DEAR 2020 CISO: ARE YOU READY?
LET’S BUILD A TWO-YEAR PLAN

Todd Fitzgerald,
CISSP,CISM,CISA,CGEIT,CRISC,PMP,ISO27000,CIPP/US,CIPP/E,CIPP/C,CIPM,ITITv3f
Managing Director/CISO
CISO Spotlight, LLC
@securityfitz
tfitzgerald@cisospotlight.com Linkedin.com/in/toddfitzgerald
Today’s Agenda

- Introduction
- The “Security Leader” Proposition - YOU
- The Information Security Vision
- Mining Jewels
- Mapping our way to protection
- Developing the plan
- Presenting to the Board
- Wrap-up
Step 1. Why Did they Hire You?

Why were you hired? Are you the first CISO? 2nd? 3rd? Was there an issue they needed to solve? What was it? Did you have a particular skill? Why did YOU take this job?
Step 2. Time to Build A Security Vision...
Reflects the organization’s core values
Supports the mission of the organization
Gets people excited about supporting the vision
Step 3. What are your crown jewels?
Process to Create Mind Map

1. Create the central idea “Data Protection” in the Center of the page
2. Add Branches to Map... Add more branches
3. Add keywords
4. Include Images if you like
5. Use curved lines
6. One keyword per line

Source: Adapted from Tony Buzan, mind map inventor
Mind Map Example

Source: Mindwerx.com
### Step 5. Planning the next 2 years+ 5

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>12 Mo</th>
<th>24 Mo</th>
<th>3-5 Year</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management Strategy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Risk Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td>Identity Management and Access Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness &amp; Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Protection Processes/Proc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protective Technology, Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Continuous Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection Processes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improvements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improvements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** M=Maturity Level Using the NIST Cybersecurity Framework

**Could Use Colors (H,M,L) or**

0=Nonexistent No Evident of practice or standard
1= Initial Ad-hoc or inconsistent
2=Repeatable consistent overall approach, but mostly undocumented
3=Defined documented approach, lacks enforcement or measurement
4=Managed regularly measures compliance and makes process improvements
5=Optimized refined compliance to best practice
Step 6. It is time to present to the board....help!!!
“Advice” for Presenting to the Board

1. Use Analogies to explain complicated concepts
2. Understand the business goal-why is the CISO in the room?
3. Are we secure? Peers-Trends-Gaps-how to fill
4. Enterprise-wide risk management
5. How are you managing risk? Framework?
6. How is risk being mitigated, avoided, accepted, transferred?
7. Risk posture most important to the board, not so much to the CISO
8. Compliance maturity, incidents are important to CISO and Board
9. Must be ‘business relevant’, talk about ‘who would target us and why’, avoid security jargon
10. Credibility-share good news and bad and what you don’t know
11. Share a story, don’t drown them in metrics, talk in $$$ where possible (have available if asked)
12. Compare with peers, industry, maturity status, risks
13. Share incidents
14. Talk $$$ - budgets, cost of downtime
15. Efficiency – managing costs down
16. Effectiveness – oriented towards new business ops, new trends, threats, technology
17. Determine how security is viewed by the rest of the organization, be relentless in demonstrating business value
18. Engagement starts below the board level and works up one level at a time
19. Need to validate risks before taking to the board
20. Establish and communicate 3 lines of defenses (control oversight, assurance, audit)
21. Position board with their responsibility
22. Communicates clear organizational governance

Source: 2017 COSAC Conference Presentation, Naas, Ireland, “Are We Boring the Board”
Todd Fitzgerald research
23. Communicate trends – invite regulators, government bodies, peers to present at add credibility

24. Communicate plan progress with a simple framework, deviation from industry standards

25. Explain the ‘ideal’ maturity level – risk appetite= difference from perfection and reality

26. What are the top 5 risks related to cybersecurity?

27. What are the actions in place to address these risks?

28. Are internal and external threats being examined?

29. Is the risk assessment holistic? Does it include vendors, suppliers – if not, could be ‘willful neglect’

30. Carve program into security processes vs technology – such as threat management, incident response, vulnerability and patch management, security operations, security architecture, and risk management

31. Discuss how we would respond to an incident to educate the board that anyone could be vulnerable

32. 49% reporting on vulnerabilities to board, followed by 25% on incident response

33. Many CISOs grasp for topics to connect with the boards!!!

34. Do we think the board cares about lost laptops and website blocking?

35. Transparency on security risks new innovations carry

36. Prioritize assets, create common risk appetite with the board to fuel business growth and innovation

37. Implement security reporting discipline and engagement between CISO and board

38. Crowded board agenda, invisible payoff vs shareholder deliverables

39. “Not our problem” outside of military and financial services

Source: 2017 COSAC Conference Presentation, Naas, Ireland, “Are We Boring the Board”
Todd Fitzgerald research
As if that wasn’t enough….

40. Overinvested in wrong priorities (preventative controls vs detect/response)
41. Risk Posture – Not tactics, security architecture, operational issues
42. Be ready for questions – board expects you as the expert to know the answers
43. Listen to their reactions- highlight next time

Source: 2017 COSAC Conference Presentation, Naas, Ireland, “Are We Boring the Board” Todd Fitzgerald research
Resources to Further Information Security Program (Available in RSA Book Store)

Steps To Build An Information Security Program

CISO Leadership Skills To Lead Program – Insight by Industry Experts & Pioneers

2 Books Available To BUILD and LEAD your Information Security Program

SIGNING IN RSA BOOKSTORE
Apply What You Have Learned Today

- Next week you should:
  - Identify your key stakeholders and participants to build the 2-year strategy

- In the first three months following this presentation you should:
  - Prepare a security vision statement with the stakeholders
  - Research threat environment/breaches specific to your industry
  - Identify the “crown jewels” and create current as-is “protection mind-maps”

- Within six months you should:
  - Develop future protection mind-maps
  - Drive an implementation project to create 18 month-2 year plan to address gaps
Thank You Very Much For Your Participation!

Todd Fitzgerald, CISSP, CISM, CISA, CGEIT, CRISC CIPP/US/E/C, CIPM, PMP, ISO27001, ITILv3f
Managing Director/CISO
CISO Spotlight, LLC
Deerfield, IL
Linkedin.com/in/toddfitzgerald
tfitzgerald@cisospotlight.com