</table>

## Foundational CIS Controls

<table>
<thead>
<tr>
<th></th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Email and Web Browser Protections</td>
</tr>
<tr>
<td>8</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>9</td>
<td>Limitation and Control of Network Ports, Protocols, and Services</td>
</tr>
<tr>
<td>10</td>
<td>Data Recovery Capabilities</td>
</tr>
<tr>
<td>11</td>
<td>Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches</td>
</tr>
<tr>
<td>12</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>13</td>
<td>Data Protection</td>
</tr>
<tr>
<td>14</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>15</td>
<td>Wireless Access Control</td>
</tr>
<tr>
<td>16</td>
<td>Account Monitoring and Control</td>
</tr>
</tbody>
</table>

## Organizational CIS Controls

<table>
<thead>
<tr>
<th></th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Implement a Security Awareness and Training Program</td>
</tr>
<tr>
<td>18</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>19</td>
<td>Incident Response and Management</td>
</tr>
<tr>
<td>20</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>
Strategic Metrics

Find metrics that tie into your mission

• Time to detect / recover from an incident
• Cost reduction in number / type of incidents
• Compliance
• Safety
• Uptime / Availability
• Reputation
What Not to Ask / Say

• Do NOT surprise the Board
• Do not talk about specific technology, types of attacks or use acronyms.
• Do not ask for budget / people, that is what your boss is for.
What Will Board Ask?

• Insurance and risk transfer
• Where does our risk appetite collide with current and anticipated regulations?
• How do we compare to others?
• What gains in efficiency have been made?
• What are the succession plans for key cybersecurity talent?
• What is the cyber risk impact of strategic decision X that is being considered?
End Goal

• The Board feels confident you know what you are doing and the organization is in good hands.
• Board members will internalize key security strategic issues as they oversee other corporate operations/decisions.
• Relevant board member(s) will reach out to you.
When you get back to work

• Identify a champion on Board you can go to for advice.
• Research every Board member.
• Identify a way to benchmark your program (Critical Controls, maturity models, NIST Framework)
Resources

- **SANS What Works**: [https://www.sans.org/critical-security-controls/case-studies](https://www.sans.org/critical-security-controls/case-studies)
- **National Association of Corporate Directors**: [https://www.nacdonline.org/](https://www.nacdonline.org/)
lspitzner@sans.org