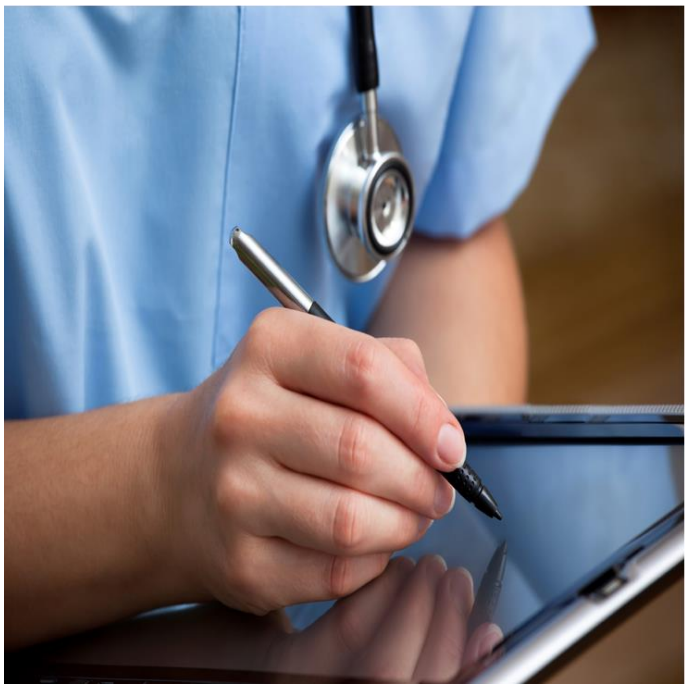
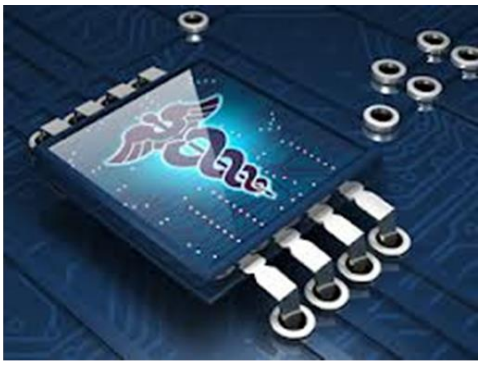
Topic Brief: Strategic Information Security Program

Healthcare Information is Under Siege





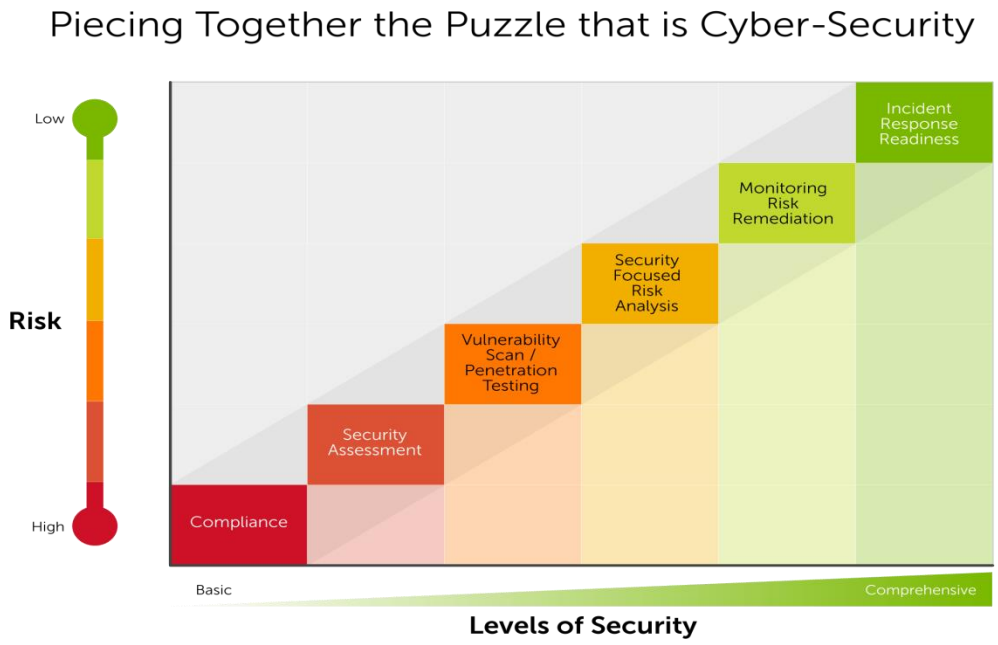
Strategic Information Security Program

Recent security events in the healthcare industry have created a heightened awareness of the threat(s) to the electronic Protected Health Information (ePHI), for which they are responsible to maintain the confidentiality, integrity and availability. The effort to protect this information can no longer be sufficiently addressed through the pursuit of compliance to the HIPAA Regulation alone.

According to the Identity Theft Resource Center, 44 percent of all registered data breaches in 2013 targeted medical companies. Furthermore, the number of information security breaches reported by healthcare providers soared by 60 percent from 2013 to 2014—more than double the increase seen in other industries—with financial losses up by a stunning 282 percent, according to PwC's Global State of Information Security Survey 2015.

The healthcare industry must center their vision on security and the security controls and policies necessary to provide the "Optimum Security", based on that organization's operating environment, necessary to defend against the increasing number of threat actors, threats, and attack surfaces against which an attack might be launched.

While a defense that will ensure this information will never be compromised is not possible, a properly designed and implemented Strategic Information Security Program, with the goal of continuous oversight and proactive remediation, offers the greatest level of security and reduces the liability of the organization should it experience a breach.



Questions to be asked as the puzzle is assembled:

Security Awareness Training

- Employees remain the number one threat to critical information assets
- Is there an ongoing enterprise awareness training campaign focused on cyber security?

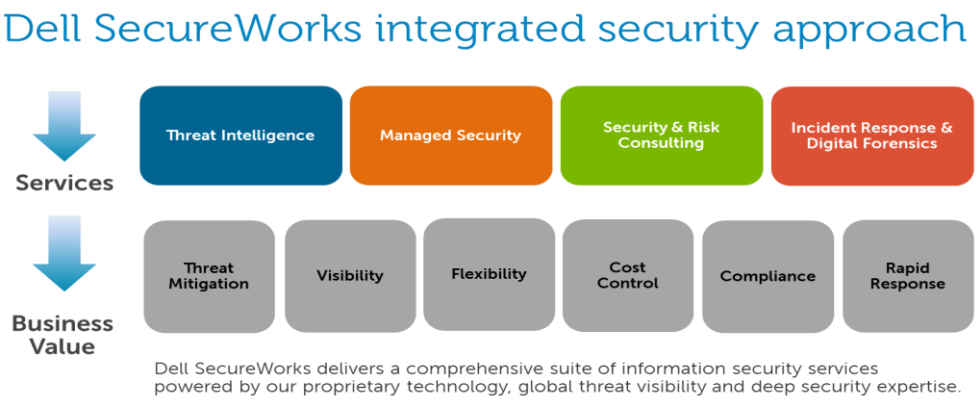
Risk Analysis/Risk Remediation

- Can the management team articulate its cyber risks and explain its approach and response to such risks?
- Is your company properly managing business associates?
- Are you measuring the degree to which your organization is meeting the board's cyber risk appetite?
- Does your organization have cyber insurance? If yes, what steps have you taken to determine if it is adequate coverage?

Incident Response Readiness

- Do you have an Incident Response Plan that includes a Contingency Plan?
- How often do you conduct Table Top tests of the plan?
- Is the plan designed such that it is flexible enough to rapidly change as the threat environment changes?
- Has management assigned clear roles and responsibilities for identifying, evaluating, monitoring, and responding to cyber-security incidents?

The magnitude of this effort and the skills required to design, implement, and maintain such an effort are such that it cannot be done by any single organization. Just as in actual war, allies must be a part of any defense plan. Each ally should be evaluated for their area of expertise that contributes to the overall defense effort. This evaluation should take into account the depth and breadth of the ally's experience. In both cases, Dell SecureWorks' Integrated Suite of Security Services is unmatched (See Figure 2) and provides a business value that is unmatched by other potential allies a client might consider.



Dell SecureWorks brings its core assets of each service area to bear when assisting a Healthcare client in the design, implementation, and continuous oversight of a Strategic

Information Security Program aimed at "Optimum Security" for that client's unique operational environment.

When this suite is delivered in conjunction with Dell Service's Healthcare and Life Sciences Group, a unique Healthcare specific plan to achieve that organization's "Optimum Security" posture is realized.

Threat Intelligence:

The Threat Intelligence Service, while a stand-alone service, is the foundation on which the other three services are tailored to a specific client's requirements. It is through the threat intelligence that an organization can be made aware of the pending threats to their industry. Of equal importance, it will serve as the means to determine weaknesses in the organization's defense thus providing the knowledge needed to plan for improvements whether they be in technology, security policy, or procedures.

Managed Security Services:

The Managed Security Service is most often used to augment existing in-house resources in the managing and monitoring of the organization's infrastructure. A critical resource provided by this service that is often a recommendation coming from the Meaningful Use certification effort is the Intrusion Protection/Intrusion Detection service. A key benefit of this service is the more frequently updated malware signature tables as a result of the Threat Intelligence Service. More recently, as a result of some highly publicized breaches, the importance of Security Awareness Training, as a service, provides custom training aimed at the client's environment and the ability to regularly test the effectiveness of the training by reinforcing the important teaching points.

Security and Risk Consulting:

The Risk Consulting Service combines the working knowledge of the Threat Intelligence Service with the skills of a security certified team to both advise and assist the client in their security initiatives. Efforts such as Risk Analysis and the implementation of a Risk Management Program to monitor the risk mitigation efforts necessitated by the Risk Analysis, performing a Security Assessment to determine the areas of the infrastructure where ePHI is maintained and what vulnerabilities exist in these areas, development of policies & procedures, and performing assessments, as required by the HIPAA Security Rule and Meaningful Use.

Incidence Response:

Since it is no longer a question of if an organization is going to be breached but when it will be breached, having an Incident Response Plan such that the organization is prepared to respond quickly and proactively is mandatory. Having the plan and having tested it and trained the key individuals in the execution of the plan such that there is no hesitation are two different things. The service offered by Dell SecureWorks can assist the client in this effort as well as be on stand-by should the client need additional personnel and/or skills not available in the organization.

About Dell SecureWorks

Dell SecureWorks is a market-leading provider of world-class information security services with more than 4,000 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.