Security Risk Management – an Introduction

Taz Wake - Security Director

t.wake@halkynconsulting.co.uk

Overview

- Introduction
- What is risk management?
- Risk management vs compliance
- Risk management frameworks
- Risk management program
- Next steps

Introduction

- This presentation gives a brief overview of what is involved in building an operational approach to address organisational risks
- Objectives:
  - Understand the central elements of an enterprise-wide risk management framework
    - Understand the limitations of relying on compliance with standards
    - Gain awareness of risk management frameworks
    - Serve as a stimulus to action

What is Risk Management?

What is Risk Management?

- Risk is often defined as the "*effect of uncertainty on objectives*".
- This is refined in the context of security to "*potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation*".
- Risk management is the process by which limited resources are allocated to achieve the optimum response to risk, prioritised in accordance with the evaluation of risks.

What is Risk Management?

- Risk management is important to the function of every business and drives the use of finite resources.
- Risk management takes place at every level in an organisation – whether or not this is formally recognised.
- Strategic risk management is driven by senior management to enable subordinate divisions to properly manage risks on behalf of the business.

Risk Management vs Compliance

Risk Management vs Compliance

- Two different functions that can work together
  - Risk management involves identifying the risks your organisation faces and determining the most suitable methods to reduce them to acceptable levels.
  - Compliance is ensuring that your organisation follows the rules and regulations governing business activities.
- Compliance can generate a source of risks which must be managed and a good risk management strategy can be used to drive compliance with regulations.

Risk Management vs Compliance

- Compliance with standards and regulations is important.
- Compliance is driven by regulatory controls.
- Failure to meet regulatory requirements for protecting personal data can result in
  - large fines or other monetary penalties
  - significant damage to reputation
- Failure to meet regulatory requirements for protecting financial information can result in
  - large fines
  - significant damage to reputation
  - loss of the licence to trade in your industry

Risk Management vs Compliance

- However - compliant is not the same as secure
  - It's only the first step towards improving information risk management
  - Regulations can't keep pace with changing threats
  - The regulations are there to protect customers and external stakeholders not your business
- Compliance becomes a security risk when it:
  - Becomes the only goal of a risk management policy
  - Encourages a "tick box" approach to managing risks
  - Gives a false sense of security that risks have been dealt with

Risk Management vs Compliance

- Remember:
  - In 2009 Heartland Payment Systems suffered a major breach compromising thousands of customer credit card details despite being PCI-DSS compliant at the time
  - In 2011 Citigroup was hacked compromising over 20,000 card holders despite the organisation being compliant with various government and industry regulations
  - Over 2011 - 2012, the ICO has fined public sector bodies over £2m despite their systems being assessed as compliant prior to the breach leading to the fines
- Following a breach, compliance is often revoked but this is too late to alert your business to the risk.

Risk Management vs Compliance

- A compliance gap is a risk that you have to manage.
- Compliance can be used to check conformity with your risk management framework / standard.
- Lastly:
  - More important than compliance with any particular Standard is the ability to demonstrate that risk is managed in the particular organisation, in its particular circumstances, in a way which effectively supports the delivery of its objectives. (HM Treasury)

Risk Management Frameworks

Risk Management Frameworks

- A risk management framework is a high level approach you can use to build your own strategy, policy and procedures for managing risks faced by your organisation.
- You can use existing frameworks produced by national or international standards organisations or produce your own.
- Examples of existing frameworks include:
  - ISACA's RiskIT, an extension of the COBIT framework.
  - NIST Special Publication 800-37
  - COSO Enterprise Risk Management — Integrated Framework

Risk Management Frameworks

- Using an existing framework can save time and effort as well providing assurance that it has been thoroughly tested by others.
- However, external frameworks are built for a generic customer base and may not properly reflect the needs, functions and requirements of your business.
- Producing your own framework can take longer but may result in a more effective result.
- There is nothing wrong with taking relevant bits from existing frameworks and building one that works for you.

Risk Management Programs

A high level approach to building an enterprise-wide risk management framework

Requirements

- Governance strategy
- Process (Plan – Do – Check – Act)
- Asset identification
- Asset / data classification
- Risk assessment
- Control assessment
- Residual risk assessment
- Treatment plans
- Review and Audit

Building a Program

- Risk management programs must be built top down.
- The first stage is determine how the program will be governed and ensure senior management support. Without this, the risk management program will fail.
- Risk appetites must be determined and documented to ensure clear understanding. The top down approach must ensure that risk appetites are appropriate and consistent.

Building a Program

- The scope of the risk management program must be clearly defined.
  - In a security risk management program you might want to ignore business "trading risks" such as competitor activity.
  - If your enterprise is complex it may be better to create supporting risk management programs for different functions or outsourced providers.
- Within the scope, you need to identify and document the relevant assets and provide a classification scheme to enable prioritisation of risks.

Building a Program

- Risk assessments are:
  - "*The process of assessing security-related risks from internal and external threats to an entity, its assets or personnel*." (ASIS Guidelines)
- This can be broken down into stages. For example:
  - Threat assessment
  - Vulnerability assessment
  - Probability assessments
  - (and many more)
- The end product of this is the security risk assessment.

Building a Program

- The output of the risk assessment should be used to drive the control assessment.
- This is the stage where you examine risks against existing controls to determine if the control is suitable or not.
- You must make sure you know the uncontrolled risk assessment first, as the effectiveness of controls changes over time.
- Where controls are weak or non-existent a risk exists that must be treated as part of your strategy.

Risk Treatment

- There are four basic treatments which can be used for risks
  - **Treat**. This is where you implement additional controls, or improve existing ones. Treatment can reduce the probability a risk will occur, reduce the impact or both.
  - **Tolerate**. Where it is not cost effective to take any action over a risk, the business may decide to simply accept it. This needs to be documented to ensure no business unit exceeds its risk appetite.
- (continues)

Risk Treatment

- There are four basic treatments which can be used for risks (continued)
  - **Terminate**. Some risks may be so harmful, or expensive to treat, that there is no option but to stop doing the activity which creates them.
  - **Transfer**. It is often possible to transfer some or all of the risk to a 3rd party. This is normally done in the form of insurance or a contractual obligation which will compel the 3rd party to bear the financial impact of a breach.

Risk Treatment

- It is possible to use a hybrid treatment, but this is often the result of the underlying risk not being clearly defined.
- Risk treatment decisions should always be documented and agreed by suitable levels of management.
- Where risks are tolerated, it is important that should the risk be realised, additional funds are not then spent to remediate it as this undermines the cost saving from tolerating the risk.

Risk Management Cycle

- Once the risk treatment options have been decided and implemented, there needs to be a process of ongoing monitoring and audit.
- Controls should be regularly assessed to ensure continued effectiveness.
- Risks should be regularly assessed to identify changes – new threats emerge, new vulnerabilities are discovered and existing threats / vulnerabilities may be repaired or made irrelevant by changes.

Risk Management Cycle

- Risk reviews should be driven by the severity of the risk and the criticality of the asset.
- When the assessment determines a change to the risks, the risk management cycle should repeat from the start.
- If new assets are introduced into the enterprise, the risk management cycle should repeat from the start.

Next Steps

Next Steps

- This presentation has been a brief, high level, overview of the process. Once you have built the framework, it is important that you continue to drive the process.
- Your risk management strategy and framework should also drive the development of your business operating and security policies.
- As part of your governance, you need to consider your organisations "maturity" towards security and risk. If you have built a process from scratch, this will be low but measuring it can help demonstrate your progress.

Next Steps

- There are additional factors you need to develop, but they are outside the scope of this presentation.
- These include, but are not limited to:
  - Risk analysis methods
  - Measurements and metrics
  - Information assurance (IA)policy, standards and processes
  - Security / IA maturity models
  - Cross-discipline frameworks to help manage overall corporate risk

Halkyn Consulting Ltd

www.halkynconsulting.co.uk

Halkyn Consulting Ltd

- Halkyn Consulting is a North Wales based consultancy specialising in security and risk management advice.
- We provide a variety of services supporting your own security and risk management functions, from helping you design frameworks to assessing your implementation and maturity.
- If you want to find out more about how you can improve your organisation's posture, or simply want to talk about security then get in touch today.

Halkyn Consulting Ltd

You can get in touch with Halkyn Consulting at:

(+44) 1244 940 858

info@halkynconsulting.co.uk

www.halkynconsulting.co.uk

Twitter | Google+ | LinkedIn | Blog Feed

References

- ISO 31000:2009 *Risk management – Principles and guidelines*
- ISO/IEC 27005:2008 *Information technology – security techniques – Information security risk management*
- HM Treasury: *The Orange Book: Management of Risk - Principles and Concepts* (2004)
- ASIS: *The General Security Risk Assessment Guideline* (2002)