5.10 Investing in network and information security

Why invest in network and information security?

ICT has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. Many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems. However, information systems can be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks. Cybersecurity incidents are increasing at an alarming pace and could disrupt the supply of essential services. The Commission’s online public consultation on ‘Improving network and information security in the EU’ found that 57% of respondents had experienced network and information security (NIS) incidents over the previous year that had a serious impact on their activities.

The likelihood and frequency of incidents and the inability to ensure protection also undermine public trust and confidence in network and information services. Across the EU, more than one in ten Internet users have already become victims of online fraud. The 2012 Eurobarometer on Cybersecurity found that 38% of EU Internet users are concerned about the safety of online payments and have changed their behaviour because of concerns with security issues: 18% are less likely to buy goods online and 15% are less likely to use online banking.

This problem affects all parts of society and economy (national and local administration, business and consumers). In particular, a number of sectors play an essential role in providing key support services for our economy and society. These sectors include banking, stock exchanges, energy generation, transmission and distribution, transport (air, rail, maritime), health, enablers of key Internet services and public administrations.

Security incidents are capable of rendering critical government functions unavailable for several days, as demonstrated by the cyber-attacks against Estonia in 2007, which severely affected not only the provisioning of online services such as e-government and e-banking within the country, but also prevented citizens from accessing online services across borders.

Public networks are strongly interconnected and an incident affecting one entity even at local level can easily spread to another entity. Due to this strong interconnection, a network effect, resulting from incidents affecting a number of similar administrations, even small and local, is more likely in the context of public administrations. Such an effect carries the risk of NIS incidents spreading within or between administrations, which could disrupt or paralyse vast fields of local and national public activities. This risk is increased by the fact that state and local administrations are often targeted by cyber-attacks and are facing very significant and rising NIS risks. Criminals in particular can use a local administration as an entry point to attack other sectors of the administration.

The resilience and reliability of public on-line services to citizens is key to building and preserving their trust in e-government. eGovernment and eParticipation are increasing with citizen demand for timely and cost-effective services and so are the NIS risks for state and local administrations. The risk of public online services being hindered by NIS problems exists at all levels of government, local or regional.

Barriers & challenges

Private actors still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture, to conduct serious risk management which involves the adoption of appropriate NIS measures and investment in security solutions. 31% of respondents (both business and consumers) to the public consultation affirmed to have no process in place to manage NIS risks. Also, 54.2% affirmed not to have any budget dedicated to NIS.

From an economic perspective security is an externality leading to market failure, i.e. market players do not see the economic rationale of bearing the full social costs of increasing the level of security but rather prioritise time-to-market or low pricing for their end products. By leaving the decision on the level of security entirely to market players the societal benefits of a more secure digital environment would not be fully reached. Businesses fail to see the potential savings induced by NIS investments. Studies have indicated that by appointing a Chief Information Security Officer (CISO) businesses could save up to half of the cost of a data breach. The same considerations apply to public administrations which do not yet see the importance of investing in NIS to ensure the continuity and reliability of the public services they provide more and more online.

How to act?

1. Build on on-going EU policies on network and information security: a European Network and Information Security Agency (ENISA) was established in 2004. ENISA advises Member States on information security and in their dialogue with industry to address security-related problems. It collects and analyses data on security incidents in Europe and emerging risks. It promotes risk assessment and risk management methods to enhance

---

135 This area of activity can be an important element of a digital strategy. It might, however, not be eligible for funding through ESIF.

capability to deal with information security threats. Finally, it is active in awareness-raising and co-operation between different actors in the information security field, notably by stimulating the cooperation between the public and private sectors and developing public-private partnerships with industry. ENISA’s web site is the European ‘hub’ for exchange of information, best practices and knowledge in the field of Information Security. The revised regulatory framework for electronic communications, in force since November 2009, requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches. These obligations had to be transposed at national level by May 2011.

All players that are data controllers (for example banks or hospitals) are obliged by the data protection regulatory framework to put in place security measures to protect personal data. Also, under the 2012 Commission proposal for a General Data Protection Regulation, data controllers would have to report breaches of personal data to the national supervisory authorities. The Commission proposes imposing NIS risk management and reporting requirements on public administrations and key private players to stimulate the creation of a culture of risk management and improve the sharing of information between the private and public sectors. The public administrations concerned include regional and local authorities.

Another aspect that deserves attention is the safety of the Internet for different segments of the population. SI Net II, is a project for the European coordination of the network of Safer Internet Centres. The specific objectives of this project are to ensure maximum cooperation and effectiveness of awareness-raising, hotlines and helplines actions across Europe and to provide logistical and infrastructural support for the Safer Internet Centres, ensuring European-level visibility, good communication and exchange of experience so that lessons learnt can be applied on an on-going basis.

2. Governance/stakeholder involvement: Public regional and local authorities should engage with relevant stakeholders. These actors should include:

- Public sector, such as national/regional ministries in charge of NIS, or regional and local governments; national or local CERTs and NIS authorities;
- Standardisation and certification bodies;
- Universities and research institutes;
- Professional and end user associations;
- Private sector: operators in specific critical sectors (banking, electricity, natural gas, transport, health), enablers of key Internet services, law firms, insurance companies. Public regional and local authorities should also make an assessment of their own needs in terms of increased NIS and in particular proceed with an audit.

3. Priority setting: NIS is important for very different sectors. In the order of estimated NIS revenues of main industries in 2010, the following consumers and main industries were major users of NIS: general services, manufacturing, public services, financial services and consumers. Business spending on NIS grew very strong in companies with more than 250 employees. The hardware market for NIS is very concentrated. All these aspects should be considered when choosing priorities within NIS markets.

4. Policy mix: In this process, regions should also seek synergies with other national and regional initiatives and EU activities. Of particular interest in this area could be:

- (a) the Horizon 2020 Framework Programme for Research and Innovation, to be launched in 2014. Horizon 2020 will support research security related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems;
- (b) Connecting Europe Facility (2014-2020), in particular regarding the deployment of Digital Service Infrastructures which aim at providing trans-European interoperable services of common interest for citizens, businesses and governments.

In February 2013, the Commission adopted a Communication on an EU Cybersecurity Strategy. The Strategy in particular contains actions to promote cyber security awareness at all levels. A cyber security championship should be organised in 2014, where university students will compete in proposing NIS solutions. A yearly cyber security month with the support of ENISA and the involvement of the private sector should be organised from 2013 onwards, with the goal of raising awareness among end users. Training on NIS should be introduced in schools as well as training on NIS and secure software development and personal data protection.
for computer science students by 2014. Finally, NIS basic training should be conducted for staff working in public administrations.

The Strategy is accompanied by a proposal for a Directive on Network and Information Security. The proposal requires in particular all the Member States to set up a well-functioning CERT, responsible for handling security incidents and risks, and appoint a national competent authority for NIS which would have a coordination role. Both would need to have adequate staff and financial resources to carry out their tasks effectively. Both CERTS and competent authorities could have regional or local branches, adopt a national NIS contingency/cooperation plan defining protocols for communication and cooperation among relevant players at national level in case of NIS incidents of a certain scale, and a national NIS strategy that would outline the strategic objectives and concrete policy actions to pursue a high level of NIS.

5. Monitoring and evaluation: Market maturity indicators are useful for monitoring the market context, IT security spending and business adoption of IT security. The study European Network and Information Security Market\(^{144}\) offers a good overview of potential market indicators. Given that the NIS market is very dynamic and rapidly evolving, it is important to keep track of new developments.

Further reading


---