VIEW FROM THE CISO - DEMONSTRATING WINS

Michael Doucet
Executive Director, Office of the CISO
Michael.doucet@Optiv.com
(613)899-7169
Agenda

❖ Complexity in our Environment
❖ Changing Perspective
❖ Cyber Program Goals
❖ Six Forces of Security Strategy Influencers
❖ Security Domains
❖ Optimized Security Program
❖ Wrap up
COMPLEXITY

Billions of Threats and Vulnerabilities

SECURITY PROGRAM

• Business aligned
• Right sized for the organization
• Prioritized
• Never completed

100’s of Regulations and Standards

2,500+ Security Technology Vendors
"As a CISO, you have a choice: either become the strategy guy, or the scapegoat.”

"This year, more than ever, I need to step back, take inventory and rationalize what we have, what’s working and what’s not. I need to focus on optimizing our current environment.”

My CFO continues to ask me to show them the measures and metrics proving we are safe with the investments we have made. The vendors won’t do this.

I’m criticized by execs as the guy who always says “no.” How do I become the guy who says “yes”?

My CapEx costs are too high, due to investments in products that are ineffective or never deployed.

25 – 30% of everything I have bought has not yet been deployed. Do I even need it? The Vendor pitch on the problem and the solution seemed to make sense?

There are too many opinions, too much information, too many experts and too little time. Everyone keeps telling me how many "things" they have – researchers, endpoints, found attacks. But none of that helps me with my problem.

“I have 17 Security agents deployed on our Desktop. I know I don’t need all of these, but who do I trust to guide to which are needed and which are redundant?”

The THE CISO CONCERNS

Proprietary and Confidential. Do Not Distribute. © 2018 Optiv Inc. All Rights Reserved.
THE CISO CHALLENGES

Back to Basics  Inventory  Rationalize  Optimize  Demonstrate
The perimeter no longer exists

Security purview must widen to meet the challenge

The path forward is unique for every business

Frameworks and blueprints can be used but must be tailored

There is an embarrassment of riches in technology

Technology must be mindfully selected and integrated for a proven purpose
Align Security Initiatives with Your Business Goals

Determine specific threats against your organization. Identify requirements to elevate your defense and response

Map Controls in Place to Protect Your Business

Build a Business Aligned Security Program
Business Model of Information Security

Security Program
  Strategy & Oversight
  CULTURE
  GOVERNANCE
  ARCHITECTURE
  COMPLIANCE
  ENABLING & SUPPORT
  EMERGENCE
  CONSUMERIZATION

PEOPLE
  Knowledge & Behavior

PROCESS
  Operations & Orchestration

TECHNOLOGY
  Architecture & Implementation
Six Forces of Security: Security Influencers

- IT Organization, Systems and Infrastructure
- Business Strategy
- Organizational Culture
- Government and Industry Regulations
- Global Social and Political Forces
- Adversaries and Threats
<table>
<thead>
<tr>
<th>Security Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Management and Transformation</strong></td>
</tr>
<tr>
<td>Privacy and Governance</td>
</tr>
<tr>
<td>Cyber Resilience</td>
</tr>
<tr>
<td>Risk Optimization</td>
</tr>
<tr>
<td>Cyber Assurance</td>
</tr>
<tr>
<td><strong>Cyber Operations</strong></td>
</tr>
<tr>
<td>Intelligence Operations</td>
</tr>
<tr>
<td>Cyber-as-a-Service</td>
</tr>
<tr>
<td>Advanced Fusion Center Operations (MDR)</td>
</tr>
<tr>
<td>Managed Security Services (MSS)</td>
</tr>
<tr>
<td>Cyber Authorized Support Services</td>
</tr>
<tr>
<td><strong>Cyber Digital Transformation</strong></td>
</tr>
<tr>
<td>Cloud Security</td>
</tr>
<tr>
<td>Product Security</td>
</tr>
<tr>
<td>Analytics/Big Data</td>
</tr>
<tr>
<td>Orchestration and Automation</td>
</tr>
<tr>
<td><strong>Identity and Data Management</strong></td>
</tr>
<tr>
<td>Identity Governance</td>
</tr>
<tr>
<td>Access Management</td>
</tr>
<tr>
<td>Data Governance and Protection</td>
</tr>
<tr>
<td><strong>Threat Management</strong></td>
</tr>
<tr>
<td>Secure Infrastructure</td>
</tr>
<tr>
<td>Adversarial Emulation (Exposure Mgmt)</td>
</tr>
<tr>
<td>Threat Detection and Response</td>
</tr>
<tr>
<td><strong>Integration and Innovation</strong></td>
</tr>
<tr>
<td>Applied Research</td>
</tr>
<tr>
<td>Design Innovation Services</td>
</tr>
<tr>
<td>Integration Services</td>
</tr>
</tbody>
</table>
The security program is aligned with the business.

The security program made progress over time in its risk mitigation goals and strategy.

WHAT DOES IT MEAN TO BE “OPTIMIZED”?

The members of the security team believed they were valuable to the organization and had an impact.

The executives of the organization saw value in the security program.

Board of Director and executive leadership interaction with the security leader.

Technology was one part of many components of the security program.
Single, Identifiable, Executive Sponsor or Advocate

Develop a Risk Steering Committee

Leverage a Control Framework

Targeted High Maturity in Some Controls

Thoughtful Deployment of Technology

Work with Great People
THIS IS A JOURNEY

- Business Aligned
- Risk Based
- Data Centric
- Threat Based
- Compliance Based
- Infrastructure Based
WITH THE RIGHT BUILDING BLOCKS

The day-to-day of the security technologies deployed to accomplish the security strategy

protected by the business from threats

security controls designed to accomplish the security strategy

what industry, and how it operates

employed by the business to accomplish its goals
The Security Journey

**Business Aligned Strategy**: Create a security program that enables your organization by understanding the business objectives, compliance objectives, threats and material risks.
In Conclusion...how good are we?

❖ Complexity in our Environment
❖ Changing Perspective
❖ Cyber Program Goals
❖ Six Forces of Security Strategy Influencers
❖ Security Domains
❖ Optimized Security Program
❖ Wrap up
VIEW FROM THE CISO - DEMONSTRATING WINS

Michael Doucet
Executive Director, Office of the CISO
Michael.doucet@Optiv.com
CHANGING PERSPECTIVE

OUTCOME TARGETED

“Inside-Out”

The path forward is unique for every business

There is an embarrassment of riches in technology

Security purview must widen to meet business needs and outcomes

Frameworks and blueprints can be used but must be tailored

Technology must be mindfully selected and integrated for a proven purpose