Writing Information Security Policy

for SMEs

SANS Information Security Webcast

21 Feb 2012
Geneva, Switzerland

version 1d

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

Member of Faculty, SANS Institute
JHerbeck@sans.org

SANS Webcast archive:
https://www.sans.org/webcasts/writing-information-security-policy-smes-94939

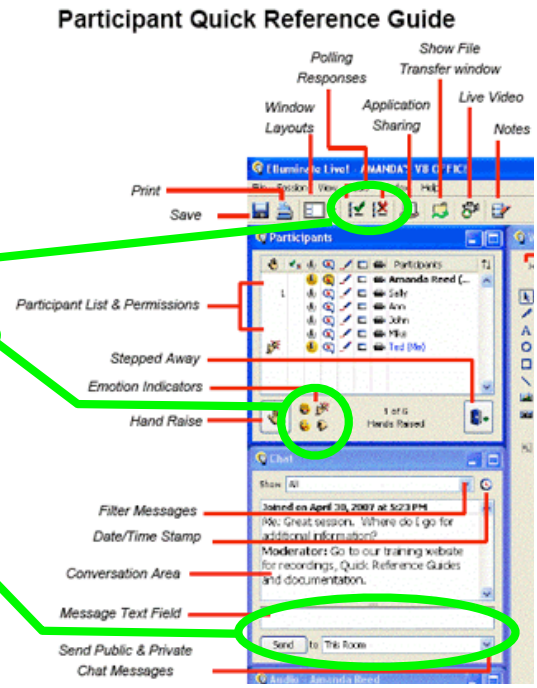
Slide handout (English):
http://nouvelstrategies.com/InfoSec-for-SMEs

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

NOUVEL

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

- Initial words
- Information security documentation
- Recognizing bad security policy
- Writing good security policy
- Final words

SME/SMB sizing and security

- When a European says SME:
  - Small and Medium Enterprise
  - fewer than 250 employees
- When an American says SMB:
  - Small and Medium Business
  - fewer than 500 employees
- SME/SMBs exist in many different sizes

Does SME size matter when considering information security?

- A medium-sized manufacturing enterprise (250 employees) could have a primitive IT environment:
  - If IT infrastructure has a security/availability problem, it doesn't affect the manufacturing/logistics capability.
- A small-sized financial services enterprise (50 employees) could have a sophisticated IT environment:
  - If IT infrastructure has a security/availability problem, it's a catastrophe for the banking/trading capability.
- Size is not a good indicator of SME security requirements.

IT level of sophistication is a better indicator for the overall level of information risk.

IT Sophistication	Low	Medium	High
Locations	1	~2-3	~3+
Servers	1	~2-3	~3+
Workstations	~1-15	~15-30	~30+
Networks	COTS	Nonstandard or >1	Multiple/WAN
Applications	COTS	Some customizing	ERP and/or customized
Emerging/advanced IT	None - few	Few - moderate	Moderate - many
Online transactions	None	Few	Many
Third party providers	1	~2-3	~3+

from "The Minimum IT Controls to Assess in a Financial Audit," the ISACA Journal, 2010, Vol 1

IT level of sophistication can be used to help define minimum security requirements.

- IT level of sophistication can be used as an indicator of information risk:
  - Higher risk could necessitate more information security.
  - Lower risk could necessitate less information security.
- IT level of sophistication was originally defined in the article “The Minimum IT Controls to Assess in a Financial Audit” in the ISACA Journal, 2010, Vol 1

  http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/1001-the-minimum-IT.pdf

Agenda

- Initial words
- Information security documentation
- Recognizing bad security policy
- Writing good security policy
- Final words

There are many types of information security documents.

Policy:	rules and regulations
Standard:	list of general requirements (mandatory)
Baseline:	list of detailed requirements (mandatory)
Guideline:	list of requirements (optional)
Procedure:	step-by-step instructions

The purpose of information security policy is to document a risk management decision.

Policy should:

1. Identify the specific risk being managed.
2. State the risk management decision:
   - Reduce (mitigate), retain (accept), transfer, or avoid.
   - Specify the “control objective” to be achieved.
3. Provide guidance on how risk is to be managed:
   - High-level specification of “controls” to be used to achieve the control objective (as necessary).

Policy by objective

Create information security policy that is descriptive, not prescriptive.

- Descriptive policy: states what is the desired outcome (the control objective).
- Prescriptive policy: states how to reach the desired outcome.
- Descriptive policy is more concise, easier to read, to understand, and to implement.
  - Is potentially more difficult to audit.

Security controls, organized by category

Function	Description
Administrative	Decisions by management, personnel, legal, or purchasing. Also includes developing policies, standards, policies, or processes.
Technical	Activities involving computer hardware, software, applications, or network infrastructure.
Physical	Badges, gates, locks, alarms, or guards.

Security controls, organized by action

Action	Description
Preventative	To stop the occurrence of undesirable events.
‣ Deterrent	To discourage the occurrence of unwanted events.
Detective	To notice the occurrence of undesirable events.
Corrective	To respond to the occurrence of undesirable events.
‣ Recovery	To restore after damage caused by the occurrence of undesirable events.

Security control matrix

	Administrative	Technical	Physical
Preventative	•	•	•
‣ Deterrent	•	•	•
Detective	•	•	•
Corrective	•	•	•
‣ Recovery	•	•	•

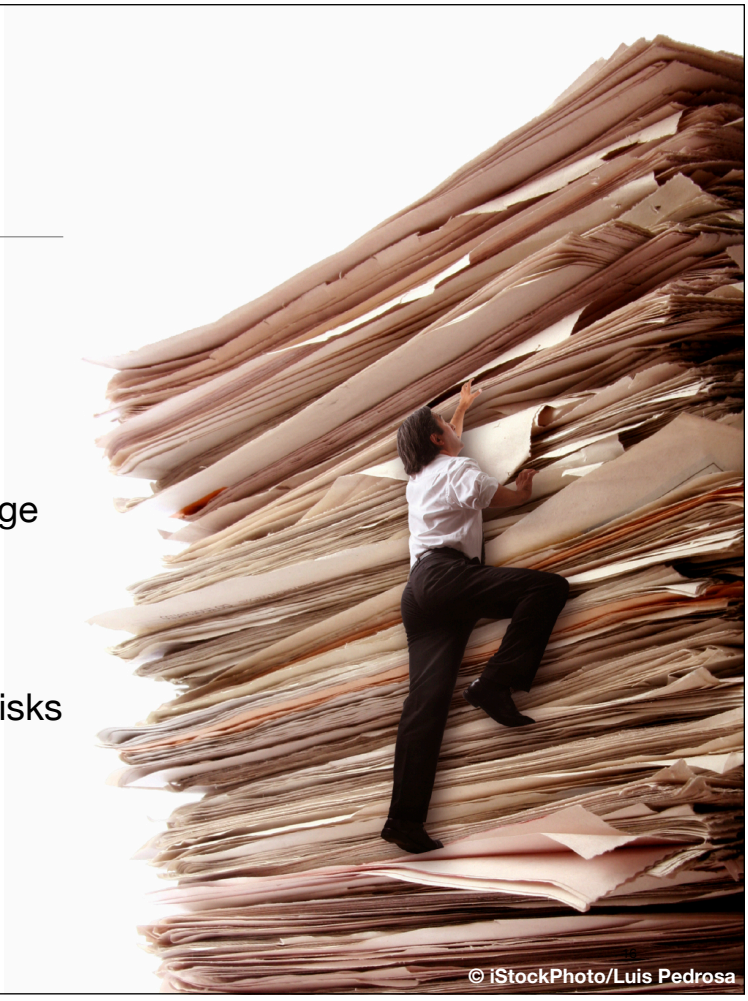
Agenda

- Initial words
- Information security documentation
- Recognizing bad security policy
- Writing good security policy
- Final words

What does bad security policy look like?

- Thick
  - many pages
- Difficult to understand
  - uses jargon/legal language
- Out-of-date
  - not updated for new systems, technologies, risks

If nobody has ever read the policy, does it improve information security?



Agenda

- Initial words
- Information security documentation
- Recognizing bad security policy
- Writing good security policy
- Final words

What does good policy look like?

- Brief
  - as few words as possible
- Easy to understand
  - uses language that's consistent with business culture
- Up-to-date
  - relevant for current systems, technology
- Policy by objective
  - an appropriate policy style for SMEs

Policy by objective: Information security policy in 3 easy steps

1. Identify risk	Identify the specific information risk being managed.
2. State decision / control objective	State the risk management decision: - Reduce, retain, transfer, or avoid. - Specify the control objective.
3. Provide guidance for potential controls (optional)	Provide guidance on how risk is to be managed: - Specify high-level controls (optional).

Policy by objective: Worksheet for network-related risk

1. Identify risk	– risk: attack via the network
2. State decision / control objective	– decision: to prevent attacks – control objective: to reduce the occurrence and severity of attack
3. Provide guidance for potential controls (optional)	– implement a securely designed network – implement a securely designed wireless network – implement a securely designed network perimeter – use secure network device configurations – prevent unauthorized access to network services

Network policy

To reduce the occurrence and severity of attack via the network:

- A securely designed network shall be implemented.
- A securely designed wireless network shall be implemented.
- A securely designed network perimeter shall be implemented.
- Secure network device configurations shall be used.
- Access controls shall be used to prevent unauthorized access to network services.

Policy by objective: Worksheet for site-related physical risk

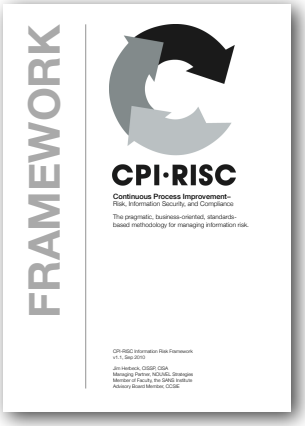
1. Identify risk	– risk: theft of information assets from business locations
2. State decision/ control objective	– decision: to prevent theft – control objective: to reduce the occurrence and severity of theft, to identify and apprehend thieves
3. Provide guidance for potential controls (optional)	– define a physical security perimeter – install and maintain keyed or electronic door locks – require workers and visitors to wear identification badges – maintain a physical or electronic access log – protect business locations from external and environmental threats – ensure delivery and loading areas are secure

Site security policy

To reduce the occurrence and severity of theft from business locations and to identify and apprehend thieves:

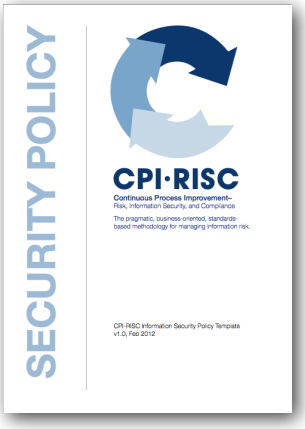
- A physical security perimeter shall be defined.
- Keyed or electronic door locks shall be installed and maintained.
- Workers and visitors shall be required to wear identification badges.
- A physical or electronic access log shall be maintained.
- Business locations shall be protected from external and environmental threats.
- Secure delivery and loading areas shall be maintained.

From previous webcast: CPI-RISC Information Risk Framework



- originally released in 2010
- defines 33 risk areas
- organized into 7 business functions:
  - management
  - legal
  - finance
  - purchasing
  - personnel
  - facilities
  - IT
- based on ISO 27001 and SANS 20 Critical Security Controls
- http://cpi-risc.org/en/CPI-RISC.html

CPI-RISC Information Security Policy Template



- published this week
- defines 33 security policies
- organized into 7 business functions:
  - management
  - legal
  - finance
  - purchasing
  - personnel
  - facilities
  - IT
- based on ISO 27001 and SANS 20 Critical Security Controls.
- http://cpi-risc.org/en/CPI-RISC.html

Network policy from CPI-RISC Information Security Policy Template

	Network policy
ITS4	To reduce the occurrence and severity of attack via the network: - A securely designed network shall be implemented. - A securely designed wireless network shall be implemented. - A securely designed network perimeter shall be implemented. - Secure network device configurations shall be used. - Access controls shall be used to prevent unauthorized access to network services.
	ISO 27001:2005 A.10.6.1, A.10.6.2, A.11.4.1, A.11.4.5, A.11.4.6, A.11.4.7; SANS CC4, CC5, CC13, CC14, CC16

Site security policy from CPI-RISC Information Security Policy Template

FAC1	**Site security policy**
	To reduce the occurrence and severity of theft from business locations and to identify and apprehend thieves: - A physical security perimeter shall be defined. - Keyed or electronic door locks shall be installed and maintained. - Workers and visitors shall be required to wear identification badges. - A physical or electronic access log shall be maintained. - Business locations shall be protected from external and environmental threats. - Secure delivery and loading areas shall be maintained.
	ISO 27001:2005 A.9.1.1, A.9.1.2, A.9.1.4, A.9.1.6

Agenda

- Initial words
- Information security documentation
- Recognizing bad security policy
- Writing good security policy
- Final words

Good policy needs to be kept up-to-date.

- When was the last time your policy was reviewed?
  - Look for old sections that are no longer relevant and need to be removed.
- Is your policy keeping pace with emerging technology?
  - Social networking?
  - Portable media?
  - Smartphones?
  - Factory automation systems?

Information security policy resources

Policy by objective resources:

- CPI-RISC Information Security Policy Template

  http://cpi-risc.org/en/CPI-RISC.html

Traditional policy resources:

- SANS Information Security Policy Project

  http://www.sans.org/security-resources/policies/

- Information Security Policy Development Guide

  http://www.sans.org/reading_room/whitepapers/policyissues/information-security-policy-development-guide-large-small-companies_1331

- UK BERR: How to write an information security policy

  http://www.bis.gov.uk/files/file49963.pdf

Upcoming Webcasts for SMEs

Mar, 2012	Managing Network-related Risk for SMEs
Apr, 2012	Managing Legal, Regulatory, and Compliance Risk for SMEs
May, 2012	Managing System-related Risk for SMEs

Writing Information Security Policy

for SMEs

SANS Information Security Webcast

21 Feb 2012
Geneva, Switzerland

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

Member of Faculty, SANS Institute
JHerbeck@sans.org

SANS Webcast archive:
https://www.sans.org/webcasts/writing-information-security-policy-smes-94939

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

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