



A Security Roadmap helps those in healthcare industries do what they need to do – use and share health information effectively and securely.

The Cisco SSR Provides an Effective Security and Compliance Roadmap for Healthcare:

- Providers
- Payers
- Pharma / Bio Engineering
- Business Associates

BUSINESS OBJECTIVES:

- Provide accurate understanding of cybersecurity risk
- Provide visibility into true regulatory compliance posture
- Provide Due Diligence prior to deployment of new technologies or M&A activities
- Enable use of new technologies that are dependent upon reliable, safe and secure computing platforms
- Facilitate improved patient and provider secure access to data
- Provide improved confidence in health information integrity, leading to enhanced treatment outcomes
- Help business associates that store, transmit or process health information demonstrate their commitment to protecting sensitive data and compete more effectively for business

Cisco Strategic Security Roadmap

Planning for Healthcare Security, Privacy and Compliance

With attacks against healthcare on the rise, the need for payers, providers, pharmaceuticals, and their business associates to prevent breaches of PHI is now critical.

The ability to safely and securely collect, store, analyze and transmit PHI helps companies reduce risks, regulatory liability and delivery costs, while at the same time instills confidence and increased willingness in the patient to actively participate in their treatment.

However, before an organization can deliver on these promises, it must discover its own information security strengths and weaknesses, identify critical business drivers and security needs, and develop and implement a roadmap for achieving success. That's where Cisco's Strategic Security Roadmap (SSR) can help.

STRATEGIC SECURITY ROADMAP

Cisco combines a world-class approach with experienced senior security experts who know how to get things done in healthcare. These vendor-agnostic seasoned professionals will help you develop and promote to the Executive Team and Board, a strategic plan for securing the organization over the next 1, 3, & 5 years.

With a global threat view provided by Cisco Talos® and industry leading practices from the tens of thousands of Cisco Healthcare Life Sciences customers, what third party security risk assessment can claim to have visibility into what your peers are doing; then to be able to leverage their lessons learned, in order to help you develop your strategic plan?

The SSR methodology is designed to comprehensively review the security posture of an organization in line with the domains of the ISO 27002 framework. It assesses capabilities against the technical controls of NIST and regulatory requirements of HIPAA, HITECH, FTC Red Flags, local State Privacy Laws, and internal corporate policies and standards.

Current capabilities are mapped by ISO domain against the CMMi maturity model to identify strengths and weaknesses. A **Future State** security model is developed based upon business imperatives, appetite for risk, and remediation of identified weaknesses. A **Roadmap and Strategic Security Plan** is developed based upon prioritization of key initiatives and an organization's willingness and appetite for change. The plan is then presented with you to the Executive Committee and the Board, to solicit active support, and if needed, additional funding for the plan to meet or accelerate its objectives.

ADDITIONAL SERVICES:

The Strategic Security Assessment is just the first step in evaluating the current and desired future state of a healthcare entity. Other complimentary services may include:

- HHS OCR Audit Readiness
- HITRUST CSF Assessment
- ISO 27001 Certification Readiness
- Security Compliance Assessments for HIPAA/HITECH, FDA, FDC Red Flags
- Privacy Compliance Assessments for EPD, Caldecott, Australian & Singapore Privacy
- PCI DSS Compliance Assessment, Attestation and Scanning (QSA / ASV)
- Security Vulnerability Assessment and Penetration Testing – external, internal, application, wireless, configuration, etc.
- Industrial Controls Assessment for pharmaceutical drug manufacture, ISO, FDA, etc.

CISCO SECURITY

We provide enterprise-class cybersecurity services which have evolved from years of experience in the world's most sophisticated and challenging environments. Our broad capabilities address the entire life cycle of an organization's security needs. We consult to help leaders optimize their resources by clarifying and prioritizing needs. Our integration services ensure the most effective application of the appropriate technology and our managed security services deliver significant gains in operational efficiency and effectiveness. What we do allows clients to focus on their core business objectives – with confidence.

For more information visit Cisco Security:
<http://www.cisco.com/security/>

THE 6-12 WEEK ROADMAP PROCESS

Depending upon the size and complexity of your organization, the Strategic Security Roadmap process typically consists of the following activities:

- Conduct interviews with key business & technology stakeholders
- Collection of artifact data to conduct comprehensive current state analysis of operations
- Establishment of business future state needs and drivers for information security
- Evaluation of legal and regulatory requirements that impact those drivers and the appropriate assessment standards to be applied.
- Creation of future state model and identification of initiatives to achieve business and compliance goals
- Mapping of corporate practices, policies, technologies, training, access controls, authentication, physical security, systems designs, and business practices against the recognized standards, and assessment of these practices for both risk and impact
- Prioritization of initiatives across a timeline that is manageable, executable and fits within company resources and operating budgets

DELIVERABLES:

You will receive several reports customized for different audiences – a Detailed Report, including an executive summary, general findings, specific findings, a gap analysis, and a business impact and risk analysis which weights each of the risks based upon their severity and potential impact on the business; and Executive Presentations for senior leadership and the Board. Where significant risks are discovered during the assessment process, Cisco will notify you immediately and will provide you with guidance and advice for remediation or mitigation.

The Detailed Report is designed to allow those in authority to drill down on specific findings, examine details, and prioritize mitigation. The report includes a gap analysis as well as recommended remediation processes for achieving the desired end-state. Executive Presentations will present in business language, justification for recommended security initiatives.

The Cisco SSR will provide Rough Order of Magnitude (ROM) costs for each initiative, which will be broken down into separate projects. It will break out estimated CapEx, OpEx and internal resource levels of effort necessary to accomplish project objectives. Furthermore it will identify critical and dependent tasks between project initiatives so you know what needs to start first. Finally, the report will help reduce your audit and compliance burden, and provide detailed findings to support later IT Security audits.