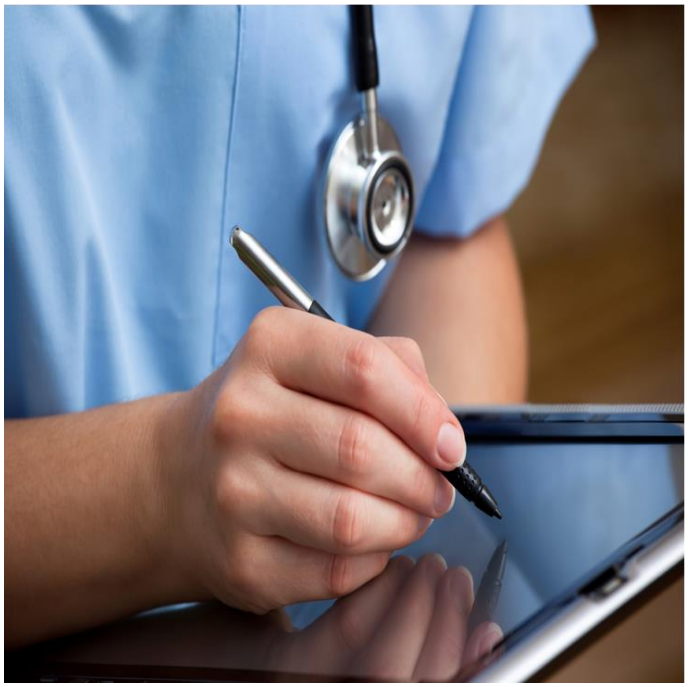
The Evolving Information Security Challenge for Healthcare Organizations

Solution Brief



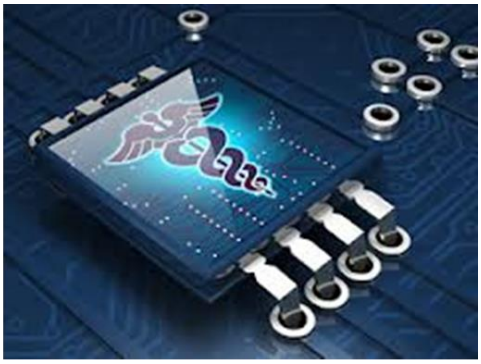


Table of Contents

Executive Summary

The success of a healthcare organization is going to become increasingly more dependent on the organization's ability to keep electronic protected Health Information (ePHI) secure (i.e., available, confidential, and ensure integrity).

An in-depth analysis of the HIPAA regulations will disclose the need to address issues from a business perspective. This business perspective can only be realized by instituting a program based on risk assessments and analyses. Gone are the days where governing and regulating bodies are prescriptive with information security. Each organization is now required to do this work. This requirement poses three important questions to an organization:

1. Do you understand the information security risks to your unique organization?
2. Have you taken steps to mitigate these risks that are appropriate to your organization?
3. Have you established an appropriate management and governance model to be sure your mitigation practices are in place and being used?

If a company does not have a documented process through which to assess cyber risk and/or does not have a person designated to be in charge of the assessment process, functionally, the organization is exposed to having no plan for cyber risk at all.

Strategic Information Security Program

A Strategic Information Security Program provides the model on which to build the processes needed to gain and maintain the business perspective. Too many healthcare organizations attempt to implement information security using an "address the current issue" approach. This most often results in a less than optimal and unsustainable solution to the broader information security problem of protecting sensitive data from unauthorized access and use which continues to grow in magnitude as Health Information Exchanges (HIE) become more widely implemented as required by the Patient Protection and Affordable Care Act (PPACA). This problem can only be solved through a sound security strategy unique to each organization's operating environment, and includes cross-organizational participation as various departments may view the same issue and its effect on the overall business perspective differently. Management needs to have a means to gain visibility and awareness of these differences if they are to resolve them and formulate a sustainable program of cost-effective cyber security that is consistent with their business plan.

A Strategic Information Security Program may contain a number of Information Security Frameworks (ISF). In the context of a healthcare organization, an ISF is a business process involving all entity organizations (i.e., Business Associates), operations sections, and relevant participants in information security. It is an ongoing process which, when fully developed, will position the organization to address the right security issues so that the business fulfills its mission. Consequently, the best approach is to adopt a strategy which will address multifaceted information security issues.

The most sustainable and accepted approach is to adopt a strategy of implementing a vetted, best practices approach to an enterprise-wide process which will address the multifaceted information security issues of a healthcare organization.

The program must be implemented in such a way as to ensure the confidentiality, integrity, and availability of the data while in storage, transmission or processing. This can only be accomplished if the program provides the means to support a life-cycle management process of continuous review of relevant security measures with regards to education, training and awareness; policies and procedures; and technology.

The fiduciary responsibilities of any organization dictate that financial decisions must be based on detailed analysis and industry accepted practices. The practice advocated by the U.S. Dept. of Health & Human Services (HHS), Office of Civil Rights, as it pertains to HIPAA, is a risk management program that weighs the cost of a security control against the probability of a vulnerability being exploited (risk) and the potential liability should the ePHI be compromised.

Lifecycle of a Strategic Information Security Program

The lifecycle of a Strategic Information Security Program can be broken down into four phases that, once implemented, create a continuous loop process to regularly review an organization's security posture and adjust to any changes to its operating environment or the industry threats.

The first phase (Plan Phase) consists of selecting the members of the Privacy Steering Committee who can then choose the standard to be used for the management of the program. Issues such as processes, policies and procedures in support of the selected standard should be developed during this phase. Following the completion of the initial lifecycle, this phase is used to review the progress made and set the strategy for beginning the next lifecycle.

Initially, in phase two (Do Phase), a review of the standard selected in phase one is used to assess the organization's position with regards to a specific law or regulation in order to understand the effort required and the controls that need to be implemented to meet the security requirements of that law or regulation. A Security Awareness Training program is developed to stress the points employees should understand regarding the requirements and necessary controls related to meeting the security and compliance requirements. A risk analysis is performed for the purpose of understanding the liability associated with that risk and priorities are determined so that a plan can be implemented to mitigate the risks while meeting the fiduciary responsibilities of the organization. An Incident Response plan is developed in this phase in order that all necessary personnel are aware of their responsibilities should a compromise occur and the requirements of the Breach Notification Rule can be met. In subsequent lifecycles, execution of the identified improvements in phase one are accomplished.

Phase three (Check Phase) is the daily operation and execution of the strategic information security program in order to detect potential threats from external sources as well as inappropriate or questionable behavior of employees. All of this data is monitored, reviewed and stored in the event of an incident. It also serves as a means of collecting data that may be factored into the financial justification for additional controls or services needed to strengthen the organization's security posture.

In Phase four, (Act Phase) activities such as a planned test of the Incident Response Plan is executed, an audit of the Security Awareness Training Program is done in order to identify areas of focus for the next phase of training, and a general assessment of the program is made so this data can be used for review by the Privacy Steering Committee in phase one of the next lifecycle.

The goal of this Solution Brief is to provide greater insight and understanding as to how Dell SecureWorks can assist a healthcare organization in designing, implementing and managing a Strategic Information Security Program as the laws, regulations and threats evolve in the healthcare industry. The focus of the Patient Protection and Affordable Care Act is on new service delivery and payment models that encourage and facilitate greater coordination of care and improved quality. This is a new way of stating the business objective of "Improved Patient Care" that is the mission of every healthcare provider.

Elements of a Strategic Information Security Program for Healthcare Organizations

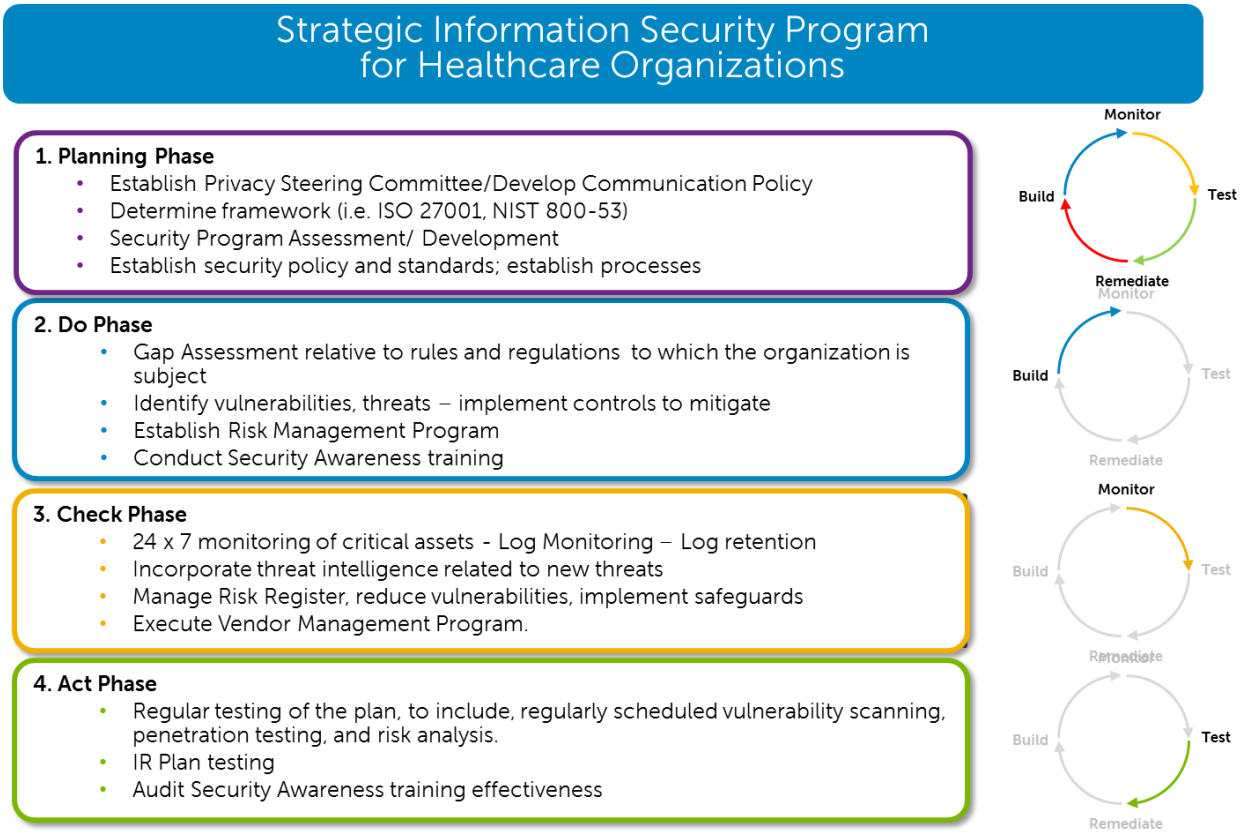


Figure 1

How Dell SecureWorks Can Help

Dell SecureWorks, through our four pillars of services – Managed Security, Security and Risk Consulting, Threat Intelligence and Incident Response, is able to assist our clients in the development of a Strategic Information Security Program and augment their efforts in the ongoing operation, maintenance, and support of change.

How Dell SecureWorks Can Help	Dell SecureWorks Services
Plan Phase – Initial Assessments	Security Program Assessment, Development and Risk Analysis Risk Management (Security) Program Development
The Do Phase	HIPAA Gap Assessment Computer Security Incident Response Plan (CSIRP) Security Awareness Training Solutions Risk Analysis (NIST 800-53; ISO 27005) Penetration Testing Vulnerability Management Vulnerability Monitoring and Prioritization
The Check Phase	Security Monitoring Managed Log Retention Global Threat Intelligence Targeted Threat Intelligence
The Act Phase	Incident Response Testing and Capability Analysis Services – TableTop Exercises CSIRP Gap Analysis Emergency Incident Response

Dell SecureWorks Services

Security Assessment and Risk Analysis
Dell SecureWorks' Security Assessment and Risk Analysis is a comprehensive security and risk assessment of your security program, including your internal and external controls, physical security, policies and procedures, gaps vs. regulations and best practices, and vulnerabilities and threats. Dell SecureWorks security consultants use best practice benchmarks to identify select control gaps and strengths. A gap analysis based approach provides sufficient control visibility to set objectives and priorities for remediation efforts.
http://www.secureworks.com/consulting/security_testing_and_assessments/risk_assessment/

Security Risk Program Development
Dell SecureWorks' Security & Governance Program Development services provide you the security, risk and compliance expertise to help you develop your strategic security, risk management and governance programs.
http://www.secureworks.com/consulting/security_and_governance_program_development/

Computer Security Incident Response Plan (CSIRP) Development
Dell SecureWorks information security consultants help you develop an effective CSIRP, based on IT security best practices and tailored to your organization's specialized needs. Your incident response plan will detail what needs to happen so you and your team can respond quickly and effectively to a security breach, and minimize the impact to your organization. In addition, your Computer Security Incident Response Plan will reflect the latest intelligence on threats and tradecraft used by attackers, and addresses the specific types of threats and scenarios of greatest concern to your organization.
http://www.secureworks.com/incident-response/incident-response-planning/computer-security-incident-response-plan-development/

Managed Security Awareness Programs
Security Awareness Training solutions help you assess your current Information Security Awareness Training programs, design new programs by top IT security advisors and provide specialized training to address areas of greatest concern to your organization. Going beyond compliance, Security Awareness Training Solutions change employee behavior and reduce risk to your organization.
http://www.secureworks.com/consulting/security-awareness-training/managed-security-awareness-training-service/

Security Awareness Training Solutions
Dell SecureWorks' Security Awareness Training Solutions help you assess your current SAT programs, improve program design with input from top security experts and provide specialized training to address areas of greatest concern to your organization. Going beyond compliance, Dell SecureWorks' Security Awareness Training Solutions change employee behavior and reduce risk to your organization.
http://www.secureworks.com/consulting/security-awareness-training/

Penetration Testing
Dell SecureWorks' Penetration Testing (Pen Test) services help you test your network security defenses and meet compliance with government or industry regulations. A penetration test (also known as ethical hacking) determines how well your organization's security policies protect your assets by trying to gain access to your network and information assets in the same way a cyber attacker would.
http://www.secureworks.com/consulting/security_testing_and_assessments/penetration_testing/

Incident Response Planning and Analysis Services
A robust Computer Security Incident Response Plan (CSIRP) is critical to minimizing the duration and impact of a security breach. With Dell SecureWorks' Incident Response Planning and Analysis services, our expert consultants work with you to prepare your organization to respond quickly and effectively to a security incident. Incorporating the latest security intelligence on threat actors and their tradecraft, we ensure your team's response procedures address even the most sophisticated threats including Denial-of-Service attacks, cybercrime and Advanced Persistent Threats (APT).
http://www.secureworks.com/incident-response/incident-response-planning/

Vulnerability Management
Dell SecureWorks' Vulnerability Management service identifies exposures and weak spots in your environment by performing highly accurate external scanning and internal scanning across the network. Vulnerability Management enables world-class vulnerability scanning without the hardware, software and maintenance requirements of scanning products. Vulnerability results are integrated into our other Managed Security Services, allowing threats against vulnerable and non-vulnerable systems to be assessed and prioritized accordingly. The Vulnerability Management technology is fully managed and maintained by Dell SecureWorks' dedicated vulnerability management team, eliminating administration and maintenance burdens so you can better focus on protecting your assets and reducing business risk.
http://www.secureworks.com/it_security_services/vulnerability_management/

Vulnerability Monitoring and Prioritization
Dell SecureWorks' Vulnerability Monitoring and Prioritization, delivered as a service, correlates external Internet breach and exploit data with vulnerability data to monitor, measure and prioritize vulnerability remediation across the client's environment. Results, including risk meter visualizations, are displayed within a dedicated business intelligence dashboard accessed via the Dell SecureWorks Client Portal.
http://www.secureworks.com/it_security_services/vulnerability_management/vulnerability-prioritization/

24x7x365 Security Monitoring
Dell SecureWorks' Security Monitoring service delivers real-time monitoring, correlation and expert analysis of security activity across your enterprise. This service improves the effectiveness of your security infrastructure by actively analyzing the logs and alerts from network devices in real time, 24x7x365. Our advanced technology platform provides our certified Security Analysts with the context needed to eliminate false positives and respond to the true threats to your information assets.
http://www.secureworks.com/it_security_services/security_monitoring/

Managed Log Retention
Provided as a hassle-free service, Dell SecureWorks' Managed Log Retention service helps organizations satisfy security and compliance requirements for log collection, storage and reporting without the management overhead and capital expense required for log management products. This service provides support for a wide range of sources, allowing capture and aggregation of the millions of logs generated every day by critical information assets such as servers, routers, firewalls, databases, applications and other systems. Our Log Retention service can support hundreds of devices per appliance - allowing for highly scalable retention of logs from across your organization.
http://www.secureworks.com/it_security_services/log_retention/

Global Threat Intelligence
Leveraging Dell SecureWorks' global threat visibility across thousands of customer networks, proprietary toolsets and unmatched expertise, the Dell SecureWorks Counter Threat Unit (CTU) security research team performs in-depth analysis of emerging threats and zero-day

vulnerabilities. Powered by CTU research, the Dell SecureWorks Threat Intelligence service delivers early warnings and actionable security intelligence enabling you to quickly protect against threats and vulnerabilities before they impact your organization. The Threat Intelligence service enables you to reduce considerable risk by closing the window of exposure more quickly, and also enables you to spend more time devoted to quickly remediating the risks most pertinent to your organization.
http://www.secureworks.com/cyber-threat-intelligence/CTU_intelligence/

Targeted Threat Intelligence
Targeted threat intelligence services allow organizations to identify and assess targeted threats and the actors behind them, gain insight into ongoing exploits at a detailed level, and take proactive steps to defend against them. Services include Targeted Threat Intelligence, Enterprise Brand Surveillance and Executive Threat Surveillance.
http://www.secureworks.com/cyber-threat-intelligence/targeted-threat-intelligence/
http://www.secureworks.com/cyber-threat-intelligence/targeted-threat-intelligence/enterprise-brand-surveillance/
http://www.secureworks.com/cyber-threat-intelligence/targeted-threat-intelligence/executive-threat-surveillance/

CSIRP Gap Analysis
The Dell SecureWorks CSIRP Gap Analysis reviews your computer security incident response plan against best practices, identifies gaps in your response procedures and provides recommendations to enhance your CSIRP's overall effectiveness when a breach occurs. Our IT security experts will conduct a detailed assessment of your existing incident response documentation, capabilities, personnel and procedures, and formulate recommendations designed to improve your CSIRP.
http://www.secureworks.com/incident-response/incident-response-planning/csirp-gap-analysis/

Incident Response Testing & Capability Analysis – Table top exercises
Through real-world simulations, Dell SecureWorks Incident Response security experts can test and evaluate the effectiveness of your CSIRP, your response procedures and how well your team responds to an attack. Periodic testing of your Computer Security Incident Response Plan will ensure your team is ready to act when a major security incident occurs. Through our CSIRP Gap Analysis service and tabletop exercises, we evaluate your team's plans and capacity to respond to and contain a major security breach. Simulations are based on our latest threat intelligence on actors and their tradecraft and are designed to stress and assess your team and procedures during an incident. During the tabletop exercises, we educate you and your team on Incident Response best practices. In the end, your team is primed for an actual security incident with a CSIRP that has undergone a robust evaluation process.
http://www.secureworks.com/incident-response/incident-response-plan-testing-and-capability-analysis/

Emergency Incident Responses
The Dell SecureWorks Incident Response and Digital Forensics practice provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach. Leveraging elite cyber threat intelligence and global threat visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents.
http://www.secureworks.com/incident-response/emergency-response/

About Dell SecureWorks

Dell SecureWorks is a market-leading provider of world-class information security services with more than 3,800 clients in 70+ countries. Organizations of all sizes rely on Dell SecureWorks to protect their assets, improve their compliance and reduce their costs. Our combination of award-winning security expertise and client support makes Dell SecureWorks the premier provider of information security services.

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks' Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyber-attacks, and recover faster from security breaches.
For more information, visit: http://www.secureworks.com

For more information, phone 877.838.7947 to speak to a Dell SecureWorks security specialist.