Managing your enterprise security effectively can add value

Let’s face it: The world is changing. Today, everything is mobile, connected, interactive, immediate, and fluid, and it takes a special kind of enterprise to compete in this world. It takes an enterprise with the agility to learn swiftly and continuously to close the expectation gap between what customers expect and what the enterprise can deliver. It takes becoming an enterprise whose business and technologies are one and the same—working in alignment to achieve strategic objectives.

One of the key requirements of becoming this kind of enterprise is the management of risk. Every business decision has inherent risk, but it’s important to understand and make decisions based on the cost and potential value of taking that risk. Chief information security officers (CISOs) no longer lie awake at night worrying only about defending their organization’s perimeters and the latest worm outbreak; challenges facing security leaders are far more complex.

As organizations innovate and grow, they make more demands on IT departments. These groups become increasingly challenged with finding the most effective way to deliver IT services to support overall business objectives in combination with more complex external compliance, legal, and regulatory requirements.

There are numerous driving forces behind the continual rise in information security costs as a percentage of overall IT budgets. These include computing, mobile working, and social media among others. Securing the enterprise cost-effectively is not an easy task; it involves strategic thinking and the ability and willingness to transform elements of your security operations and management proactively.

Many chief information officers (CIOs) and CISOs are still unsure about how to recognize their information security priorities, as well as the opportunities and risks associated with some of the key market drivers, such as cloud and mobility. As a result, you are likely to have faced some of these tough questions:

• What are our biggest information security risks and what are the cost implications?
• What are the dangers of using social media freely for our marketing activities?
• Will our new IT services be secure enough to protect business and customer data?
• Can I use my tablet to get work emails?
• Do we comply with our legal, regulatory, and governance requirements?

Because every organization has different information security needs, it is important to understand what those needs are and their impact on your business in terms of opportunities and threats. At HP, we make it our priority to help you understand the areas of security that are critical to you and how these can be managed effectively with confidence.
Get a complete understanding of your security posture in one day

Most organizations are too busy fighting fires to spare the time to take a hard look at their overall information security strategy. Our aim is to let you do this in a single day by identifying your biggest challenges, looking at how you are currently addressing them, and showing how you can use our maturity model to implement a prioritized roadmap to develop your capability.

During the one-day, interactive workshop, senior HP consultants use highly informative visual displays to share with you what they have learned from their vast experience of information security. By involving business and IT stakeholders in this process, we can create an environment that helps align key initiatives and priorities. Ultimately, the goal of the workshop is to facilitate faster decision-making and cross-team collaboration—so that you can begin your journey to becoming a secure enterprise.

Experience security transformation—live

Effective information security protects stakeholder value by lowering business risk and delivering more effective and efficient use of information resources. In this strategic workshop, we enable you to understand your information security capability by using a simple management framework, which consists of five functions: fundamental services, strategy management, infrastructure management, issue management, and compliance management. From this we can draw a “roadmap” with priorities specifically designed to support your strategic and functional goals.

To do this, the HP Enterprise Security Discovery Workshop takes you though the following steps:

• Setting the scene: Provide a discussion around business drivers and market trends, giving an overview of where information security fits into your organization as a whole.

• Information-centric security: Define the important factors in moving from a tactical approach to information security based on infrastructure and technology “fixes” to an approach that is strategic and information- and data-centric.

• The approach: Give you an understanding of the framework that will be used to assess your current information security issues.

• Current state: Deliver an assessment of the issues that contribute to your current level of information security maturity.

• Transformation journey: Develop a customized roadmap, using the results of the current-state assessment to discuss and prioritize the issues raised.

• Next steps: Agree on recommendations and short-, medium-, and long-term actions based on the roadmap.

Here are five reasons to sign up for HP Enterprise Security Discovery Workshop:

• Gain insight into the market trends and drivers and how these impact your organization’s current information security posture.

• Take a business-driven, strategic approach to information security.

• Identify priority projects based on information security capability issues.

• Build and implement a transformation plan.

• Bring key stakeholders together to allow free-flowing discussions, cross-team collaboration, and agreement about the future management of information security in your organization.

What is next?

Contact your account manager to discuss booking a workshop or email us at securityworkshop@hp.com