Information Security

for SME’s

SANS Information Security Webcast

22 Nov 2011
Geneva, Switzerland

Jim Herbeck
Managing Partner, Nouvel Strategies
JHerbeck@NouvelStrategies.com

Member of Faculty, SANS Institute
JHerbeck@sans.org

Webcast archive:
https://www.sans.org/webcasts/information-security-smes-jim-herbeck-94849

Slide handout (English):
http://nouvelstrategies.com/InfoSec-for-SMEs

Slide handout (French):
http://www.hesge.ch/heg/ccsie/CCSIE_ressources.html

MANAGING INFORMATION RISK FOR THE SMALL AND MEDIUM ENTERPRISE

Agenda

- Introduction to Information Security
- Assessing Risk
- Implementing Information Security
- Verifying Compliance
- Final Words

What is information security?

- The discipline of protecting information resources:
    - information
    - computer hardware
    - computer software
    - IT infrastructure
    - people
- Protection ensures:
    - confidentiality
    - integrity
    - availability

Misconceptions about information security

- Information security is an “IT thing”.
- Adequate information security is already included in products you buy.
- There’s very little an SME can do about information security.
    - Therefore, there’s no reason to try.

How much information security is enough?

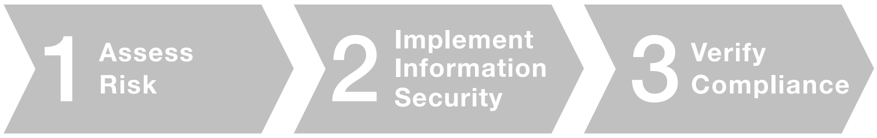
- A difficult question to answer–because it’s the wrong question. The correct question is:

How much information risk is my business able to tolerate?

- Businesses determine their own risk tolerance levels, with a few exceptions:
  - data privacy (government legislation)
  - credit cards (PCI-DSS)

Simple strategy for information security and information risk management

- Use a 3-step strategy:



1 Assess Risk

2 Implement Information Security

3 Verify Compliance

- Each step produces an “output” used as the “input” for the next step.

- Process is repeated annually, with incremental improvements accumulating over time.

Agenda

- Introduction to Information Security
- Assessing Risk
- Implementing Information Security
- Verifying Compliance
- Final Words

What is information risk?

- Risk is the potential harm that may be caused by a future event.
- Information risk focuses on harm to information- and IT-related resources.
  - Loss of confidentiality, integrity, or availability.
- Information risk is the responsibility of many parts of the organization in addition to IT:

- management	- human resources
- legal	- purchasing
- finance	- facilities

Misconceptions about risk management

- Risk assessments take 6-12+ months to perform.
- Risk assessments may only be performed using complicated methodologies.
- Managers love the risk assessment process and will be happy to devote endless time and resources until the risk assessment has been completed at some point in the distant future.

Simple strategy for information risk assessment

Jan	12-month risk assessment (no information security program implemented; no risks reduced)
Feb	
Mar	
Apr	
May	
Jun	
Jul	
Aug	
Sep	
Oct	
Nov	
Dec	

Jan	1-month risk assessment
Feb	Implement information security program to reduce risk
Mar	
Apr	
May	
Jun	
Jul	
Aug	
Sep	
Oct	
Nov	
Dec	

Primary purpose of information risk assessment

- Goal of risk assessment is to identify the “top risks” to be corrected or “mitigated”.
  - Most organizations are only capable of targeting 5-10 information risks per year.
- During a “rapid” risk assessment, it should be possible to identify most of the top risks.
  - Any risks that were missed should be identified when the process is repeated the following year.

Risk metrics

- A measurement is the result of counting; a quantitative value indicating the size, length, or amount of something.
- A metric is a the result of analysis; a qualitative or subjective interpretation of a measurement.

Risk Level	Color	Face	Level of risk and potential impact on operational performance, compliance, and financial reporting
H	Red	🙁	High
M	Yellow	😐	Medium
L	Green	🙂	Low

The role of risk metrics

- Risk metrics have two important roles:
  - Quantifying the current level of risk.
  - Demonstrating the success of your information security program.

Risk assessment and risk metrics will be discussed in more detail during next months webcast “Risk Management for SME’s”.

Agenda

- Introduction to Information Security
- Assessing Risk
- Implementing Information Security
- Verifying Compliance
- Final Words

Review the risk assessment

- An information security implementation plan should be in response to an information risk assessment.
- Management reviews the responses for all identified risks. Possible responses include:
  - risk reduction
  - risk avoidance
  - risk retention
  - risk transfer
- Management approves the risk treatment plan.

Prepare implementation plan

- Select security measures to implement based on risks areas identified in risk treatment plan.
- Reference existing standards for “D-I-Y” (Do-It-Yourself) guidance (following slides).
- Develop information security policy that states risk management objectives.
  - How to write good information security policy will be discussed in more detail during a future webcast “Writing Information Security Policy for SME’s”.
- Implement the plan.

Guidance: Code of Practice

- The Code of Practice for Information Security Management is the global standard for best practice:
  - Defined by ISO 27002:2007 (115 pages)
    - Originally published as BS 7799:1995, ISO 17799:2000.
- Provides numbered control objectives and controls.
  - Control objectives: risk reduction goals.
  - Controls: administrative, technical, or physical means used to reach control objectives.

Guidance: Information Security Management System

- An Information Security Management System (ISMS) is quality management system for information security:
  - Defined by ISO 27001:2005 (34 pages)
    - Originally published as BS 7799 Part 2:1999.
  - Concerned with protecting confidentiality, integrity, and availability of information assets and resources.

Section numbers between ISO 27001 and 27002 are identical.

Guidance: SANS 20 Critical Security Controls

- The SANS 20 Critical Security Controls (SANS 20) are technical controls for improving information security, published by the SANS Institute:
  - Defined by a consortium of US government agencies and information security professionals.
  - Published on the SANS Institute website:
    - http://www.sans.org/critical-security-controls
  - Many controls can be automated.

How to select security measures for managing specific risks?

- Selecting security measures to implement to reduce specific risks is a complex topic for non-technical managers.
- Future webcasts will be devoted to these topics.
  - For example, how to manage the risk associated with having computers attached to the Internet will be discussed in more detail during a future webcast “Managing Network-related Risk for SME’s”.

Agenda

- Introduction to Information Security
- Assessing Risk
- Implementing Information Security
- Verifying Compliance
- Final Words

Compliance assessment

- Compliance assessments are performed to ensure that:
  - Information security controls are effectively meeting information security policy objectives.
  - Information security policy objectives are effectively mitigating information- and IT-related risk.
  - The organization is complying with all applicable laws and regulations involving information security and data protection.
- The “assessment process” looks similar to an “audit process.”

Audit vs. assessment

- Audits and assessments are very similar, but there are two important differences
  1. The goal of an audit is “attribution,” to identify risks and determine the root cause (who’s to blame).

     The goal of an assessment is to identify risks, so they can be corrected. It’s a “no-fault” or “non-attribution” process.
  2. Only certified auditors can perform an audit.

     Anyone can perform an assessment.

Assessment checklist

- The most important part of the assessment is the checklist that’s used.
  - the checklist includes a list of questions about risk areas that SME’s would commonly need to be concerned about.
  - the answers to the questions determine whether the risks are being adequately controlled.
- It’s possible to find audit/assessment checklists online, but take care:
  - your assessment will only be as good as your checklist.
- Future webcasts will cover this topic in more detail.

Agenda

- Introduction to Information Security
- Assessing Risk
- Implementing Information Security
- Verifying Compliance
- Final Words

Stay pragmatic, business-oriented, and standards-based

- Pragmatic
  - sensible and realistic, based on practical rather than theoretical considerations.
- Business-oriented
  - information security serves the business (not vice versa).
- Standards-based
  - use well-respected, established standards to simplify your efforts and ensure compliance.

Upcoming Webcasts for SME’s

Dec, 2011	Risk Management for SME’s
Jan, 2012	Writing Information Security Policy for SME’s
Feb, 2012	Managing Network-related Risk for SME’s

Information Security
for SME’s

SANS Information Security Webcast

22 Nov 2011
Geneva, Switzerland

Jim Herbeck
Managing Partner, Nouvel Strategies
JHerbeck@NouvelStrategies.com

Member of Faculty, SANS Institute
JHerbeck@sans.org

Webcast archive:
https://www.sans.org/webcasts/information-security-smes-jim-herbeck-94849

Slide handout (English):
http://nouvelstrategies.com/InfoSec-for-SMEs

Slide handout (French):
http://www.hesge.ch/heg/ccsie/CCSIE_ressources.html