Security Analytics: putting the science into security management

As the pressure on business increases, so does the complexity of the security challenges. As a result, security teams are finding it increasingly hard to achieve, measure, and communicate a measurable reduction in business risk.

So how should a security team determine the best possible strategy? How much should be spent? What should be prioritised? What trade-offs are to be accepted between lowered risk and business disruption? How to champion and justify security decisions to the business?

HP Enterprise Security and HP Labs have a shared vision for next-generation security management: one that helps our clients achieve a measurable reduction in business risk, along with a lower long-term investment in information security.

Security Analytics is at the heart of this vision and is about creating tools and methodologies to rigorously address the challenges that security teams face in driving more effective security strategies.

The HP IS and HP Labs approach is to use mathematical systems and economic models to analyse not only the technological aspects of an infrastructure, but also the social, economic, behavioural, and policy aspects that affect business and security outcomes. As such, it involves the integration of a wide range of sciences including computer science, mathematics, economics, human factors, and cognitive science.

The HP approach

Packaged Security Analytics

By combining HP IS expertise in Security Governance with HP Labs’ expertise in Security Research, we are able to offer a packaged consulting engagement featuring repeatable, short-term engagements to address security management challenges (people, process, policy, and technology) in two key areas:

• Vulnerability and Threat Management (VTM)
• Identity and Access Management (IAM)

The value of these engagements is:

• A rigorous exploration of your (VTM or IAM) system, with prediction and “what-if” capabilities
• Shared multi-stakeholder understanding of the business and security trade-offs
• Justified decision to introduce science into your Information Security Management System (ISMS)
• The opportunity to expand

In common with all of HP’s customer engagements, HP Enterprise Security works closely with an organisation to understand its business drivers, security policy, and regulatory framework.

Security Analytics elements

1. Problem Definition

The process starts with a meeting with our consultants to discuss your unique challenges and determine a precise terms of reference and engagement model. Although the process is iterative, clearly there are many areas that can be analysed, and therefore, our consultants will take a strategic approach to establish a way forward that is closely aligned with the needs and priorities of your organisation.
2. Model Construction
This is an iterative process involving workshops, data gathering, and interviews with key stakeholders. The diagram below is a screenshot of the security analytics tool showing a typical VTM model. The internal processes and decisions are in grey, and the external threat environment is in red.

3. Model Exploration
The model can be “executed” and measurements taken—such as time taken to patch or have other mitigations in place. Using our proven, sophisticated tools, we can run thousands of such simulations with different parameters to predict possible outcomes through rigorous “what-if?” analysis.

The graphs below show outputs from a typical engagement, which looked at the current status of risk exposure and the predicted effects of two different security investment strategies. For example, a starting point for a VTM engagement is “We have a complex collection of process and technology controls: patching, antivirus, intrusion prevention, accelerated patching, and so on. Are we doing enough, too much, should we doing more to reduce risk, or is the business disruption already too much?”

4. Decision-making
It is important to bring the analysis to a conclusion, to ensure there is a shared understanding of the conclusions and consequences. Our team of consultants are backed by full service capabilities, and closely aligned with the ongoing HP Labs investment in Security Analytics.

As such, we are well placed to help you champion and see through your decisions, and to put in place changes in ongoing security governance relating to IAM or VTM. In short, these short-term packaged engagements are a perfect way to start introducing scientific rigor into your ISMS.

About HP Enterprise Security
HP has a history of pioneering solutions that are proven to deliver an effective and measurable reduction in organisational risk, a lower long-term investment in information security, and an improved security posture. Whilst other security companies focus on security threats and help organisations lock down information to protect it, our success is driven by viewing information security differently.

HP Enterprise Security experts take a proactive and risk-based approach, ensuring the freedom of information within and around the organisation whilst enabling new opportunities such as cloud and “consumerisation.”

About HP Labs
HP Labs is the exploratory and advanced research group for Hewlett-Packard, tackling complex challenges facing HP’s customers and society, whilst pushing the frontiers of fundamental science.

The goal of the Cloud and Security Lab is to create a trustworthy information-system environment by applying knowledge of mathematics, modelling, systems, and security to enable safe participation in the online world.

For more information
Go to www.hp.com/enterprise/security