RSA Conference 2016

Learning Labs

Developing a Cyber Strategy:

Prepare your company before Zero Day strikes

Post-Conference Summary

Facilitator:

Brandon Neff

President, Innové Strategy

210-464-5709

brandon.neff@innove.com

www.innove.com

Learning Lab Summary

The Learning Lab applied a corporate version of military intelligence planning models used to help corporate officers improve preparation and resiliency before and after a cyber security incident. In this session, members worked in teams to apply the cyber preparedness and resiliency framework to create a Cyber Security Strategy focused on preparation and pre-coordination (vs. response). Notional case studies explored during the session included retail, banking, cloud services, and oil and gas.

Learning Lab Objectives

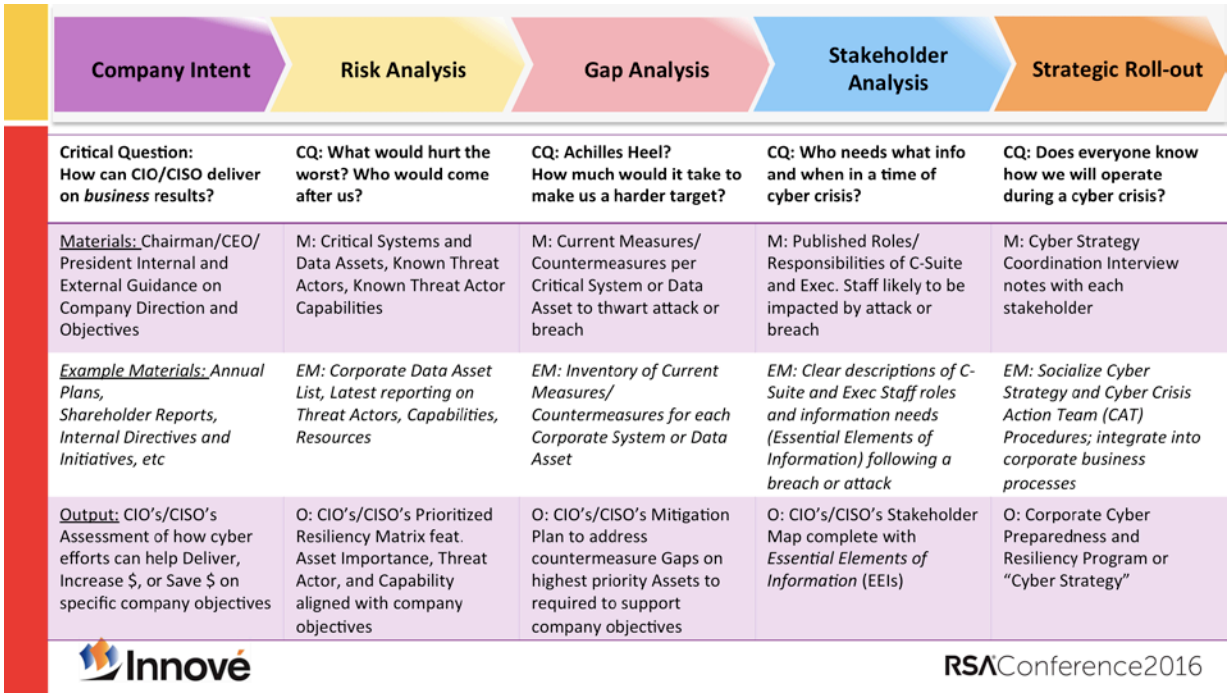
- **Introduce participants to the cyber preparedness and resiliency framework and use two well known military operations to demonstrate its usefulness**

- **Participants gain new perspective on their day-to-day activities to improve their organization's cyber preparedness and resiliency by considering how their cyber programs align with and support core business objectives**

- **Participants gain better understanding of specific phases of (and associated materials required to develop) a cyber preparedness and resiliency program**

- **Participants have the experience (Learning Lab) and the supporting framework to develop and implement a cyber preparedness and resiliency program in their respective organizations**

Cyber Resiliency and Preparedness Insights



Company Intent	Risk Analysis	Gap Analysis	Stakeholder Analysis	Strategic Roll-out
Critical Question: How can CIO/CISO deliver on *business* results?	**CQ: What would hurt the worst? Who would come after us?**	**CQ: Achilles Heel? How much would it take to make us a harder target?**	**CQ: Who needs what info and when in a time of cyber crisis?**	**CQ: Does everyone know how we will operate during a cyber crisis?**
Materials: Chairman/CEO/ President Internal and External Guidance on Company Direction and Objectives	M: Critical Systems and Data Assets, Known Threat Actors, Known Threat Actor Capabilities	M: Current Measures/ Countermeasures per Critical System or Data Asset to thwart attack or breach	M: Published Roles/ Responsibilities of C-Suite and Exec. Staff likely to be impacted by attack or breach	M: Cyber Strategy Coordination Interview notes with each stakeholder
Example Materials: Annual Plans, Shareholder Reports, Internal Directives and Initiatives, etc	*EM: Corporate Data Asset List, Latest reporting on Threat Actors, Capabilities, Resources*	*EM: Inventory of Current Measures/ Countermeasures for each Corporate System or Data Asset*	*EM: Clear descriptions of C-Suite and Exec Staff roles and information needs (Essential Elements of Information) following a breach or attack*	*EM: Socialize Cyber Strategy and Cyber Crisis Action Team (CAT) Procedures; integrate into corporate business processes*
Output: CIO's/CISO's Assessment of how cyber efforts can help Deliver, Increase $, or Save $ on specific company objectives	O: CIO's/CISO's Prioritized Resiliency Matrix feat. Asset Importance, Threat Actor, and Capability aligned with company objectives	O: CIO's/CISO's Mitigation Plan to address countermeasure Gaps on highest priority Assets to required to support company objectives	O: CIO's/CISO's Stakeholder Map complete with *Essential Elements of Information* (EEIs)	O: Corporate Cyber Preparedness and Resiliency Program or "Cyber Strategy"

- **"Cyber…it's not just for IT anymore": Participants noted that cyber security is being seen as more of a "business risk" versus as an IT security challenge**

- **"We can't 'boil the ocean'…optimizing cyber spending is important": Prioritizing cyber security and risk mitigation measures for those Critical Systems and Data Assets (CSDAs) required for core business needs and objectives**

- **"Everybody loves cyber": Participants acknowledged growing interest in cyber security activities among C-suite colleagues and within corporate boards, but noted difficulty in effectively communicating across senior leadership teams**

- **"What do we mean when we say 'cyber'?": Participants noted that raising "cyber fluency" among C-suite colleagues and their boards is growing in importance**

- **"Looking outside the foxhole": Cyber security is becoming more "anticipatory" with a focus on better understanding of "threat actors", their specific intent, and their relative capabilities against our Critical Systems and Data Assets**

- **"Cyber preparation and response is a team sport": Corporations (through various C-suite functions) respond to cyber incidents, not just IT professionals…they need to be prepared to be effective in their response**

- **"Preparation is the Key to Resiliency". The best time to prepare is now, but knowing how to prepare is essential. There are five phases required to ensure proper due diligence, achieve better preparation, and thus, better resiliency following any future cyber security incident**