Building your Resilient Cyber Strategy

In the cybersecurity world, winging it is never a strategy that leads to success. Factors including a constantly changing perimeter, technological innovation, fluctuating compliance requirements and the challenges of securing a remote workforce have cemented the fact that those who have a plan win. Optiv’s Cyber Strategy and Roadmap offering enables the definition and development of a holistic cyber strategy that aligns with your overall business objectives. Our industry-tested approach includes understanding your business and threat profile, which coupled with our strategic visioning workshops helps determine your cyber north star and build out of a robust cyber strategy and actionable roadmap.

Optiv Solutions

Our Cyber Strategy and Roadmap offering delivers a customized methodology and approach taking into consideration your organization’s priority objectives. By completing the following three phases, we’ll know what you need and the efficient way to protect what matters.

Phase One
Business Profiling
- Determine key risks and threats through a business, industry and competitor lens
- Identify risk appetite levels for organization based on executive stakeholder inputs
- Determine current technology environment
- Understand the compliance landscape applicable for the organization

Phase Two
North Star Definition
- Conduct visioning workshops with executive stakeholders to understand desired target state of the cyber program
- Understand hopes, fears and legacy that drives the vision and mission of the cyber function
- Compare with industry peers to get perspective on typical security capabilities, IT and security headcount, budget, etc.

Phase Three
Strategy and Roadmap
- Define a cyber strategy that aligns with business priorities as well as the defined vision and mission for the cyber program
- Develop an actionable three-to-five year roadmap that enables the organization to progress towards their desired target state
A Builder's Guide

Use Optiv’s Cyber Strategy Framework as a guide to identify cyber requirements across each security capability that need to be addressed as part of the cyber risk management process.

### Cyber Strategy Framework

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Governance</th>
<th>Cyber Risk Management</th>
<th>Compliance &amp; Assurance</th>
<th>Awareness &amp; Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST Cybersecurity Framework</td>
<td>Defense</td>
<td>Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO/IEC 27001</td>
<td>• Identity &amp; Access Management</td>
<td>• Threat &amp; Vulnerability Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FedRAMP</td>
<td>• Application Security</td>
<td>• Brand Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td>• Third Party Risk Management</td>
<td>• Security Event Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI DSS</td>
<td>• Privacy &amp; Data Protection</td>
<td>• Cyber Analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Infrastructure Security</td>
<td>• Security Operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cloud Security</td>
<td>• People and Workplace Monitoring</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Case Study

**Customer Profile**

Fortune 100 technology manufacturer

**Desired Outcomes**

Complete a holistic strategic maturity assessment of the company’s central security offices across cybersecurity, investigations, physical security, supply chain security, product security and enterprise resilience, and provide investment options to mature individual programs.

**Client Benefits**

- Developed individual security frameworks to assess and manage the various central security offices.
- Provided current state maturity and potential target state maturity of each security domain.
- Offered a roadmap with a set of investment options to each security office, along with high level recommendations the security offices could choose from to improve their maturity.

**Solution**

By leveraging industry standards and leading practices, Optiv developed customized frameworks for individual security programs to determine the state of each security domain. We conducted risk appetite reviews, threat assessments and maturity assessments for each security program against its developed standards and a budget analysis for the security offices.

#### Why Clients Choose Optiv

**Expert Minds**

Optiv’s security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

**Leading Practices**

Our knowledge of industry leading practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

**Client-First Culture**

Optiv’s passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

**Proven Methodologies**

Optiv has developed proven methodologies and accelerators to help ensure superior outcomes for your projects and programs.

### A Builder's Guide

Secure greatness™

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2022 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.