

Implications of IT security regulation on international trade

Heidi Lund, Senior Adviser, National Board of Trade Sweden



Heidi M-B Lund

Consumer Research (Finland, The Netherlands) 1993-1994

Special Adviser (Swedish Board for Accreditation and Conformity Assessment) 1996-2005

Assessor/ Trainer/Expert in EU financed technical assistance-projects in the field of Quality Infrastructure (Western Balkans, MEDA-region, Poland, Turkey) 2005-2009

Senior Adviser (National Board of Trade Sweden) 2010- 2018 technical barriers to trade, international regulatory co-operation, EU FTAs and trade related technical assistance

Strategic Adviser (Swedish Civil Contingencies Agency), cybersecurity 2018

Senior Adviser (National Board of Trade) 2019 - technical barriers to trade, international regulatory co-operation, EU FTAs and trade related technical assistance

What is IT security?

Virus

Clean desk policies

Attached files

Information security management system (ISMS)

Ransomware

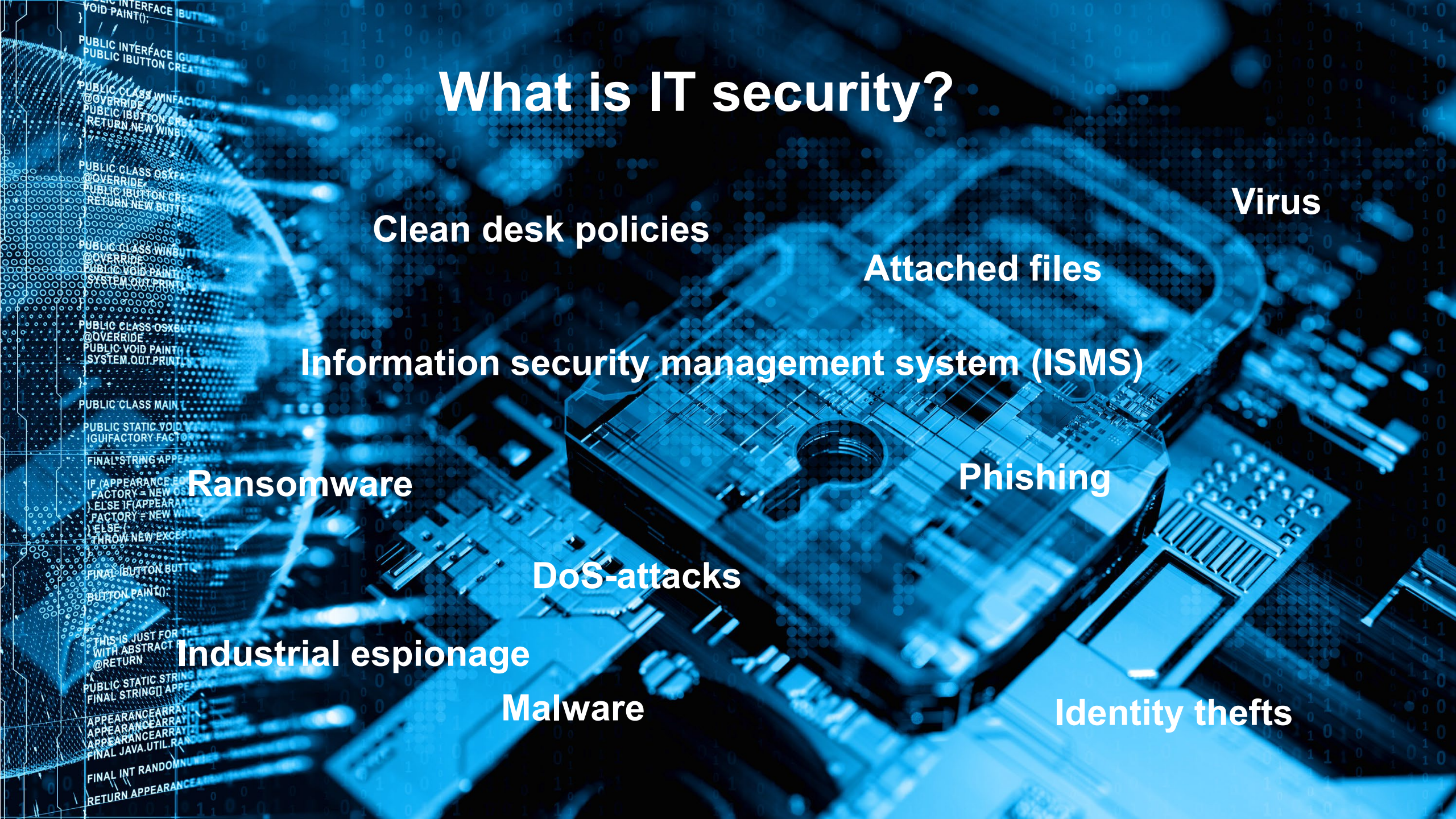
Phishing

DoS-attacks

Industrial espionage

Malware

Identity thefts



```
void paint();  
public interface IGUIFactory  
public IButton createButton()  
  
public class WinFactory  
@Override  
public IButton createButton()  
return new WinButton();  
  
public class OSXFactory  
@Override  
public IButton createButton()  
return new OSXButton();  
  
public class WinButton  
@Override  
public void paint()  
system.out.println("WinButton");  
  
public class OSXButton  
@Override  
public void paint()  
system.out.println("OSXButton");  
  
public class Main  
public static void main()  
IGUIFactory factory = new WinFactory();  
final String appearance = "OSX";  
if (appearance.equals("OSX"))  
factory = new OSXFactory();  
else if (appearance.equals("Win"))  
factory = new WinFactory();  
else  
throw new Exception("Invalid appearance");  
final IButton button = factory.createButton();  
button.paint();  
  
// THIS IS JUST FOR THE TEST  
// WITH ABSTRACT FACTORY  
@Return  
public static String appearance = "Win";  
final String[] appearances = {"Win", "OSX"};  
appearanceArray = appearances;  
appearanceArray2 = appearances;  
final java.util.Random random = new Random();  
final int randomNumber = random.nextInt(appearances.length);  
return appearanceArray[randomNumber];
```

Why does the National Board of Trade Sweden analyse the subject?

Cybersecurity regulation has a major impact on the trade of ICT and risk to generate more barriers to trade!

<https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2018/the-cyber-effect.pdf>





Why is IT security regulation of ICT so important now?

- Number of people online and communicating through Internet increase all the time
- The number of security incidents and attacks increase and entail more and more serious consequences
- **There is a false security and reliance in the system...?**

Why do various countries have different views on IT security regulation?

- Perception of national assets or critical information
- Capabilities (technical knowledge and infrastructure) to protect assets and critical information

These two parameters are extremely difficult to harmonize internationally!



PART II

Cybersecurity of ICT – Regulatory options and consequences for policy making

How can IT security be addressed through regulation?

Requirements on IT-products

- Product requirements
- Requirements on conformity assessment (certification /evaluation)



To what extent is IT security in ICT regulated?

- National Security
- Goods within critical infrastructure
- Commercial IT products

Information to be secured

NATIONAL SECURITY

Communication Security (COMSEC)
Classified Information

Regulated by laws and regulations

TO BE REGULATED

Based on NIS Directive and the coming Cybersecurity Act in the EU, it might be likely that a larger number of stakeholders and products will be subjected to cybersecurity requirements than before

OTHER DATA

COTS

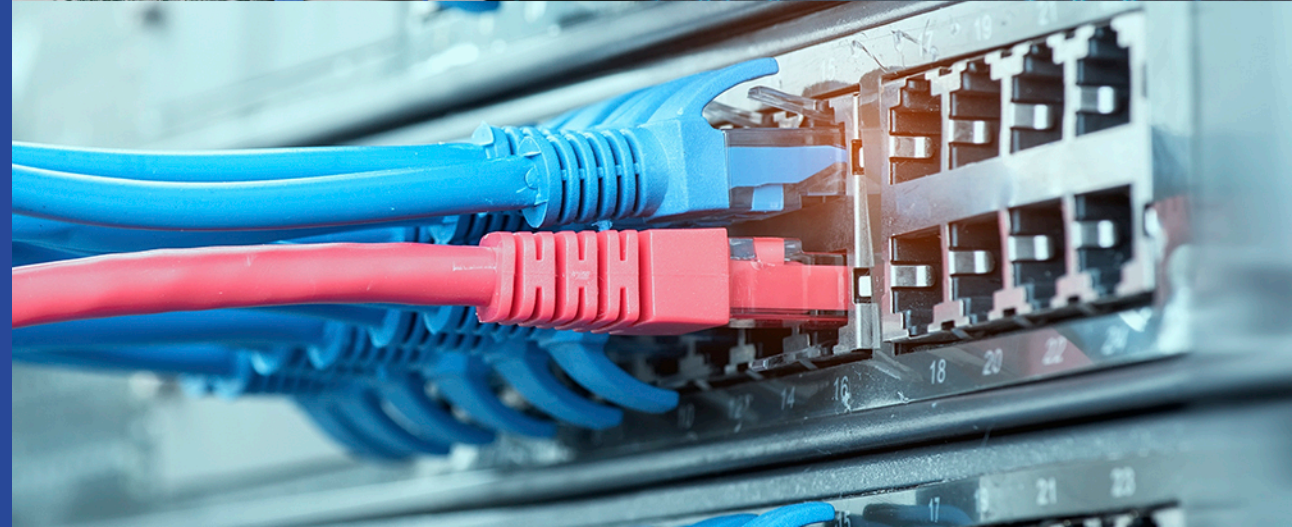
(Commercial off-the-shelf) products

Not relevant to regulate or self-regulation by industry

How can IT security be managed through regulation?

Requirements on IT-products

- Product requirements
- Requirements on conformity assessment (certification /evaluation)
- Requirements on IT infrastructure





International regulatory cooperation

- + International standard for cyber certification with mutual recognition of certificates
- Standard is generic and creates a need for additional national requirements
- New regulatory tools and strategies will embrace product specific requirements but need to observe international systems for compliance

Existing regulatory strategies- PROs and CONs

- Status quo
- Requirements on cyber certification of ITC
- Requirements on the infrastructure where ICT is used

Cyber regulation as a policy challenge

NATIONAL SECURITY

REGULATORY OBJECTIVE:
TO PROTECT THE STATE AND ITS
CITIZENS AGAINST ALL KINDS OF
NATIONAL CRISES

TRADE POLICY

REGULATORY OBJECTIVE:
TO PROMOTE FREE TRADE AND
MARKET ACCESS WHILE RECOGNISING
THE RIGHT TO REGULATE TO PROTECT
SAFETY, HEALTH, ENVIRONMENT AND
NATIONAL SECURITY



Conclusions

- Regulatory initiatives that concern IT security of ITC are extremely important!
- Regulatory initiatives on IT security for ICT embrace several policy areas which require a holistic perspective!
- It is necessary to analyse regulatory initiatives from a trade perspective!

Policy conclusions and take aways

Trends and issues to follow

Privatisation of critical infrastructure services

- The state has less and less control of service providers IT solutions
- The cyber landscape and priorities of individual countries different
- Each country is forced to evaluate policy options on regional and international level carefully
- **To manage or even coordinate cyber resilience through regulation internationally is likely to be more demanding than coordination in another policy domain!**

Trends and issues to follow

In the field of cybersecurity of ICT: regulatory fragmentation rather than regulatory harmonisation

- Need to evaluate trade dependencies in relation to regulations
- Small countries might suffer from regional/ international regulatory solutions not taking their trade partners conditions into account
- **It can be expected that countries become “less loyal” to policy principles as they see cybersecurity partly falling in the scope of national security!**
- **Some part of incident reports and harmful cyber activity might fall off the radar!**

Trends and issues to follow

Privatization of regulation

- Public-private partnerships will be essential – as ICT regulation (standardization) is more and more driven by business, and in sector specific communities
- An increased insight in sectors and technologies are also vital for evaluation of new draft regulations as well as for the enforcement of legislation (which is a challenge in cyber as such)
- **There is a need to more closely follow standardisation initiatives in the field of cybersecurity to for a holistic view on where technology is moving!**

How about regulatory tools to be used?

- **Nothing connected to Internet is safe!**
- Cyber certification may raise cybersecurity but only if countries can mutually agree on certification schemes that prove to cover prioritized (often inter linked) vulnerabilities
- **It is reasonable to expect that countries have strong national interests- which might result in "standards wars"- why the policy makers should consider relying on regulatory schemes with open, transparent standards setting !**

Cybersecurity requirements- how?

The success in addressing cybersecurity in ICT are dependent on

- ✓ Improving the knowledge and skills of cybersecurity in general by the creation of strong security culture overall – tools such as regulatory frameworks such as NIS are good for raising cyber resilience for vital society functions
- ✓ Shifting the focus of security measures as far as possible to the initial stage of product life cycle:



although complex to address by technical regulation..

Thank you for your attention!



Heidi is an experienced adviser and trainer for executive level in industry, trade, government, EU institutions and national administrations in emerging economies, in the field of implementation and enforcement of technical regulations, standards, conformity assessment procedures and market surveillance.

Heidi authored the report 'The Cyber Effect: The implications of IT security regulation on international trade'. The report explores the ways regulation of IT security has a bearing on international trade and market access. Her other recent work includes technical barriers to trade (EU/WTO), EU standardization policy, international regulatory cooperation (UNECE, OECD) and regulatory aspects in EU free trade agreements.

Heidi has also extensive experience in trade-related capacity building and she has delivered technical assistance in the field of the development of National Quality Infrastructure in nearly thirty countries.

Heidi works as Senior Adviser at the National Board of Trade Sweden:

heidi.lund@kommers.se