IMF 2013

Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management

Karin Bernsmed and Inger Anne Tøndel, SINTEF ICT

Presented by Inger Anne Tøndel

Kaspersky lab – Global IT Security Risks: 2012

(survey: more than 3 300 senior IT professionals from 22 countries)

"cyber-threats (…) were seen as the second biggest danger to business"

Businesses Facing Increasing Cyber Threats: Security Experts

Text Size

2013 | 7:08 AM ET

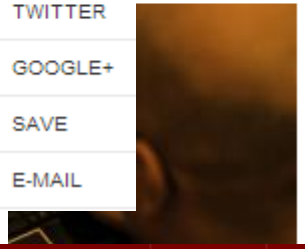
FACEBOOK witter 67 +1 0 LinkedIn 18 Share

TWITTER

GOOGLE+

SAVE

E-MAIL



Disastrous cyber-war attacks that could be life threatening are not far off if the government and businesses do not take action soon, security experts warned Wednesday at the Kaspersky Cyber-

Obama Order Gives Firms Cyberthreat Information

By MICHAEL S. SCHMIDT and NICOLE PERLROTH
Published: February 12, 2013

WASHINGTON — President Obama signed an executive order on Tuesday that promotes increased information sharing about cyberthreats between the government and private companies that oversee the country's critical infrastructure, offering a weakened alternative to legislation the administration had hoped Congress would pass last year.

TECHNOLOGY

Addressing the cyber sec

It's time for cyber defence to be acknowledged

TAGS: board-level, cyber security, cybercrime, IT risks, M

BBC News Sport Weather Travel Future Auto

NEWS UK POLITICS

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environ

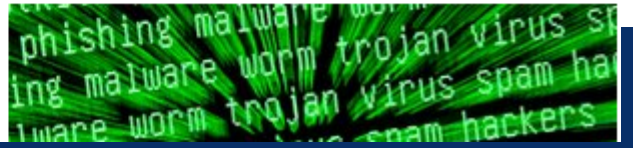
England Northern Ireland Scotland Wales UK Politics Education

Share

12 February 2013 Last updated at 09:38 GMT

National Audit Office warns UK needs more skilled cyber-crime fighters

A lack of skilled workers is hampering the UK's fight against cyber crime, the National Audit Office (NAO) has warned.



SINTEF

Organisations must expect to be attacked, and must be prepared that their systems will eventually be compromised.

Resilience

- Capability of recognizing, adapting to and coping with the unexpected (Woods)
- The intrinsic ability of an organisation/system to maintain or regain a dynamic stable state, which allows it to continue operations after a major mishap and/or the presence of a continuous stress (Hollnagel)
- Change of focus from avoiding that anything goes wrong to ensuring that everything goes right (Hollnagel)

You can't manage what you don't measure!

Current status: Measuring incident response for ICT

- Information security metrics – subject to research, suggested by standards organisations, used by businesses
  - The presence of and adherence to plans
  - Incident statistics
  - Detection and response statistics
  - Consequences
  - Incident management cost and performance
  - Culture and learning aspects

- Observation: Lack of methods for evaluating an organization's ability to take a proactive approach to incident management

The REWI method

- Resilience-based Early Warning Indicators
- A collection of self-assessment measures
- Successfully applied for evaluating resilience in the Norwegian petroleum exploration and production section, from a safety perspective

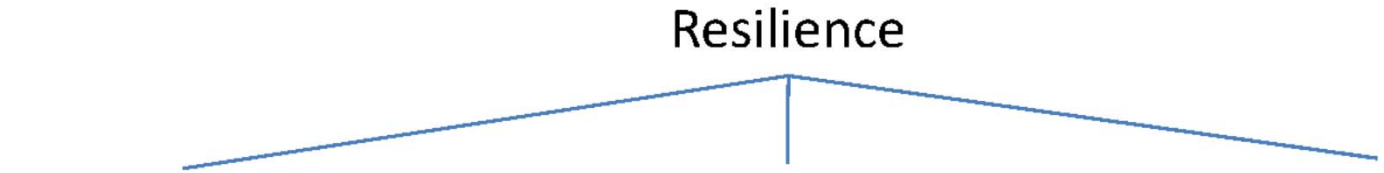
Resilience attributes

- **Risk awareness**
  - Degree of risk understanding, knowing what to expect and what to look for

- **Response capacity**
  - Ability to respond given an incident
    - Knowing what to do
    - Ability to withstand stress without suffering damage
    - Ability to respond timely and sufficiently

- **Support**
  - Presence of established support systems – in case of tough decisions/trade-offs
  - Ability to uphold critical support functions (technical, human and organizational)

Contributing success factors



Risk awareness

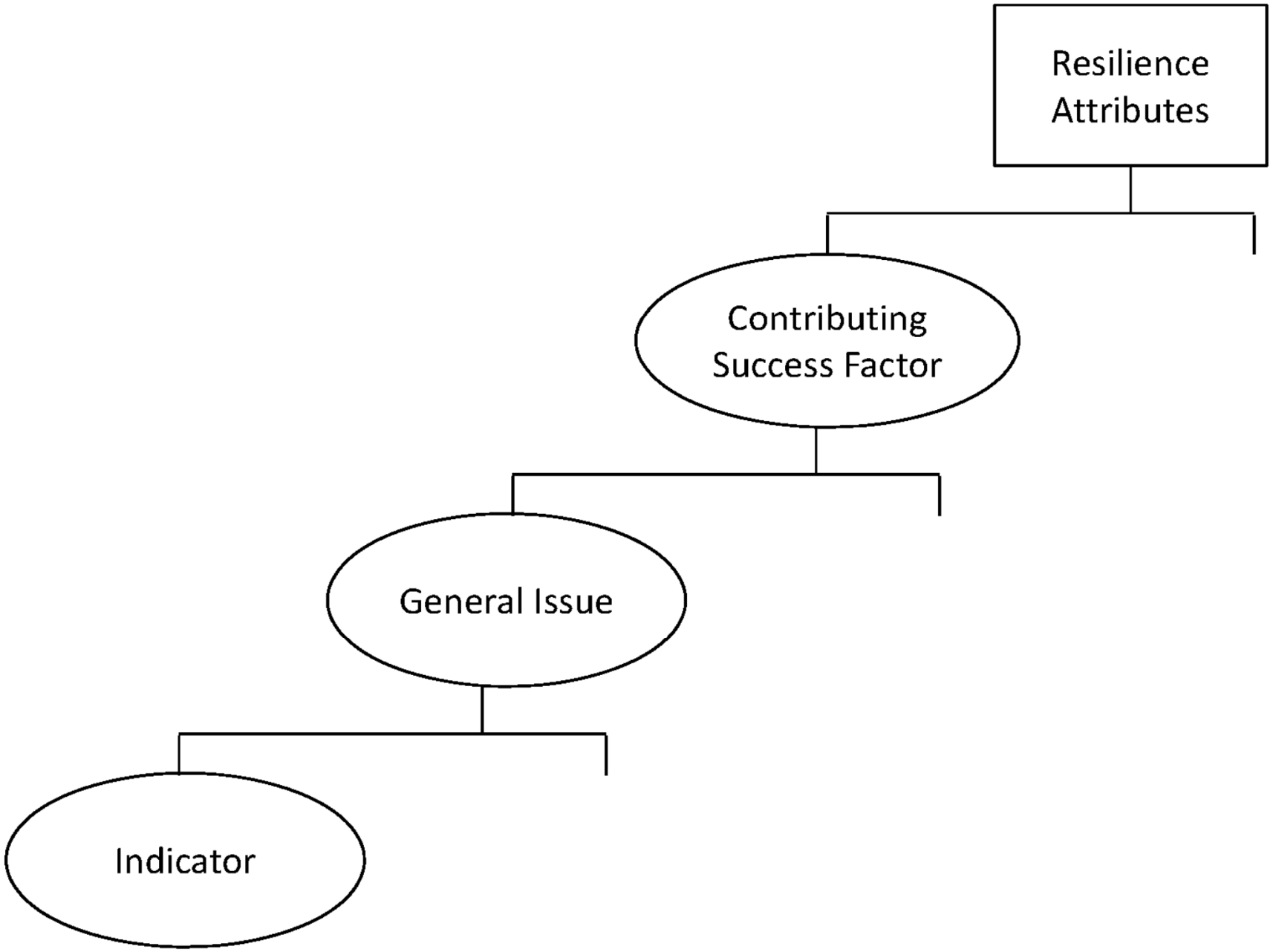
- Risk understanding
- Anticipation
- Attention

Response capacity

- Response
- Robustness of response
- Resourcefulness

Support

- Decision support
- Redundancy (of support)


Resilience Attributes
Contributing Success Factor
General Issue
Indicator

CSF: Risk understanding

- Do we have knowledge about the ICT system and its components?
- Do we have personnel with information security competence?
- Do we report on security incidents?
- Do we have appropriate defence mechanisms?
- Is the organisation's security policy efficient?

CSF: Anticipation

- Do we have updated knowledge about relevant threats?
- Do we learn from experience?

CSF: Attention

- Do we discover security incidents?
- Do we have appropriate audit mechanisms?
- Do the audit mechanisms work as intended?
- To what degree do users bypass security mechanisms?
- Are there any trends in reported security incidents?
- Are there any changes (organisational and technical) in the IT system?

CSF: Response

- Do we have personnel with the ability to handle incidents?
- How do we train on dealing with potential incidents?

CSF: Robustness of response

- Do we have sufficient redundancy in skills among the employees?
- Do we have sufficient backup capacity/redundancy for the necessary critical functions?
- Is the communication between involved actors sufficient?
- Do we manage incidents in compliance with existing policies?

CSF: Resourcefulness

- Does the incident response team have sufficient resources?
- Do we have adequate IT systems to support timely updating of necessary information?

CSF: Decision support

- Do we have adequate decision support staffing?
- Do we have adequate ICT decision support systems?
- Do we have adequate external support?

CSF: Redundancy of support

- Are critical decision support systems redundant?
- Are critical information systems redundant?

Table II: Candidate indicators for Anticipation: What security incidents we can expect.

RISK AWARENESS (1) - ANTICIPATION (1.2)		
No	**Name**	Ref
1.2.1	**Do we have updated knowledge about relevant threats?**	
1.2.1.1	Percentage of system that has been subject to risk analysis	-
1.2.1.2	The frequency with which risk analysis has been performed	-
1.2.1.3	Percentage of stakeholder groups that were represented during the risk analysis	[22]
1.2.1.4	Percentage of identified risks that have a defined risk mitigation plan	[22]
1.2.2	**Do we learn from experience (ours and others)?**	
1.2.2.1	Percentage of incidents that are a recurrence of previous incidents	[8]
1.2.2.2	Percentage of reported incidents that have been followed up and mitigated	-
1.2.2.3	Percentage of security incidents that exploited existing vulnerabilities with known solutions	[10], [11], [22]
1.2.2.4	Percentage of reported security incidents where the cause of the incident was identified	[8]
1.2.2.5	Percentage of identified corrective action that has not been implemented	[12]

Steps

1. Prepare the evaluation
2. Select the indicators
3. Implement the indicators and interpret the data
4. Review and update the indicators
5. Integrate the indicators with other self-assessment initiatives

Step 2: Select the indicators

- In the paper: 69 indicators
  - Business can also identify their own…
- Workshops with relevant stakeholders:
  - Workshop 1: review the concept of resilience, the CSFs, and the general issues
  - Workshop 2: select the indicators – no more than 10-20!

Metric		Target value	Observed value	Interpretation
ID	*Definition*			
2.1.2.1	The frequency with which training is conducted	Monthly	A few times a year	Yellow
2.1.2.4	Percentage of training scenarios last period which involved necessary external personnel	100%	25%	Red
…	…			

High score on an indicator: So are we resilient?

- Resilience lies in the combination of success factors, so that the organisation
  - is risk aware
  - has response capacity
  - has adequate support

Context of this work

- Research project IMMER – Information Security Incident Management and Emergency Preparedness in ICT-based operations
  - ICT-based operations: collaboration, sharing of information and decision-making across organisational and geographical borders supported by ICT

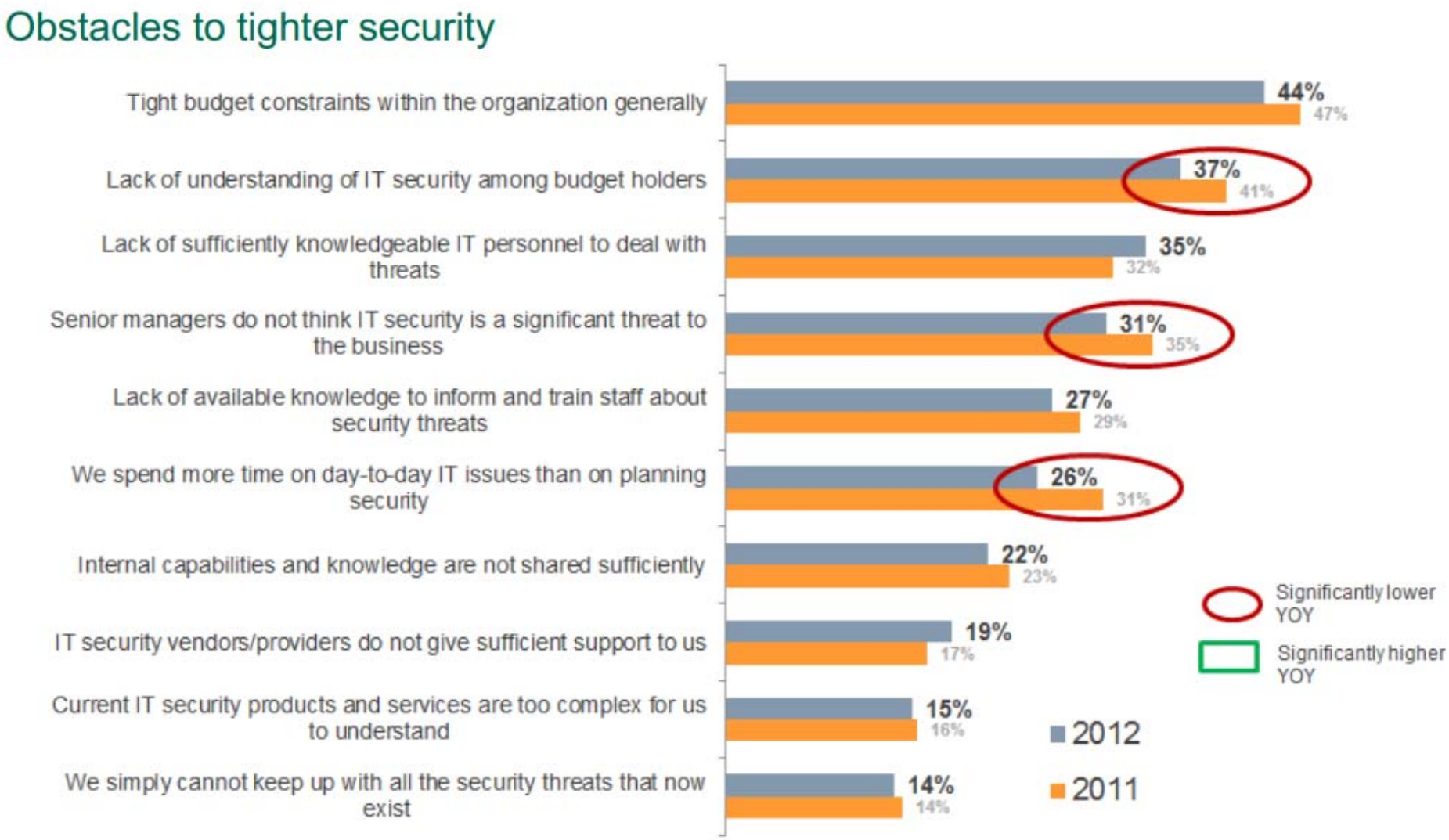
- Funded in part by the Research Council of Norway
- Project leader: IntraPoint
- Other industry partners: DOF Subsea, E-CO Energy, Statoil, SJ (Swedish Railroad), Shell

To sum up…

- Aim: Fill a gap in order to improve the ability to manage for resilience when it comes to ICT incidents
  - Adapted REWI method for dealing with information security
  - A systematization of "common sense"

Kaspersky lab – Global IT Security Risks: 2012

(survey: more than 3 300 senior IT professionals from 22 countries)



Thank you!

inger.a.tondel@sintef.no