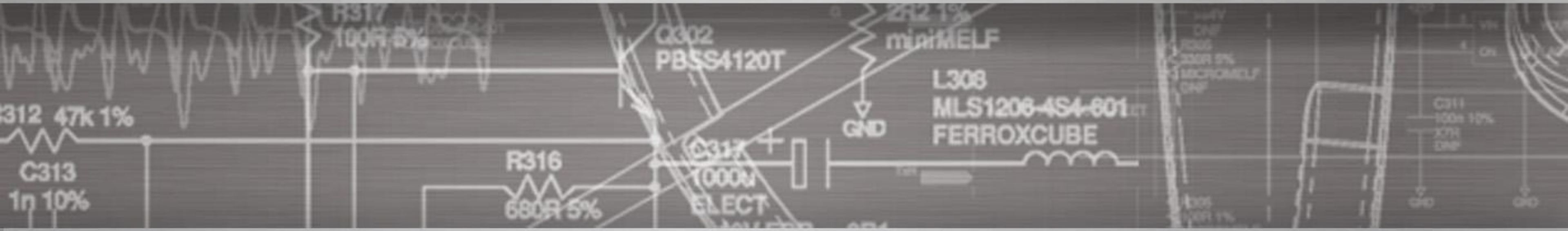
ENGVALL SECURITY

Information security

Strategic considerations in a national perspective



„Internet is just a hype…“

- Ines Uusman Swedish Minister of communication (12 May 1996)

Strategic considerations in a national perspective

Agenda

- **Part 1 Case study**
  - Ericsson 2003
  - Estonia 2007
  - Carema 2011
  - Tieto 2011
  - Swedish Government 2012
- **Part 2 Five action rules for successive information security**
  - Value perspective
  - Responsibility
  - Forum
  - Building competence and knowledge
  - Indicators
- **Part 3 Swedish information security strategy**
  - History
  - National strategy for information security
  - National forum SAMFI
  - CERT.se
  - National plan for the management of severe IT incidents
  - SGSI

Strategic considerations in a national perspective

Ericsson 2003

- General description
  - System intrusion in the purpose of stealing vital information and to affect on system integrity
- Attack vectors
  - Exploring general system vulnerabilities
  - System intrusion leading to authorized access
  - Collecting information on site
  - Encrypted information transfer session
- Aim
  - Selling information
  - Selling consultation services
- Consequences
  - Modified the platform of T 68
  - Gathered classified information:
    - JAS 39 Gripen
    - Erieye

Strategic considerations in a national perspective

ENGVALL SECURITY

Estonia 2007

- General description
  - Cyberattacks on Estonia refers to a series of cyber attacks that began April 27,2007 and swamped websites of Estonian organizations, including Estonian parlament, banks, ministries, newspapers and broadcasters,
- Attack vectors
  - Most of the attacks that had any influence on the general public were DoS or DDoS type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution. Spamming of bigger news portals commentaries and defacements including that of the Estonian reform party website also occurred
- Aim
  - Show of force by inflict on the possibility to run the national administration
- Consequences
  - Disruption in bank system, health care news flow and general society
  - administration

Strategic considerations in a national perspective

Carema 2011

- General description
  - The websites of the swedish private run healt company CAREMA was chosen as target for the hacker community “Anonynoumys”.
- Attack vectors
  - DDoS
- Aim
  - Public statement
- Consequences
  - All services connected with the website was disrupted and the company suffered severe business losses

Strategic considerations in a national perspective

Tieto 2011

- General description
  - Friday the 25th of November 2011 Tieto, a major hosting and supervision IT-company, was hit by a vital and fatal error in the data store system and the reserve system minutes later. 50 major costumers was involved Including municipality administration governmental administration, pharmacies, banks, universities, Stockholm city administration.
    The company have classified all details
- Attack vectors
  - Not released
- Aim
  - Not clarified/released
- Consequences
  - brought major assets of society administration down
    for two days. All customers working with tools connected to the web was out of business

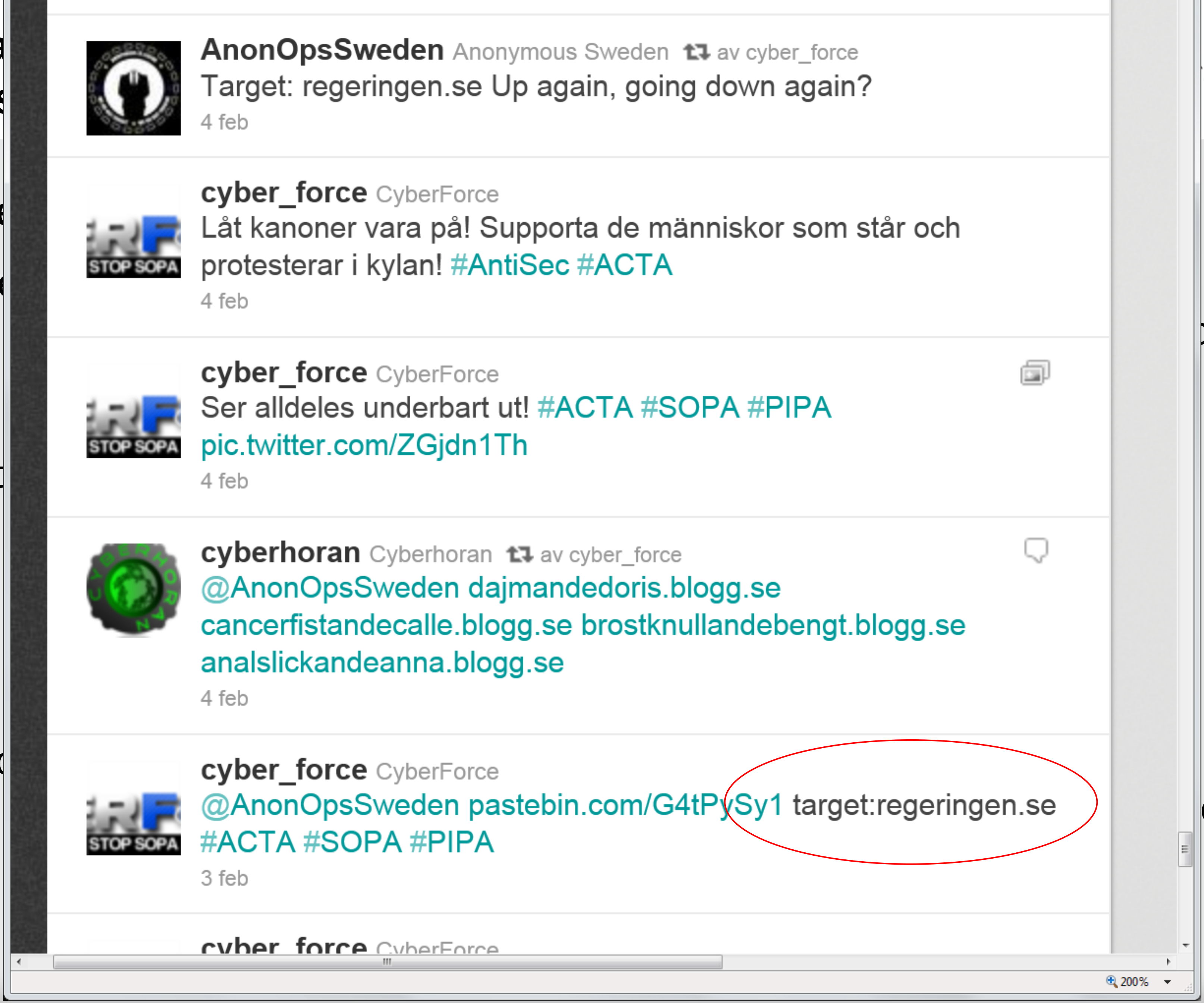
Stra
pers

Swe

- Ge
- At
- Ai
- Co

cial

es



AnonOpsSweden Anonymous Sweden av cyber_force
Target: regeringen.se Up again, going down again?
4 feb

cyber_force CyberForce
Låt kanoner vara på! Supporta de människor som står och protesterar i kylan! #AntiSec #ACTA
4 feb

cyber_force CyberForce
Ser alldeles underbart ut! #ACTA #SOPA #PIPA pic.twitter.com/ZGjdn1Th
4 feb

cyberhoran Cyberhoran av cyber_force
@AnonOpsSweden dajmandedoris.blogg.se cancerfistandecalle.blogg.se brostknullandebengt.blogg.se analslickandeanna.blogg.se
4 feb

cyber_force CyberForce
@AnonOpsSweden pastebin.com/G4tPySy1 target:regeringen.se #ACTA #SOPA #PIPA
3 feb

cyber_force CyberForce

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

Three types of aggressors and how to respond

- The dumb
  1. Doesn´t care who he affects
  2. Spamming
  3. Virus (known profiles)
  4. Chain letters
  5. Fraud
- The evil
  1. Wants you
  2. Specific idea
  3. Generally skilled
  4. Network in hand
  5. DoS
  6. Intrusion
  7. Worms and Trojans
- The rich
  1. Unlimited resources
  2. Contacts with providers of IT
  3. States or extremely well established hacker-networks
  4. All vectors

- Low profile business and non vital low level society administration
  1. Standard security setups
  2. Documented routines for security management
- Important level of society administration and high profile business
  1. Thorough understanding of own core business vital assets
  2. Top management commitment to security
  3. High level of security awareness
  4. Security management of high quality
  5. Referring to international standards
- Administration of great national importance and extremely vital business
  1. Vital aspects analyzed to the point
  2. Tailored solutions
  3. Robust communication
  4. Security trained personnel
  5. External systems
  6. Vetting
  7. Inhouse

Strategic considerations in a national perspective

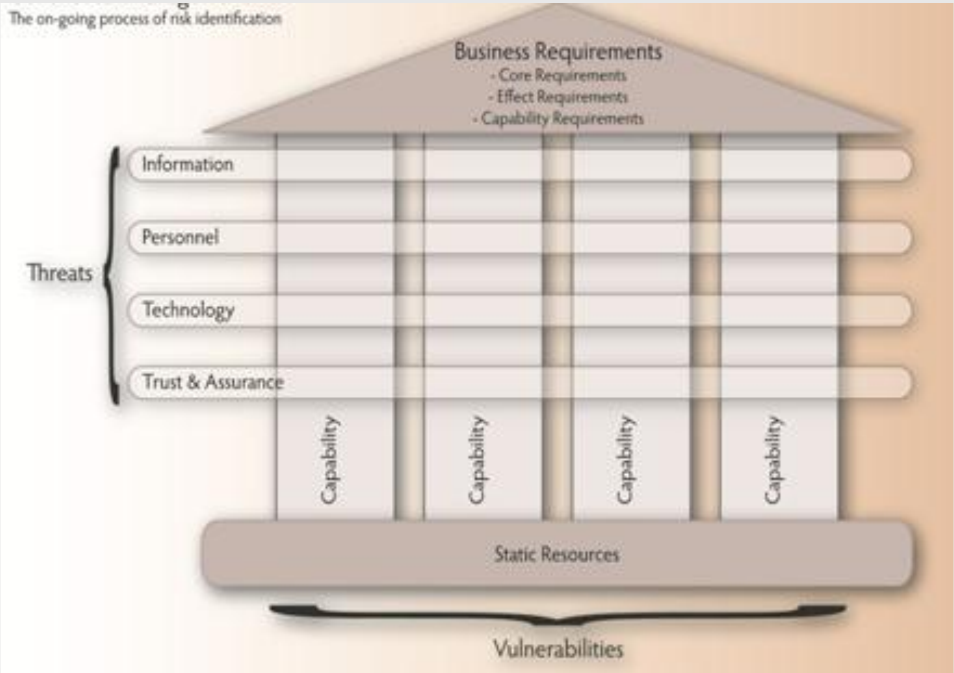
Part 2 Five action rules for successive information security

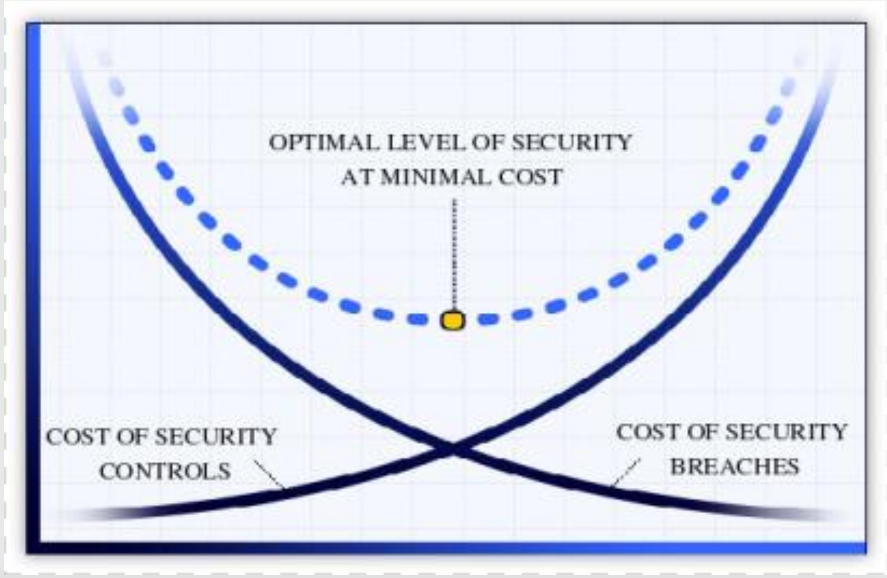
- How do we think wisely in relation to these examples of attacks
  - 1. Since there are:
    - a lot of modus operandi
    - a lot of different type of actors/aggressors
    - a huge amount of information to protect
  - 2. Since we can’t handle life without our systems

Strategic considerations in a national perspective

Part 2 Five action rules for successive information security

- Value perspective
    - Analyze your business, what is core business most important
    - components and what is the value of that.
    - (What if… and what if not…)





Strategic considerations in a national perspective

Part 2 Five action rules for successive information security

- Responsibility
  - Divide responsibility
  - Put names on the lists, not functions
  - Follow up

Strategic considerations in a national perspective

Part 2 Four action rules for successive information security

- Forum
    - Common problems common soloutions
    - Where do we take decisions
    - Where do we divide responsibilities
    - Where do we speak the thruth!

Strategic considerations in a national perspective

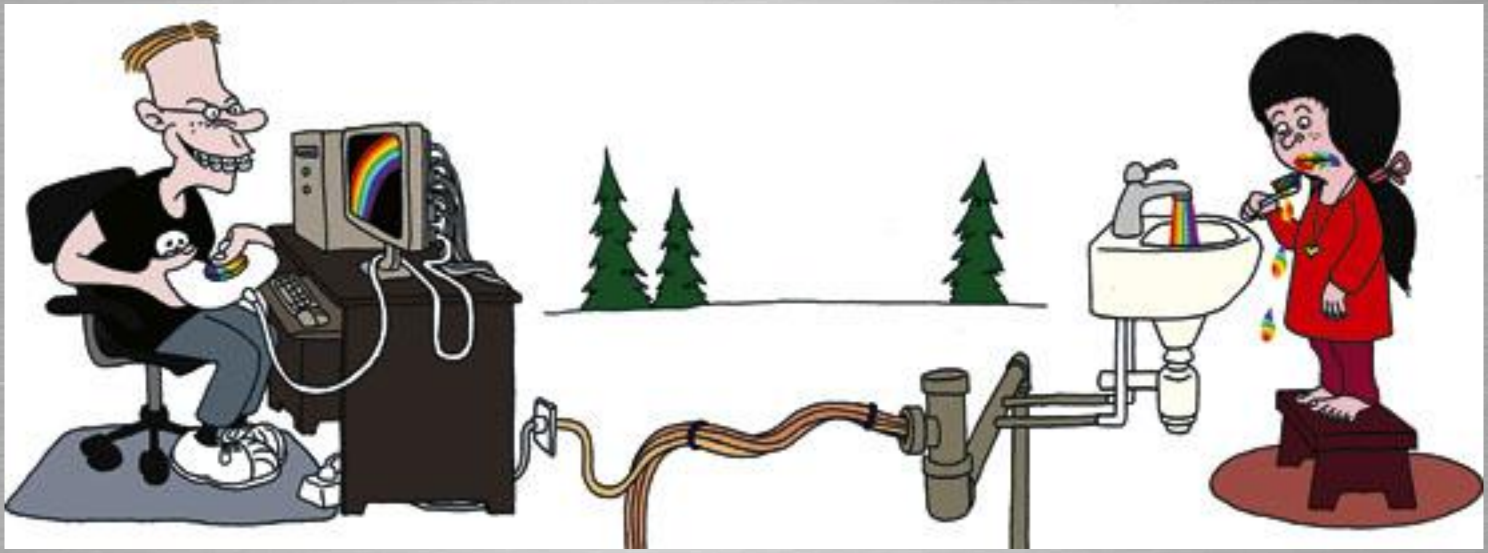
Part 2 Five action rules for successive information security

- Indicators
  - Hard to tell when and where
  - Hard to tell how and why
  - But there are better and verse trends

Strategic considerations in a national perspective

Part 2 Five action rules for successive information security

- Building knowledge and competence
  - In order to educate
  - Certify
  - Develop action plans
  - Develop rules and regulations



Water is essential in every society that’s
why all types of threats against our water should be embraced
by our authorities including those on the cyber arena

Strategic considerations in a national perspective

Part 3 Swedish national information security achievments

- History
- National strategy for information security
- National forum SAMFI
- CERT.se
- National plan for the management of severe IT incidents
- SGSI

CERT.SE KONKURRENSNEUTRAL IT-SÄKERHET FÖR NÄRINGSLIV OCH OFFENTLIG SEKTOR

MSB Swedish Civil Contingencies Agency

SWEDISH ARMED FORCES

PTS

CSEC

FRA

Polisen

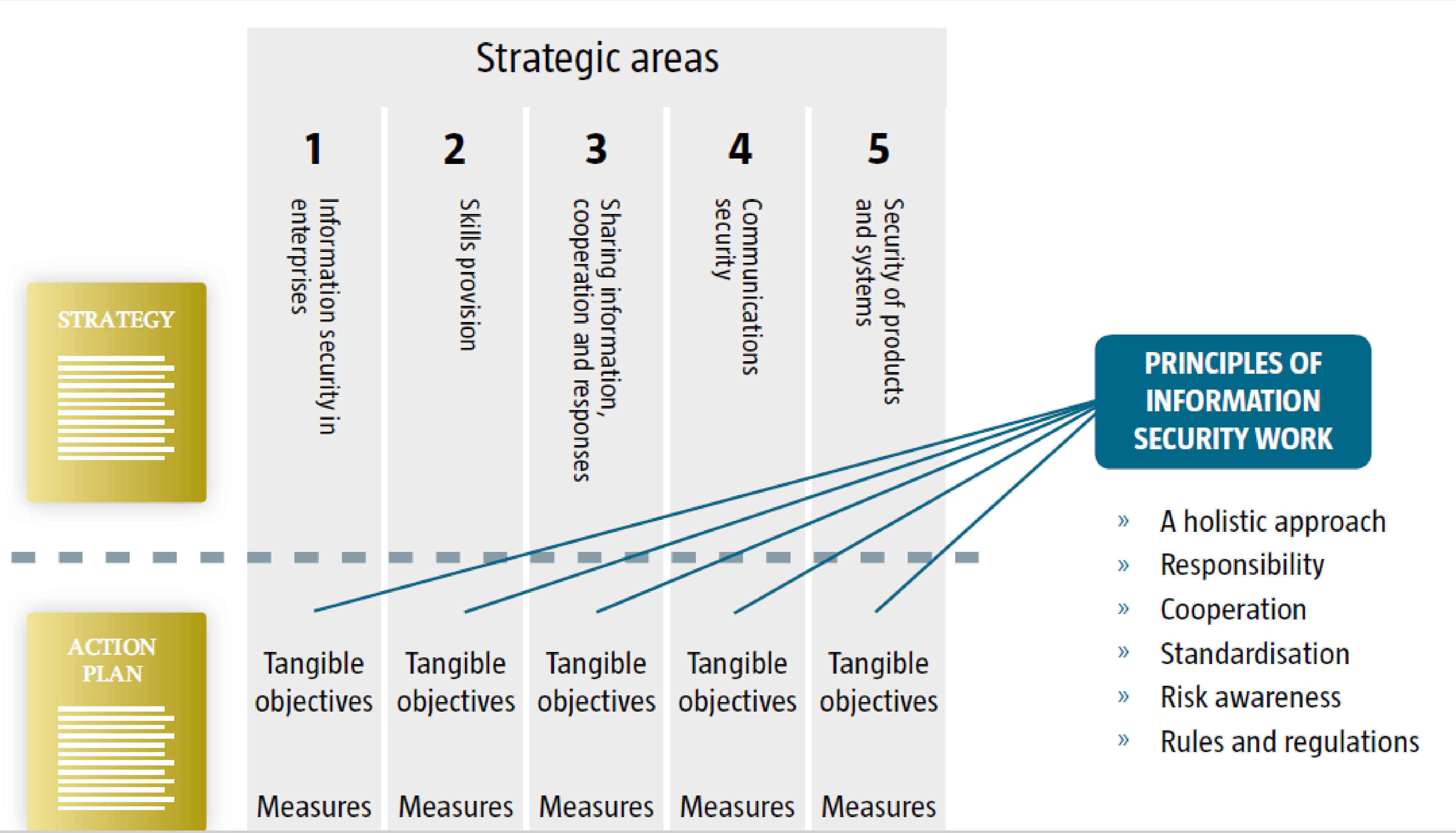
Strategic considerations in a national perspective

Part 3 History

- 1980-1995 We are all beginners at some point
- 1995-2000 Understanding the need
- 2000-2008 Learning and arguing
- 2008-2012 Down to business

Strategic considerations in a national perspective

Part 3 National strategy for information security



Strategic areas

1 Information security in enterprises

2 Skills provision

3 Sharing information, cooperation and responses

4 Communications security

5 Security of products and systems

STRATEGY

ACTION PLAN

Tangible objectives

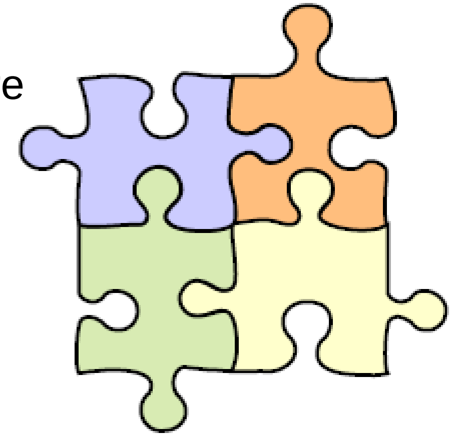
Measures

PRINCIPLES OF INFORMATION SECURITY WORK

- » A holistic approach
- » Responsibility
- » Cooperation
- » Standardisation
- » Risk awareness
- » Rules and regulations

Strategic considerations in a national perspective

Part 3 National plan for the management of severe IT incidents



National situation picture

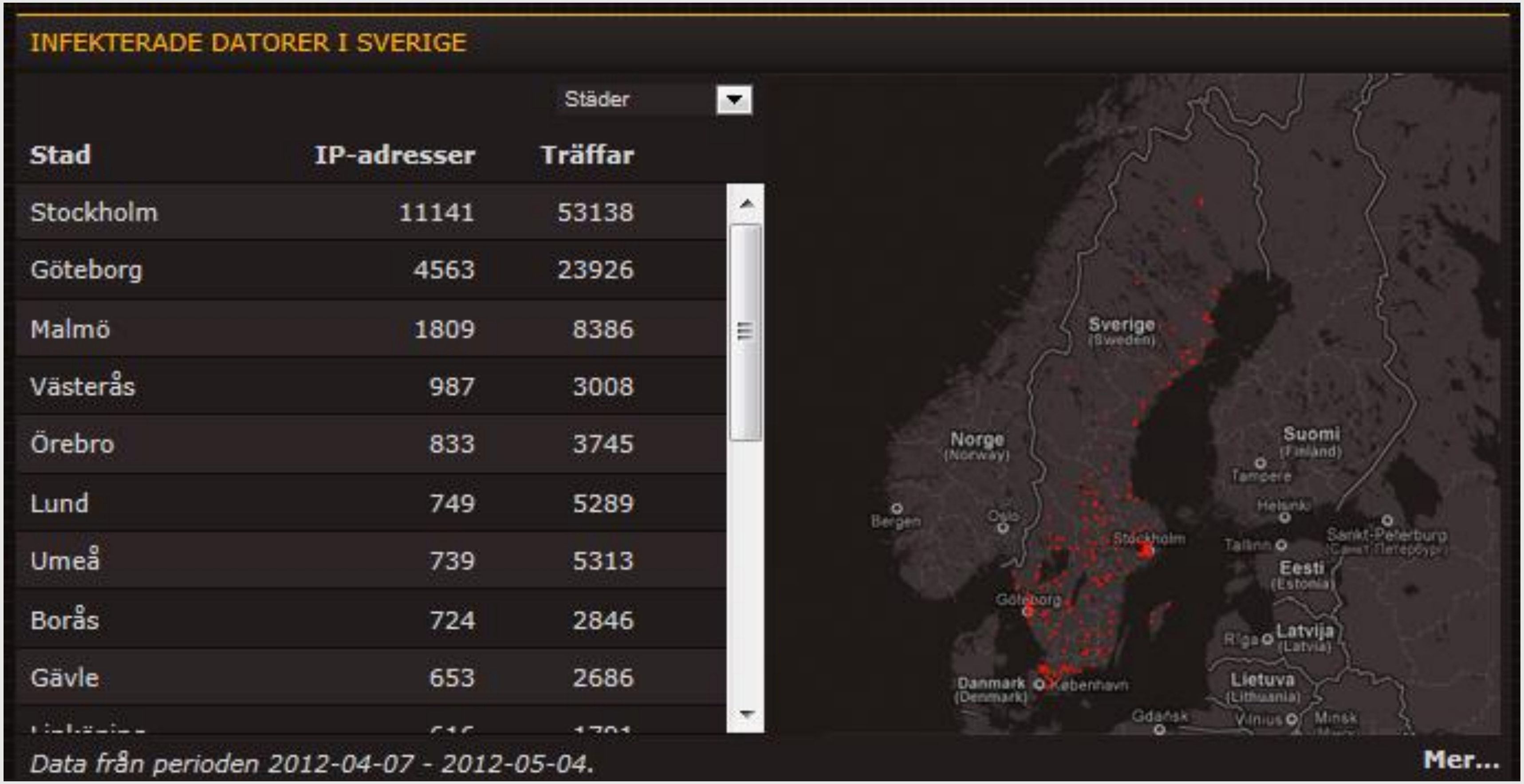
Information coordination

Common consequnce and action assessment

Thechnical onsite liasson

Strategic considerations in a national perspective

Part 3 CERT.se



INFEKTERADE DATORER I SVERIGE

Städer

Stad	IP-adresser	Träffar
Stockholm	11141	53138
Göteborg	4563	23926
Malmö	1809	8386
Västerås	987	3008
Örebro	833	3745
Lund	749	5289
Umeå	739	5313
Borås	724	2846
Gävle	653	2686
Linköping	616	1701

Data från perioden 2012-04-07 - 2012-05-04.

Mer...

Strategic considerations in a national perspective

Part 3 National forum SAMFI

The following agencies cooperate in SAMFI:

· Authority Civil Contingencies Agency (MSB)
· Post and Telecom Agency (PTS)
· National Defence Radio Establishment (FRA)
· Security Police (SAPO) and National Crimina lInvestigation Department
· Defence Materiel Administration (FMV) (CSEC)
· Armed Forces (FM) / Military Intelligence and security Service (MUST)

Strategic considerations in a national perspective

Part 3 SGSII

Secure communication between agencies
Secure communication with EU (TESTA)
Connects more than 20 agencies
Separated from open internet
Encrypted

?