Metrics for Organizational Cybersecurity Practices

Benjamin C. Dean
Consultant to OECD Secretariat

Metricon X
Stevens Institute of Technology
Jersey City, NJ, USA

March 22, 2019

Agenda

- The problem
- OECD project overview
- Framework
- Lessons + recommendations
- Q&A

Benjamin C. Dean
@benjamindean | ben@iconoclast.tech

The Problem: unanswerable questions

Cybercrimes against businesses, US Dept. of Justice, 2005

Table 15. Most frequent computer security vulnerabilities, by type of incident, 2005

Inadequate security measure	Type of incident: All incidents	Cyber attack	Cyber theft	Other
Anti-virus software	62%	66%	10%	38%
Anti-spyware/anti-adware	47	36	10	62
Internal controls	31	28	29	24
E-mail logs and filters	27	24	10	27
Firewall	26	25	9	22
Personnel policy	24	19	34	22
Misuse of authorized access	18	11	46	15
Number of businesses*	4,525	3,899	718	1,544

Note: Number of businesses may sum to more than total because businesses could detect more than one type of incident. Detail may sum to more than 100% because respondents could provide multiple vulnerabilities.

*Represents the number of businesses that detected incidents and provided information on security inadequacies.

The Problem: laundry lists

ABACUS survey, Australia, 2009

26 What type of computer security related policies did your business have during the 12-month period ending 30th June 2007?

(Cross all that apply)

Refer to glossary

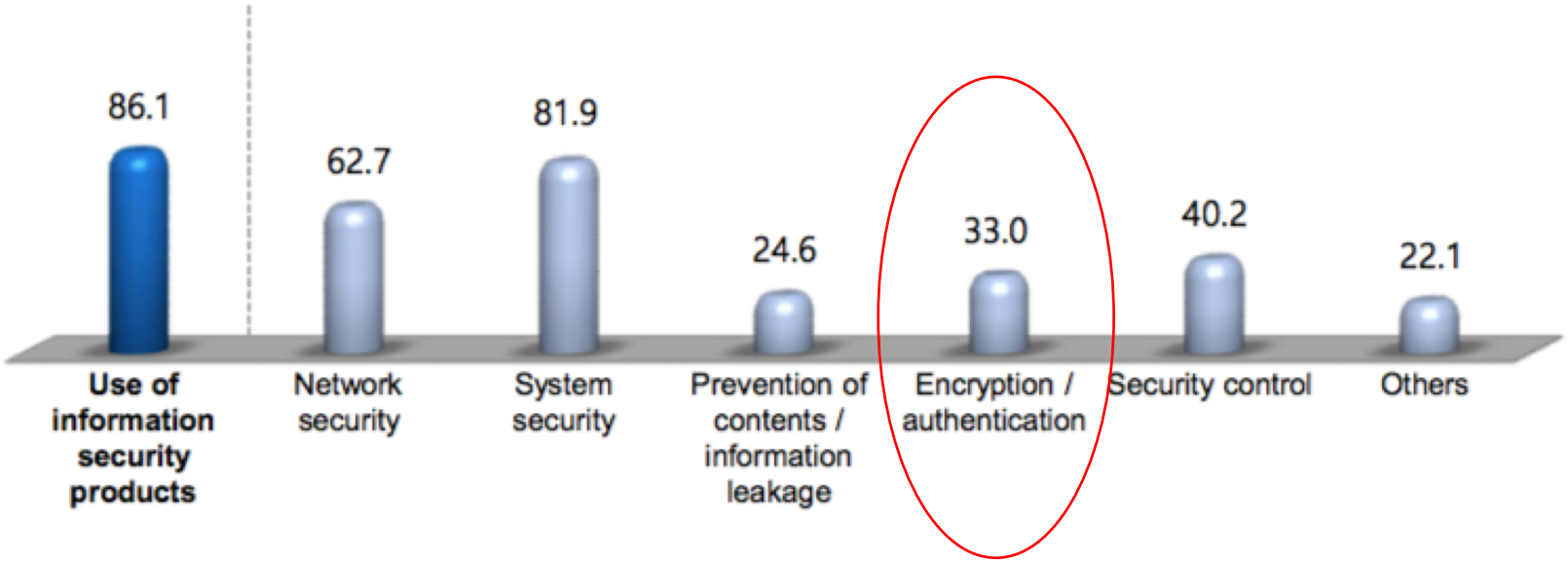
Did not have any computer security policies	☐ → Go to Q28
Staff/user related policies	
Employee education and awareness program	☐
Segregation of duties	☐
System content monitoring	☐
Wireless technology acceptable use policy	☐
IT acceptable use policies	☐
Mobile policies (such as mandatory encryption of data stored on mobile devices)	☐
User access management	☐
Background checks	☐
Mandatory reporting of misuse / abuse of computer equipment	☐
Documented standard operating procedures	☐
Monitor internet connections	☐
Account / password management policies	☐
Staff / user related policy used but unable to specify	☐
Other (Specify)	☐
Security testing policies	
System penetration testing	☐
System audit policies	☐
Risk assessment policies	☐
Security testing policy used but unable to specify	☐
Other (Specify)	☐

Continued over page.....

The Problem: not technically informed

Survey on information security in businesses, Korea, 2015

[Figure 7] Utilization of Information Security Products (Multiple Responses, %)



The Problem: poorly worded concepts

Community survey on ICT usage and e-commerce in enterprises, Eurostat, 2019

E8.	**Does your enterprise have insurance against ICT security incidents?**	Yes☐	No☐

Benjamin C. Dean
@benjamindean | ben@iconoclast.tech

Project overview

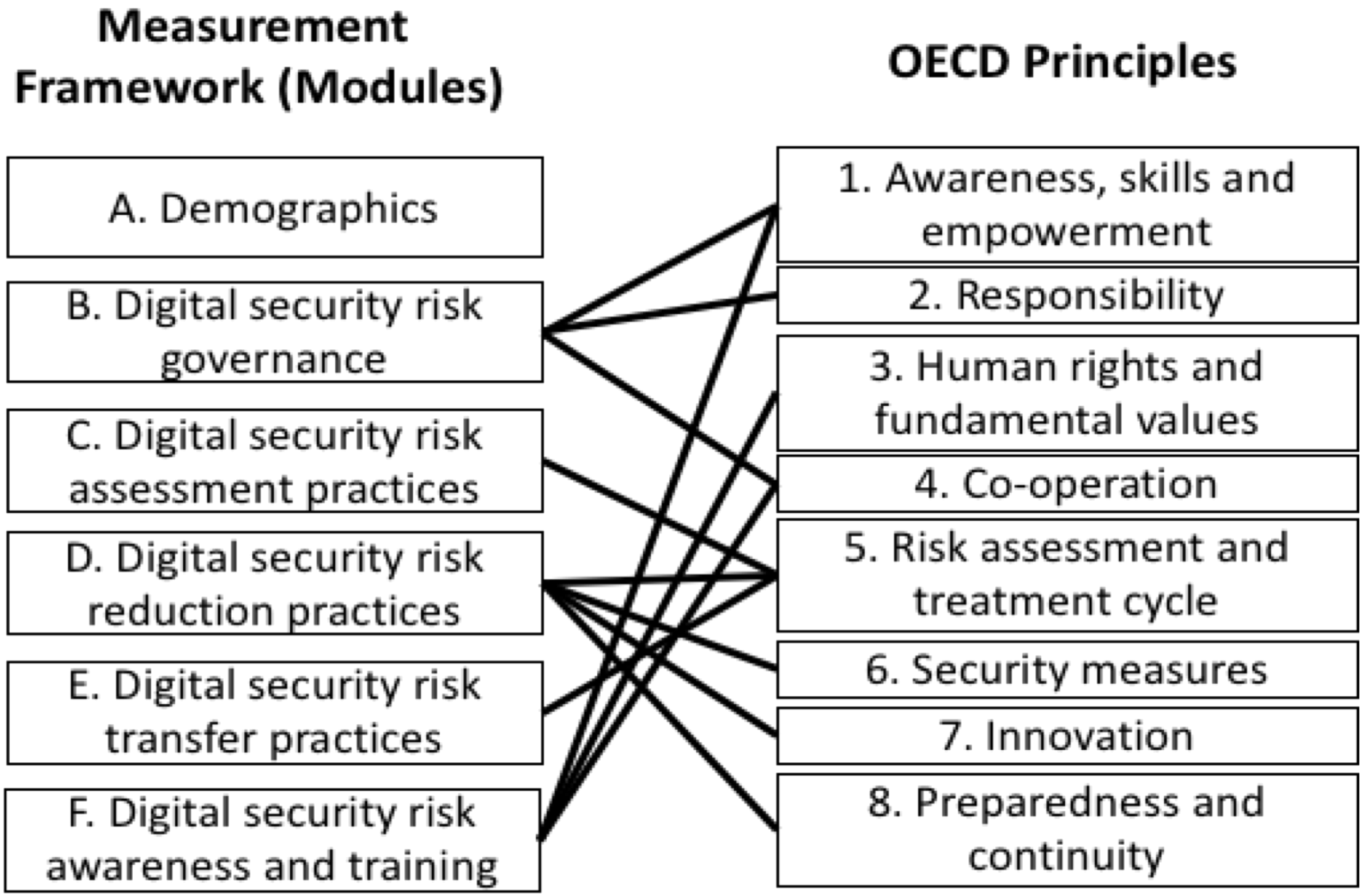
- **Goals**: Establish a measurement framework of digital security risk management practices (particularly SMEs)
- **Make it**:
  - Conceptually clear
  - Succinct
  - Organisational – not technical
  - Focus on what is done i.e. practices
  - Relevant to policymakers

Benjamin C. Dean
@benjamindean | ben@iconoclast.tech

Project overview

- **Timeline**: 2-year project
- **Audience**: policymakers, national statistical offices, insurers
- **Final report** (soon to be published):
  - Section 1: methodological issues
  - Section 2: the measurement framework
  - Section 3: pilot results
  - Recommendations

Framework built on OECD principles



Short framework explanation

- Six modules with eighteen indicators
- Uses OECD “model survey” framework
  - **Governance** – who is in charge, how are decisions made, do you communicate internally?
  - **Risk assessment** – what do you do to assess your risks?
  - **Risk treatment**:
    - **Risk reduction** – what do you do to reduce your risks? Is it informed by risk assessment?
    - **Risk transfer** - what do you do to transfer your risks? Why?
  - **Risk awareness & training** – what do you do to raise awareness and teach people about managing their digital risk exposure?
- See appendix for full framework

Benjamin C. Dean
@benjamindean | ben@iconoclast.tech

Lessons learned + recommendations

Cognitive testing and pilot yielded insights

1. Further reduce number of indicators
2. Simplify language
3. Move toward maturity model
4. Better assess the ‘depth’ of practices

Benjamin C. Dean
@benjamindean | ben@iconoclast.tech

ANNEXES

The full framework (1)

Module/ Indicator	Description
A	**DEMOGRAPHICS**
A1	Proportion of enterprises by geographic location
A2	Proportion of enterprises by size
A3	Proportion of enterprises by economic activity
A4	Proportion of enterprises by turnover
A5	Proportion of enterprises by digital intensity
B	**DIGITAL SECURITY RISK GOVERNANCE**
B1	Proportion of enterprises that have responsibilities for digital security risk allocated to a specific role within the organisation
B2	Proportion of enterprises that have a policy in place to manage digital security risk
B3	Proportion of enterprises that have a process in place to monitor and review digital security risk management
B4	Proportion of enterprises that had structures or processes in place to enable cooperation and for reporting on digital security risk management within the enterprise

The full framework (2)

Module/ Indicator	Description
C	**DIGITAL SECURITY RISK ASSESSMENT PRACTICES**
C1	Proportion of enterprises that assess digital security risk as part of the overall enterprise risk management
C2	Proportion of enterprises that regularly take specific actions as part of the digital security risk assessment
D	**DIGITAL SECURITY RISK REDUCTION PRACTICES**
D1	Proportion of enterprises that took risk reduction measures
D2	Proportion of enterprises that share information on threats, vulnerability, incidents and risk management practices or security measures
C	**DIGITAL SECURITY RISK ASSESSMENT PRACTICES**
C1	Proportion of enterprises that assess digital security risk as part of the overall enterprise risk management
C2	Proportion of enterprises that regularly take specific actions as part of the digital security risk assessment

The full framework (3)

Module/ Indicator	Description
E	**DIGITAL SECURITY RISK TRANSFER PRACTICES**
E1	Proportion of enterprises that use insurance to transfer digital security risk
E2	Proportion of enterprises that did not purchase an insurance policy, by reason for non-adoption
E3	Proportion of enterprises that transfer digital security risks through an insurance policy, by type of risks transferred
E4	Proportion of enterprises that adopt other risk transfer practices
F	**DIGITAL SECURITY RISK MANAGEMENT AWARENESS AND TRAINING**
F1	Proportion of enterprises that adopted awareness-raising and training practices on digital security risk management