Trends in Informationssicherheit

Prof. Dr. B. M. Hämmeli,
bmhaemmerli@bluewin.ch bhaemmerli@acris.ch
Trends in Information Security

1. Happy that the system runs / Optimizing availability before 1985 Feasibility
2. IT-Security = Encryption (Technicians problem) up to 1992 Hard Core Crypto Approach
3. IT Security is delegated to the Security Officer up to 1995 Task Delegation, not Risk!
4. IT Security is chief’s issue up to 1999 Risk Owner takes Responsibility
5. Process oriented IT Security up to 2002, QM Approach: At the end will be turn out well.
6. IT Security has its price. Therefore Security is suggested from the security officer and decided about from the business line manager: Risk Based / Risk Management Approach. Today still easier to fund line management funded and wanted security. “Commander in Charge Model”: benefit oriented, adaptation to actual risks from 2000
7. Corporations are low on money. Society feels not under potential threat. Reduction to laws & frameworks (governance & compliance issue). from 2003 Reduction to legal demands
Trends in Information Security

11. **2008 ongoing**: Operating under Attack. There is no attack free time. (early started in 2004)
12. **2010 ongoing**: Strategic efforts on SCADA security
14. **2012 ongoing**: Cloud Computing as enlarged outsourcing: no way of return. The role of CISO will - and must - be redefined! Organizational, legal, security cultural issues will dominate the security office. Loyalty must be redefined and improved: an ultimate challenge, in a more-and-more hire and fire environment.
16. **2014 ongoing**: Risked based security investments in CIIP, Cyber defense, SCADA-sec and “crown jewels”. Even so the need for security is recognized, the budget does not allow to react fast: Only few extra budget will be approved.
17. **2015 ongoing**: heavy investment into security research in SCADA, OS, confidentiality, CIIP, Cyber defence and attack: world competition on information dominance. US, RU, China, D, GB, F, Korea, Taiwan … compete. Multi-surveillance must be assumed …
18. Further more …
   Reshaping surveillance or revolution … Citizen will no more accept data space ruling (might occur before 2020)
   Simultaneously: Nationalization of IT, attempts to create political cyber boarders as e.g. China has done. VPN and Proxy? story
On Identity

Intro: who am I: Sketch on Identity

Key Questions

What is between you and your bank account today?

Identity: is all. Bank, Cell, Health, Computer & Devices, Smart meter etc.

Where we need to be identified, where we need to be anonymous?

Where we want to be in private in small groups?

What we want to store confidential, and where?
Netgear private NAS: Terms and Conditions

We use information as otherwise permitted by law.

We may share information with third parties.

We will share information within the NETGEAR family of companies. This includes VueZone, for example.

We may share information with third parties who provide services for us. For example, we share information with vendors who help us send emails and operate our websites. We also share information to fulfill your purchases.

We may share information with our business partners. For example, share information with our partners that run our applications.

We may share information with any successor to all or part of our business. For example, if all or part of our business was sold we may give our customer list as part of that transaction.

We will share information if we think we have to in order to comply with the law or to protect ourselves. For example, we will share information to respond to a court order or subpoena. We may also share it if a government agency or investigatory body requests. We might also share information when we are investigating potential fraud. We may share information for other reasons we may describe to you.

You have certain choices about our marketing and tracking tools.

You can opt out of receiving our marketing and promotional emails. To stop receiving our marketing and promotional emails, click here or follow the instructions in any marketing email you get from us. You can opt out of receiving marketing and promotional emails related to VueZone through your VueZone.com account. Don’t worry! Even if you opt-out of getting marketing emails, we will still be sure to send you important transactional messages. For example, we may still contact you about your orders. You will also continue to receive critical technical information about your NETGEAR products.

We do not share information with third parties for their independent marketing or promotional purposes.

You can control cookies and tracking tools. To learn how to control these, visit our About our Ads section below.

You can choose not to install our applications or fill out a warranty card. This choice may limit your warranty service.
Section 1: Motivation & Setting up the Scene

Pre-Introduction

Setting up the Scene:
Real Cases: What are next strategic periods challenges?
Catastrophic Cases
“People underestimate catastrophic risk.” Sibos 2011, John Trundle, managing director, risk management, Euroclear
Power blackout, nuclear waste, great disaster
What would be the impact of a Cyber Tsunami?
June 2008 the Georgian government was under cyber attack

The attack came from a vast amount of computers in many countries

Source: Master thesis presentation Margrete Raaum Nov-3-2011, University CERT Oslo
Setting up the Scene II

APT: Advanced Persistent Threats
Mandiant’s Attack Lifecycle Model for APT: Mandiant Study 2013

New Dimension of Threats: 140 + enterprises, average time of visit 11 month

*** No defense of Malware detectors ***

Largest APT1 data theft from a single organization:

6.5 Terabytes
over 10 months
Mandiant 2013: 141 APT’s: World wide …
Attacks from Chinese Army’s Hacking Unit 31398?

U.S. law to restrict government purchases of Chinese IT equipment
*Reuters, March 27, 2013*
E-banking Fraud
... physical drive by against counter measures ...
Parking lot University Bochum (picture Dirk Schadt)
Secure communication

but the end-device remains insecure

Challenge: Hardening multi-purpose computer with broad scale usage
Strong authentication is a pre-requisite, but not enough!!!

Other options: in person meetings
secure (non – connected) …
… special systems
Attacks go towards Application
Trend towards Application Attacks

Top Site Category
Online shopping sites are 21 times more likely to deliver malicious content and work as counterfeit software sites, than simple sites.

2013 Cisco Annual Security Report
Setting up the Scene: Conclusion

1. **Cyber security is essential**, and must be lived and maintained on a new level! In-spite of cyber security limitations, which cannot be overcome, actions are demanded.

2. All major government act according the same lines: **Information dominance**. There is no good or bad, it just **is**! Criminals are using equal methods.

3. **Military Cyber Forces** is tools as army, navy and air-force for pursuing its own interest / will against the counter party, when normal political means have failed*.
   As in military, on crime scene the “optimal tools with lowest risks and least effort” is taken to perform crime

4. **“Crown Jewels”** (most precious information assets) must be cared for differently than normal IT.

5. Prepare of next Strategic Cyber Period e.g. : Computer nomad with **BYOD**, **Big Data** for new wave of aggregation and correlation options, **Advanced Persistent Threats APT**, worldwide **Cloud Computing** and **Industrialization of IT** (IT-services will be produced in shared infrastructures, more cost-efficient and professional than today) etc …

*Carl von Clausewitz 1780-1831: Citation: “Military Force as an instrument that states and other political actors use to pursue the ends of policy, in a dialectic between opposing wills, each with the aim of imposing his policies and will upon his enemy.
Section 2: Resilience and Preparedness

Response in case we cannot avoid …
Releasing a new Agency …
With cyber security official and with regular direct access to him

Hackers, and a few keystrokes and their programs are called “Weapon of Mass Destruction!”

More harmful than the nuclear bomb! (2012)
Preparation Recommendation CEPS* No. 3

*CEPS: Center for European Policy Studies: The Critical Infrastructure in the EU
Covered issues: CIP but with strong focus on IT and CIIP


• Background preparation of the meetings and protocols of the group meeting
• Background research and exchange of relevant material
• Strong content and organizational effort by CEPS (Andrea Renda et al.). Chair prepared some meeting content and (co-)guided through meetings.
• It is a contribution to the debate on C(I)IP which intends to stimulate discussions.

Example: Increase policy and operational focus on resilience and preparedness.

Next slides will give an introduction and an overview
It is about what we can do, if we cannot avoid …

or

Operating under (permanent) attacks (… as normal operation), which introduces a new view.
There are just too many HILF* Risks ....

Source: www.coop.ch/pb/

“We need active discussions about how much we are willing to pay and what we should do to prepare.”

Sibos 2011: John Trundle, managing director, risk management at central securities depository, Euroclear

and what service level we wish to attain

A. Mühlheim CIO SwissGrid & B. Hämmerli

and we need to prepare, for when we cannot avoid ...

Next slides ...

*HILF High Impact, Low Frequency
Resilience and Plan B: Example Deepwater Horizon

We extend from the grand challenges (inter-)dependencies and cascading effect to resilience with the example of Deep Water Horizon

Basic Attributes of Infrastructure Systems:
Resilience (Systems are less vulnerable, less exposed)
Incident (what is, when the event happens)
Plan B (have always another option prepared)
Insurance (yes, but there are other aspects ...)
Business continuity

Grand Question:
How must to invest in pre-incident and how much in Plan B and crises Management?
Deep Water Horizon – Before the Disaster
A “fail-safe” System Failed: No Plan B

Nesting pelicans are seen landing on May 22 as oil washes ashore on an island that is home to hundreds of brown pelican nests as well as terns, gulls and roseate spoonbills in Barataria Bay.

http://www.huffingtonpost.com/2010/04/30/louisiana-oil-spill-2010_n_558287.html
Resilience Needs to be a Part of the Design, The Role of Insurance, Disaster Recover Plan / Reconstruction

Demand: “Resilient cyber, physical and social systems must be robust, redundant, resourceful, and capable of rapid response”
CIP Event Cycle (just another integrated view)

Preparedness should emphasize all six DoD phases:

Source: DoD US
Recommendation CEPS No. 3

Increase policy and operational focus on resilience and preparedness. The need to protect critical infrastructures (CIs), including critical information infrastructure (CII), must be fully understood by policymakers, as the awareness of this policy issue leads to a paradigm shift in the way we think about infrastructure policymaking.

Key questions on resilience and preparedness:
What we expect? What is the need?
What we can afford? What are the dependencies?
What is a political supported minimum level for EU?

... and which diversity is acceptable e.g. between emerging and wealthy member states

→ discussion with Africa at this stage ...
Section 3:

Definitions and short introduction in (C(I)IP

Including the three grand challenges leading to

⇒ Recommendation CEPS No. 4 & 5
Critical (Information) Infrastructure Protection

Sectors / Services within sectors

Definition **Criticality of Services**:
Services, organizations and institutions, which are (absolutely) *essential to the public community* such that failure or disruption of which will result in *long-lasting supply bottlenecks and/or other dramatic consequences* for *substantial elements of the community*, are considered as critical.

Source: ETHZ CIIP Handbook

A **Sector** consists of one or **Multiple Services**

Example Sectors: next slide
### Sectoral coverage of national CIP plans (OECD)

<table>
<thead>
<tr>
<th>Sector</th>
<th>Australia</th>
<th>Canada</th>
<th>Netherlands</th>
<th>UK</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy (including nuclear)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Health care</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Water</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency services</td>
<td>x</td>
<td></td>
<td>Emergency services</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemicals</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defence industrial base</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other sectors or activities</td>
<td>Public gatherings, national icons</td>
<td>Legal/ judicial</td>
<td>Dams, commercial facilities, national monuments</td>
<td>Space and research facilities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: OECD (2008)*
## Swiss Sectors

<table>
<thead>
<tr>
<th>Sectors</th>
<th>Sub-sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>Natural gas supply, Oil supply, Power supply, Banks</td>
</tr>
<tr>
<td>Financial services</td>
<td>Insurance companies, Information technologies, Media, Telecommunication</td>
</tr>
<tr>
<td>Information- &amp; communication technologies (ICT)</td>
<td>Chemical and Pharmaceutical Industry, Mechanical and Electrical Engineering Industries</td>
</tr>
<tr>
<td>Industry</td>
<td>Foreign representations and headquarters of international organizations, Cultural property, Parliament, government, justice, administration, Research Institutes</td>
</tr>
<tr>
<td>Public administration</td>
<td>Medical care and hospitals, Laboratories, Civil defense</td>
</tr>
<tr>
<td>Public health</td>
<td>Armed forces, Civil defense, Emergency organizations (police, fire service, emergency medical service and rescue services)</td>
</tr>
<tr>
<td>Public safety</td>
<td>Air transport, Water transport, Postal services, Rail transport, Road transport</td>
</tr>
<tr>
<td>Transport</td>
<td>Water supply, Drinking water supply, Waste, Wastewater</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criticality Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high criticality</td>
</tr>
<tr>
<td>High criticality</td>
</tr>
<tr>
<td>Regular criticality</td>
</tr>
</tbody>
</table>
Grand Challenge 1: Domino Effect, Cascading
Grand Challenge 2: Dependency and Inter-Dependency

A depends on B

Interdependent or mutual dependent

- Complex: A depends on B, B on C, …, and Y on A and B

By Suanne Jantsch
Example (inter-)dependencies ... Take with you: Complexity!!
Question: Should we look at IT as a separate sector?

Concept: **ICT integrated infrastructures:**
No infrastructure of today runs without IT!

From a Governmental point of view, both views are necessary,
*IT as a sector and IT as an integrated part of each sector.*
Internal Structure of IT-Support:

Extreme long production chain.

And: It will be deeper in future with SOA (software oriented Architecture) and SaaS (Software as a Service)

Remember: per sector and per nation
CEPS Recommendation No 4

Build Long-term CIP strategy for EU.

The EU needs a forward-looking well defined strategy, and strong political commitment. The strategy should include key pillars such as the development of best practices, education exercises and training, the promotion of R&D and fostering information sharing between public and private operators and suppliers. The fact that suppliers are often global players, while public policymakers act at a local level, makes the policy dialogue more difficult and international coordination even more important.
Key Public-Private-Partnership (PPP) Issue: Building Trust
The Key to Information Sharing

Trust is the essence and cannot be commanded!

- All Hazard
- Rules, Regulations & Law
- Standards and Benchmark
- Audit
- All Forms of Pressure
- Metrics
+ Sector wise
+ Recommendation
+ Self Assessment
+ Common Exercise
+ Good Practice

It’s about the art to do the doable and not to dream on idealism

Thesis of Margrete Raaum at HIG
Recommendation No 5

Foster trust between information sharing partners.

Public-private-partnership (PPPs) offers a good way to **facilitate trusted information sharing among the key EU stakeholders**; however, given the unique challenge posed by the need to coordinate the approach across EU 27 it needs to be carefully planned and orchestrated. **It needs time, clear rules, sector-specific arrangements and sharing units of limited size (Nr. of experts):** this issue needs to be addressed upfront and carefully in order to **ensure successful international and EU-level cooperation.**
Recap

Section 1: The cyber security situation has changed dramatically in the last years and will continue to do so, with IPv6, Green IT, Smart Grid, Internet of Things and new threats.

Section 2: A closer look on resilience and preparedness.

Section 3: gave insights into CIP fundamentals (three grand challenges: Cascading, Dependency and ICT Supported Infrastructure). Needed action: Long-term CIP Strategy (National and EU) and on Trust (Public Private Partnership) according the CEPS report were discussed.
Section 5: Discussion & Questions
Section 2

Implementing Governmental CIP Measures: The Public Private Partnership PPP

Recommendation CEPS No. (5), 7
Why we need to act by now? Situation Analysis and Needs:
Service Supply of Nations: From Monopoly to Free Market

Free Market introduced:
- Competition (lowest rate possible)
- Many service provider with corporate security
- Delegation of the supply task
- Overall guarantee of supply and its securing measures skipped
- Structure is still centralized, (partly with common nodes and/or Infrastructure (Telco)

CIP is the answer to secure the old fashioned “public service” for (inter) & national purpose
Public Private Partnership

... A collaboration of Government and Service Provides with the goal to maintain national supply chain and create preparedness.

Possible Set up:

Each party should carry its own cost
Government should pay for facilitating the partnership

Conclusion

The role of suppliers and the global challenges are underestimated heavily by today! Let us work and let us work together.
Extended Public Private Partnership

Government

Service Provider
(Also Chains and Cloud)

IT) Suppliers have limited resources and should act on regional level:
issues: resources, liability, effectiveness

Imagine: a large scale: Computer-Chernobyl  -Fukushima ?!
Recommendation CEPS No.7

Adopt “new approaches” for industry-government cooperation.

The EU should adopt a flexible approach to CIP policy, by establishing through primary legislation only the general principles and main outcomes sought through EU CIP policy, and leaving it to the industry to devise the best technical measures that fulfill the desired levels of resilience.
Implementing Governmental CIP Measures: Structuring PPP in Europe

Recommendation CEPS No. 1, 2, 8
IT Attacks: It’s a Global Challenge

Local
National Regulator
Start Catastrophes
Global
Global IT Regulator?
Service Providers
Suppliers

Conclusion: There is a need for structured exchange
IT Attack: it’s a Global Challenge

Political structure must be considered!
Subunit ➔ District ➔ Member States ➔ Regional ➔ EU ➔ Globe

How to live the subsidiarity successfully?
And to guarantee self-determination MS?
Recommendation No 1

A thorough subsidiarity test should be performed for each economic sector.

The increasing inter-dependence between infrastructures and between countries, as well as the inter-links between physical infrastructure and the information infrastructure create a compelling argument for coordination of CIP policy at the international level. The European Commission should thus perform a thorough subsidiarity test to clearly identify areas where acting in common is more desirable, and areas that may remain under national competence in C(I)IP policy. The test should be run for each of the economic sectors involved.
It's a Global Challenge

Local Challenge  Global Suppliers

Call Mr. Europe
Sector wise subsidiarity

MS 1..................MS 27

Consequences:
EU and sectors have to prioritize the effort of supplier’s global support team!
Recommendation No 2

One single EU top level agency.

The EU must adopt an all-hazards approach by empowering – in line with a consolidated trend in many countries – a single agency to deal with CIP and CIIP issues. The agency’s mandate should include both preparedness and response coordination including operating an EU hotline for emergency management and early warning.

Remember: Internal organization should be sector-wise.
Recommendation No 8

Integrate CIP into the EU policymaking processes.

Impacts on CI resilience should be introduced as a mandatory step in the Commission’s Impact Assessment system, whenever the policy issue at hand potentially affects, even if indirectly, the resilience or vulnerability of CIs.

» Contribution of Eyal on risk assessment