

# **IT-Security beyond borders**

Recommendations from a working group  
in the Danish Board of Technology

**English Summary**

# IT-Security beyond borders

Recommendations from a working group in the Danish Board of Technology

## **English Summary**

### **Project Leadership at the Danish Board of Technology**

Projectmanager Bjørn Bedsted, bb@tekno.dk

### **The members of the working group are:**

- Preben Andersen, DK-CERT
- Christian Wernberg-Tougaard, Member of ENISA's advisory panel on "Awareness Raising".  
Director for Unisys
- Brian Birkvald, leader of IBM's security group in Denmark
- Morten Storm Petersen, Signaturgruppen A/S
- Carsten Stenstrøm, Director of Technology Security, DR
- Lars Neupart, Neupart A/S

Further information about the project is available at the Danish Board of Technology's website [www.tekno.dk](http://www.tekno.dk).

# English summary

## Background for the project

Technological development has brought about the phenomenon of an increasing number of societal functions being integrated with the Internet; including for instance, the public sector, the banking industry, and buying and selling of goods. This trend increases society's vulnerability to cyber-crime and means that poor IT-security, as often seen in the form of software flaws or lack of protection against viruses and hackers, still has serious consequences. For this reason, global interconnectedness via the Internet increases the risk of threats coming from anywhere in the world.

Among the analysis institutes and law enforcement agencies around the world, there is a clear consensus that problems associated with cyber-crime are widespread and growing. One explanation is that the global Internet is particularly well suited for criminal activity. The culprits typically hide behind networks of computers, located in numerous countries, making Internet-borne criminal action incredibly difficult to investigate and solve. The fact that cyber-crime becomes more complex and criminal action harder to detect, also points to the fact that cyber-criminals are also becoming increasingly skilled in their trade.

Though the problems grow ever greater, IT-security issues are poorly addressed in both Denmark and internationally, in respect to other forms of crime. The amount of scientific investigations and publicly available statistics regarding cyber-crime are highly limited; just as concrete initiatives to prevent and confront cyber-crime are characterized by a lack of resources and focus.

For Denmark to meet its official goal of being an innovative knowledge and entrepreneurial society, able to punch its weight at the global level, Danish citizens and companies must be able to communicate securely; both within and beyond Denmark's borders. This is an important prerequisite for taking full-advantage of globalization's potential and hence a prerequisite for Denmark's welfare in the future.

It is therefore necessary that Denmark, the EU, and the world at large, seriously increase their efforts in preventing and fighting national and transnational cyber-crime. Many of the security problems with which Denmark stands cannot be solved nationally – they require international solutions.

A working-group on "IT-security Beyond Borders", under the auspices of the Danish Board of Technology (DBT), has developed recommendations that go significantly farther than previous efforts in the arena of IT-security in Denmark have been able to. The working group holds that it is high time to take concrete and well-aimed steps in the form of, among other things, lawmaking, certification, and labeling programs.

The working group also feels that Denmark, being the technically capable, knowledge intensive, and resource-endowed nation that it is, should go forth and pave the way for such steps to be taken on European and international level, where they can have a real effect.

This will, furthermore, actuate a competitive advantage for Denmark, should it take the reins. Through such actions, Denmark can increase the opportunity to establish itself out in front in the area of security solutions and concepts, which can then be provided to other countries should they wish to follow the Danish model. The working group points out that Denmark could contribute greatly in this area, to the benefit of the global society.

## Six concrete recommendations

The working group has sought to develop and present internationally-focused recommendations for cross-border IT-security problem areas that are seen to be among the most problematic now and in the near future.

The goal is that all of the recommendations presented should be realizable in practice. The group advises that the recommended solutions will be set in motion as soon as possible, and simultaneously in the six problem areas. It is furthermore the working group's intention that the recommendations should contribute to improving Danish and international IT-security – a prerequisite to citizens and firms being able to harvest the many benefits that a digitally-connected world has to offer.

Here is an overview of the problem areas addressed in the report and a brief description of the working group's recommendations:

### 1. Vulnerabilities in software and hardware

**Problem:** Vulnerabilities in hardware and software, such as operating systems and packaged programs is were the most serious of all IT-security problems in 2006 are, as measured in the number of instances and their consequences.

The consequences of these vulnerabilities are of greater consequence for small and medium-sized enterprises (SME's), public institutions and private citizens, rather than large firms.

**Solution 1:** Develop a model that ensures security updates in software are installed on the users' computers directly after a security flaw is found. The process should be imperceptible for the basic user while advanced users should be given the option to steer their own update process. Large program updates, often called 'service-packs' by some providers, would however remain installable only after user acceptance.

**Solution 2:** There should be EU regulation that vendors of electronic, network-based (IP based) hardware such as computers, telephones, MP3-players, alarm-systems, and in the future even refrigerators, must deliver their products with the latest firmware and software updates pre-installed.

**Solution 3:** Denmark/the EU should create a "white-list" for software and hardware. The public sector could then set the example and drive the market by only using white-listed IT-products.

**Solution 4:** A certification program for Internet Service Providers (ISPs). All ISPs in the EU are obliged to follow a code that at least meets the standard set by the Danish ISP Security forum's code of conduct. Within 3-5 years, it should be made law that all ISP's are ISO 27001-certified (or meet an equivalent thereof).

### 2. Inadequate knowledge of IT-security

**Problem:** Inadequate knowledge is a significant cause of the lack of security. The human factor is, i.a. important in relation to "phishing", identity theft and the spread of harmful programs that can "crash" a computer. This can obviously cause the loss of data from the harddisk including documents, photos, films, music, etc.; and for companies, the loss of client records and intellectual capital. The lack of IT-security knowledge is rarely an isolated problem for the firms and citizens who are ill-secured. The consequences of poor security can spread to a firm's customers, partners, etc., and the people listed in private user's address list – in total, causing exponential damage and economic loss. In light of this, it is necessary that network administrators, employees and managers prioritize security much higher than they do today. And general awareness and knowledge of the population at large should be significantly raised.

**Solution 1:** A greater focus on IT-security in school. The security aspect should be connected with students' use of computers throughout the course of their education.

**Solution 2:** Establishing "The Board for Greater IT-security" focusing on citizen awareness.

**Solution 3:** Regulation against "Cyber-pollution".

### **3. The inability to differentiate between secure and insecure products and services**

**Problem:** An ever greater number of products and services contain an element of connectivity (Internet Protocol – IP-based) and thus it is ever more relevant to offer secure products and services to users with the aim of improving the general security level. This includes computers, mobile phones, harddisk recorders in TV's, media centers, refrigerators, and similar items in a private home. In the near future, nearly all apparatus, including cars, boats and planes, will contain IP technology and be connected to the net. Security problems are expected to increase further because these products will continue to be produced around the world by numerous manufacturers, making it evermore difficult for end-users and companies to comprehend and handle the security aspect.

**Solution:** Denmark should take the initiative to develop a concept for labeling internet-connected products, meaning that private persons and companies are given the ability to see the security level of a given product. For example, a star-rating as in the auto-industry's "crash-test" scheme, could be implemented. The labeling program should include the entire EU, and thereafter spread to the global market.

### **4. The lack of concerted, transnational police efforts and prosecution in the cyber-crime arena**

**Problem:** Cyber-crime is a difficult arena for law enforcement agencies in Denmark as well as the EU and world at large. Interpol is largely absent from the fight against IT-related crimes and Europol's roll is relatively small due to limited resources. The growing amount of cyber-crime on a global plane is fraught with inadequate police efforts. It is problematic that the prevention and investigation of cyber-crime is generally prioritized so low in comparison with other police investigations, that the sector receives few resources and therefore has an acute lack of personnel with the competency to make a change in and outside of Denmark.

**Solution 1:** Structuring the efforts: acknowledging cyber-crime as a new law enforcement specialization. Appointing at least one unit responsible for cyber-crime in each police district, and establishing a central authority that can address complex cases concerning cyber-crime professionally – nationally and internationally. Prioritizing cyber-crime should not come at the cost of other police activities. Rather budget increases are needed to supplement the efforts.

**Solution 2:** Increasing the knowledge level: Law enforcement authorities must be equipped with greater competency across the board – from the education of specialists in the various sectors of cyber-crime, to increasing the knowledge of prosecutors and judges.

**Solution 3:** Further development of international cooperation agreements, which can ensure more efficient and effective processing of transnational cyber-crime cases.

### **5. Lack of secure identification**

**Problem:** Communication security is a prerequisite for the free flow of information, efficient eGovernment, and thus better public service in the future. Citizens' usage of the increasingly integrated economic service infrastructure in the EU and around the world, can be halted by the lack of a clear identification mechanism, nationally and across the EU. This could, i.a. minimize the risk of the abuse of personal data. One could imagine a mechanism that would eliminate the difficulties connected with the exchange of patient records between Danish and foreign hospitals. It is a national responsibility to create a digital identification that can protect citizens' personal data against, i.e. identity theft. The working group concludes that all citizens in Denmark and the EU at large, should be equipped with an identification mechanism with strong security.

**Solution:** Denmark should establish a long-term strategy for the further development of the existing "Digital signature" into a "citizen service passport", seen as a 'digital identity, which then helps to minimize the risks involved in eGovernment, eTrade, and other forms of electronic communication. The goal is that, in the long run, all EU citizens should have an interoperable digital ID. The working group points to a project under development in Austria, as a source of inspiration. The Danish development work should be coordinated in relation to the entire EU, with the goal of building a secure, EU-interoperable "citizen service infrastructure", using common and open communication standards.

## **6. The lack of focus on IT-security in public procurement**

**Problem:** Under 5% of the criteria found in contracts for the public procurement of IT account for security. The working group finds that IT-security is not taken seriously when the EU and its member countries take bids on infrastructure and systems contracts. It is problematic that technical specifications for IT-security and privacy in the public procurement of IT products are either lacking or non-existent, and that these contracts seldom contain a “connectedness analysis”, meaning an assessment of the consequences of a security breach on all of the interconnected public units, many of which are not themselves a part of the procurement agreement.

**Solution:** Regulation stating that IT-security must be a key parameter in all public procurement contracts, where IT is a component. Specification sheets and bids should contain both a security and connectedness analysis that assesses the consequences of a security breach for interconnected sectors.