Managing System-related Risk
for SMEs

SANS Information Security Webcast

15 May 2012
Geneva, Switzerland

version 1b

Jim Herbeck
Managing Partner, Nouvel Strategies
Member of Faculty, SANS Institute
Co-founder and Advisory Board Member, CCSIE

JHerbeck@NouvelStrategies.com

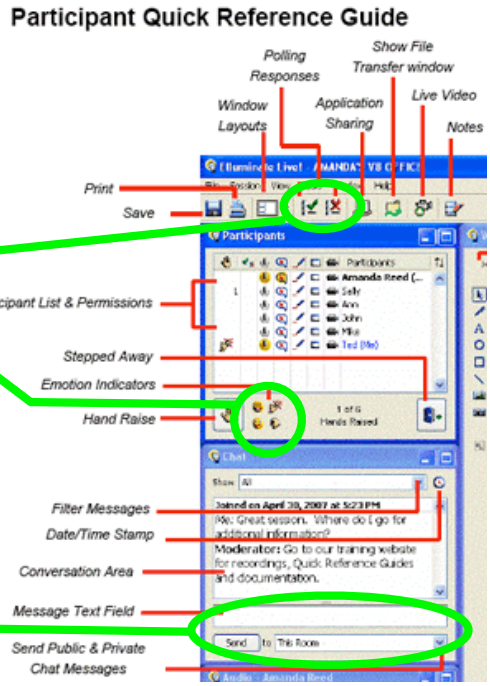
SANS Webcast archive:
https://www.sans.org/webcasts/managing-system-related-risk-smes-95141

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

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

Welcome to the webcast!

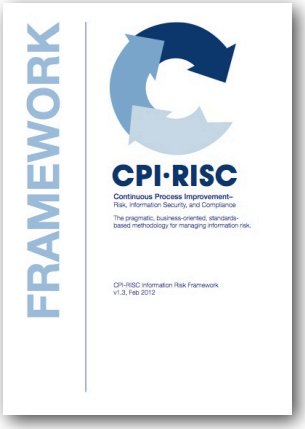
- Java-based Elluminate platform
  - audio, whiteboard, interaction
- Interaction
  - polling: answer questions
  - emoticons: provide feedback
  - chat: ask questions
- After the webcast
  - replay webcast archive
  - download handout



Agenda

- Defining system-related risk
- Likelihood and severity for SMEs
- Controlling system-related risk for SMEs
- Final words

Where can you find a pragmatic, business-oriented, standards-based list of system-related risk?

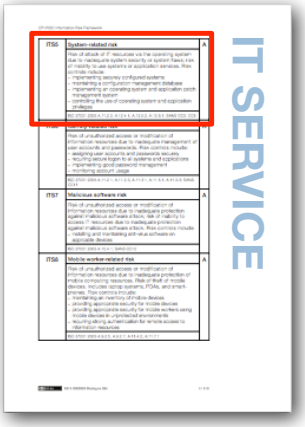


CPI-RISC* Information Risk Framework

- based on ISO 27001, ISO 27002, and SANS 20 Critical Security Controls (v3.0)
- originally released in 2010
- defines 33 risk areas, organized into 7 business functions:
  - management
  - legal
  - finance
  - purchasing
  - personnel
  - facilities
  - IT
- http://cpi-risc.org/

* CPI-RISC: Continuous Process Improvement–Risk, Information Security, and Compliance

CPI-RISC* Information Risk Framework: ITS5 summarizes system-related risk



Based on ISO 27001, ISO 27002, and SANS 20 Critical Security Controls (v3.0)

- A.11.2.2 (ISO 27001) or 11.2.2 (ISO 27002)
- A.12.4.1 (ISO 27001) or 12.4.1 (ISO 27002)
- A.12.5.2 (ISO 27001) or 12.5.2 (ISO 27002)
- A.12.6.1 (ISO 27001) or 12.6.1 (ISO 27002)
- SANS CC3
- SANS CC8

* CPI-RISC: Continuous Process Improvement–Risk, Information Security, and Compliance

Summarized for civilians: System-related risk

As a result of inadequate system security or system flaws:

- the risk of the loss of confidentiality or integrity of information resources
- the risk of the inability to use systems or application services

Controls for reducing system-related risk

- implementing securely configured systems
- maintaining a configuration management database
- implementing an operating system and application patch management system
- controlling the use of operating system and application privileges

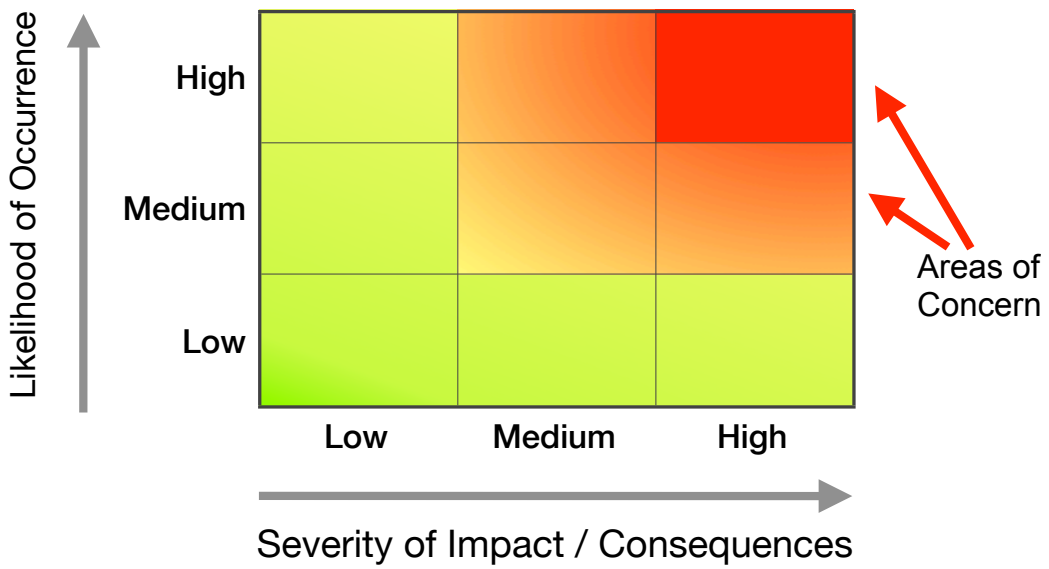
What criteria are used to categorize system-related risks?

- attack vector:
  - risks associated with system-based attacks
- responsible person/third party:
  - risks managed by system manager/system service provider
  - desktop and server systems might be managed separately
- control type:
  - risks managed with operating system software, patches, and configuration
- doesn't include:
  - malicious software risk (controlled with anti-virus software)

Agenda

- Defining system-related risk
- Likelihood and severity for SMEs
- Controlling system-related risk for SMEs
- Final words

Why do we care about likelihood and severity?



What's the most serious system-related risk?

- unauthorized access of information resources via the operating system (assume the network was hacked or the attacker has system console access):
  - could compromise confidentiality
  - could compromise integrity
  - could compromise availability
- advanced persistent threat (APT)
  - undetected, unauthorized access over a potentially long period of time

Realistically, what's the impact for an SME?

- direct loss: financial
  - finance application could be manipulated
    - fraudulent invoices could be created and paid.
- indirect loss: embarrassment, loss of reputation, loss of customers, loss of income, legal penalties, SLA / contractual problems
  - customer information could be stolen
  - application services could be modified (website defaced)
  - system services could be interrupted (server crash)
  - users could be impersonated (fraudulent email sent)

Agenda

- Defining system-related risk
- Likelihood and severity for SMEs
- Controlling system-related risk for SMEs
- Final words

What are the steps for controlling any risk?

1. Identify the risk.
2. Determine the risk management decision and define the control objectives.
3. Select controls to be used for achieving control objectives.
   - Choose a variety of control types.
4. Develop the plan for implementing controls.
   - Implementation plan may span multiple years.

Steps 1, 2, and 3: Controlling system-related risk

1. Identify risk	– risk: attack via the operating system
2. Define decision / control objective	– decision: to prevent attacks – control objective: to reduce the likelihood and severity of attack via the operating system
3. Select controls	– implement a system policy – implementing securely configured systems – maintaining a configuration management database – implementing an operating system and application patch management system – controlling the use of operating system and application privileges

Implementing a System Policy*

[administrative/preventive control]

To reduce the likelihood and severity of attack via the operating system:

- Securely configured systems shall be implemented (using a standard operating environment (SOE)).
- A configuration management database shall be maintained.
- An operating system and application patch management system shall be implemented.
- The use of operating system and application privileges shall be controlled.

* System Policy: system-related portion of the information security policy

Implementing securely configured systems
[technical/preventive control]

- A system manager or system service provider should design and implement the organization's Standard Operating Environment (SOE):
  - specify the versions of all operating system and application software
  - determine security requirements for all applications and systems
  - specify the appropriate use of:
    - operating system warning banners
    - operating system security features (e.g. disk encryption)
    - operating system access controls (e.g. default permissions)
    - file integrity tools to detect unauthorized system changes
- The SOE should be documented.

Using a Standard Operating Environment (SOE)
[administrative/preventive control]

- A documented list of all software required for business purposes (to support business processes).
  - if it's not in the SOE, it's not on the system
- SOE's are complicated to implement politically, but relatively easy to implement technically:
  - Windows 7 AppLocker allows further restrictions, by controlling what applications individual users can use.
- Good resource for SMEs: the Center for Internet Security benchmarks.

  http://www.cisecurity.org/

Maintaining a Configuration Management Database (CMDB)

[technical/preventive]

- A system manager or system service provider should maintain a Configuration Management Database (CMDB) of all systems and their current software configurations:
  - changes to systems should be updated in the CMDB
- A CMDB can improve security incident response
  - systems with vulnerable software or configurations can be quickly identified

Implementing an operating system and application patch management system

[technical/preventive, technical/detective]

- A system manager or system service provider should manage technical vulnerabilities in operating system and application software.
  - vulnerabilities identified by vendors (and others) should be evaluated and, if necessary corrected
- Patch management infrastructure should be used to manage the acquisition, testing, and distribution of operating system and application patches.
  - patch management software should keep logs of where patches have been installed
  - patch management software should update the CMDB

Controlling the use of operating system and application privileges

[technical/preventive, technical/detective]

- A system manager or system service provider should ensure the limited use of “privilege”:
  - only give access to privileged accounts (Unix root account, Windows administrator account) to individuals who need privileged access to do their jobs
  - avoid giving local root/administrator access to anyone
  - avoid giving full privilege when it may be possible to give partial privilege (using the Unix sudo command, Windows user rights)
- Log and monitor the use of privilege.

Note: the worst abusers of privilege are typically in the IT Department

Summarized for civilians: Controlling system-related risk

1. Write a System Policy.
2. Proactively plan for secure systems and applications:
   - Define role for system management (internal/external).
   - Define and document security requirements for systems and applications.
   - Define a Standard Operating Environment (SOE):
3. Implement secure systems and applications:
   - Implement secure systems and applications, based on your SOE.
   - Maintain a Configuration Management Database (CMDB), to document your secure configuration.
   - Implement a patch management system, to manage vulnerabilities in operating system and application software.
   - Implement file integrity tools to detect unauthorized system changes.
4. Control IT staff (internal/external) by limiting and monitoring the use of privilege.

Reviewing the control matrix: Has anything been missed?

	Administrative	Technical	Physical
Preventative	✔	✔	[site security policy]
▸ Deterrent	✔	✔	[site security policy]
Detective	✔	✔ [log monitoring]	[site security policy]
Corrective	[incident plan]	[backup system] (partial restore)	[site security policy]
▸ Recovery	[DRP plan]	[backup system] (full restore)	[site security policy]

Step 4: Developing multi-year implementation plan

- Determine how many years your implementation plan will span.
- Based on constraints, plan what to implement each year:
  - implement preventive controls first
- Don't forget verifying control effectiveness:
  - vulnerability assessment tools can verify the existence of technical vulnerabilities
  - the Center for Internet Security has benchmark scoring tools that can verify secure configurations

Agenda

- Defining system-related risk
- Likelihood and severity for SMEs
- Controlling system-related risk for SMEs
- Final words

What about Host-based Intrusion Detection?

- host-based Intrusion Detection Systems (HIDS) include:
  - file integrity monitoring
  - log file monitoring
  - network port monitoring
- HIDS is an advanced technology that can reduce system-related risk

HIDS is split over several CPI-RISC risk areas

- File integrity monitoring:
  - system-related risk
- Log file monitoring:
  - operational integrity and availability risk
    (most data centers have tools to aggregate and monitor system logs)
- Network port monitoring:
  - malicious software risk
    (most anti-virus software is now providing some forms of "endpoint" protection...)

Upcoming Webcasts for SMEs

Jun, 2012	Managing Third Party Risk for SMEs
Jul, 2012	Managing Malicious Software Risk for SMEs
Aug, 2012	Managing Employee Risk for SMEs

Managing System-related Risk
for SMEs

SANS Information Security Webcast

15 May 2012
Geneva, Switzerland

version 1b

Jim Herbeck
Managing Partner, Nouvel Strategies
Member of Faculty, SANS Institute
Co-founder and Advisory Board Member, CCSIE

JHerbeck@NouvelStrategies.com

SANS Webcast archive:
https://www.sans.org/webcasts/managing-system-related-risk-smes-95141

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

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