Security Economics and The Internal Market

1 Executive Summary

Network and information security are of significant and growing economic importance. The direct cost to Europe of protective measures and electronic fraud is measured in billions of euros; and growing public concerns about information security hinder the development of both markets and public services, giving rise to even greater indirect costs. For example, while we were writing this report, the UK government confessed to the loss of child-benefit records affecting 25 million citizens. Further revelations about losses of electronic medical information and of data on children have called into question plans for the development of e-health and other systems.

Information security is now a mainstream political issue, and can no longer be considered the sole purview of technologists. Fortunately, information security economics has recently become a live research topic: as well as collecting data on what fails and how, security economists have discovered that systems often fail not for some technical reason, but because the incentives were wrong. An appropriate regulatory framework is just as important for protecting economic and other activity online as it is offline.

This report sets out to draw, from both economic principles and empirical data, a set of recommendations about what information security issues should be handled at the Member State level and what issues may require harmonisation – or at least coordination. In this executive summary, we draw together fifteen key policy proposals. We held a consultative meeting in December 2007 which established that almost all of these proposals have wide stakeholder support. We believe they will provide a sound basis for future action by ENISA and the European Commission.

Recommendations

1: There has long been a shortage of hard data about information security failures, as many of the available statistics are not only poor but are collected by parties such as security vendors or law enforcement agencies that have a vested interest in under- or over-reporting. Crime statistics are problematic enough in the traditional world, but things are harder still online because of the novelty and the lack of transparency. For example, citizens who are the victims of fraud often have difficulty finding out who is to blame because the incidents that compromised their personal data may have been covered up by the responsible data controllers. These problems are now being tackled with some success in many US states with security-breach reporting laws, and Europe needs one too.

We recommend that the EU introduce a comprehensive security-breach notification law.

2: Our survey of the available statistics has led us to conclude that there are two particularly problematic 'black holes' where data are fragmentary or simply unavailable. These are banks and ISPs. On the banking side, only the UK publishes detailed figures for elec-

tronic fraud, broken down by the typs of attack. Similar figures are probably available to regulators in other Member States but are not published.

We recommend that the Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime.

3: On the ISP front, it is widely known in the industry that well-run ISPs are diligent about identifying and quarantining infected machines, while badly-run ISPs are not.

We recommend that ENISA collect and publish data about the quantity of spam and other bad traffic emitted by European ISPs.

4: People who leave infected machines attached to the network, so that they can send spam, host phishing websites and distribute illegal content, are polluting the digital environment, and the options available are broadly similar to those with which governments fight environmental pollution (a tax on pollution, a cap-and-trade system, or private action). Rather than a heavyweight central scheme, we think that civil liability might be tried first, and suggest

We recommend that the European Union introduce a statutory scale of damages against ISPs that do not respond promptly to requests for the removal of compromised machines, coupled with a right for users to have disconnected machines reconnected if they assume full liability.

5: A contentious political issue is liability for defective software. The software industry has historically disclaimed liability for defects, as did the motor industry for the first sixty years of its existence. There have been many calls for governments to make software vendors liable for the harm done by shoddy products and, as our civilisation comes to depend more and more on software, we will have to tackle the 'culture of impunity' among software developers.

We take the pragmatic view that software liability is too large an issue to be dealt with in a single Directive, because of the large and growing variety of goods and services in which software plays a critical role. Our suggested strategy is that the Commission take a patient and staged approach. There are already some laws that impose liability regardless of contract terms (for example, for personal injury), and it seems prudent for the time being to leave standalone embedded products to be dealt with by regulations on safety, product liability and consumer rights. Networked systems, however, can cause harm to others, and the Commission should start to tackle this. A good starting point would be to require vendors to certify that their products are secure by default.

We recommend that the EU develop and enforce standards for network-connected equipment to be secure by default.

This need not mean Common-Criteria certification of consumer electronics; it would be quite sufficient for vendors to self-certify. However, the vendor should be liable if the certification later turns out to have been erroneous. Thus if a brand of TV set is widely compromised and becomes used for hosting phishing and pornography sites, the ISPs who paid penalty charges for providing network connectivity to these TV sets should be

able to sue the TV vendor. In this way the Commission can start to move to a more incentive-compatible regime, by relentlessly reallocating slices of liability in response to specific market failures.

6: There has been controversy about vulnerability disclosure and patching. Recent research has shown that the approach favoured by the US Computer Emergency Response Team (US CERT) – namely responsible disclosure – gets better results than nondisclosure or open disclosure. However, some firms still take a long time to issue patches for vulnerabilities, and we believe that liability would help them along.

We recommend that the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for unpatched software to speed the patch-development cycle.

7: Vendors also dissuade people from patching by bundling patches with upgrades and with disfeatures such as digital rights management.

We recommend security patches be offered for free, and that patches be kept separate from feature updates.

Likely future steps include making end-users liable for infections if they turn off automated patching or otherwise undermine the secure defaults provided by vendors. A useful analogy is that it's the car maker's responsibility to provide seat belts, and the motorist's responsibility to use them.

8: The next set of issues concern consumer rights. At present, the ability of consumers to get redress when they are the victims of fraud varies considerably across Member States. This issue was fudged during the preparation of the Payment Services Directive but now needs to be brought back on to the agenda.

The European Union should harmonise procedures for the resolution of disputes between customers and payment service providers over electronic transactions.

9: Some companies use marketing techniques that break various EU laws and/or exploit various loopholes in ways that should be banned or that provide cover for criminal activity. We need to abolish the business exemption for spam, criminalise firms who buy botnet services through third parties, and criminalise firms that install spyware on consumer computers without full user consent and without providing easy uninstallation.

We recommend that the European Commission prepare a proposal for a Directive establishing coherent regime of proportionate and effective sanctions against abusive online marketers.

10: The flip side of this is consumer protection, which will over time become much more complex than just a matter of payment dispute resolution. We already have an Unfair Contract Terms Directive, but stakeholders have raised other issues as well. Consumer protection in the broad sense is too wide for this report but will need attention.

ENISA should conduct research, coordinated with other affected stakehold-

ers and the European Commission, to study what changes are needed to consumer-protection law as commerce moves online.

11: The IT industry has tended towards dominant suppliers. As systems become increasingly interconnected, a common vulnerability could trigger cascading failures. Diversity, then, can be a security issue as well as a competitive one.

We recommend that ENISA should advise the competition authorities whenever diversity has security implications.

12: As for critical national infrastructure, one particular problem is the lack of appropriate incentives to provide resilience in competitive network markets.

We recommend that ENISA sponsor research to better understand the effects of Internet exchange point (IXP) failures. We also recommend they work with telecomms regulators to insist on best practice in IXP peering resilience.

13: As well as providing the right incentives for vendors and service providers, and protection for consumers, it is important to catch cyber-criminals, who at present act with near impunity thanks to the fragmentation of law-enforcement efforts. In order for the police to prosecute the criminals they catch, cyber-crimes must be offences in all Member States.

We recommend that the European Commission put immediate pressure on the 15 EU Member States that have yet to ratify the Council of Europe Convention on Cybercrime.

14: Furthermore, as nearly all cyber-crimes cross national borders, cooperation across jurisdictions must be improved. Joint operations and mutual legal assistance treaties have so far proved inadequate.

We recommend the establishment of an EU-wide body charged with facilitating international co-operation on cyber crime, using NATO as a model.

15: Finally, a number of regulations introduced for other purposes have caused problems for information security researchers and vendors – most notably the dual-use regulation 1334/2000, which controls cryptography with a keylength in excess of 56 bits, and the implementations of the cybercrime convention in some Member States that have criminalised the possession of 'hacking tools' (which can also catch security researchers). The security industry needs a 'friend at court'.

We recommend that ENISA champion the interests of the information security sector within the European Commission to ensure that regulations introduced for other purposes do not inadvertently harm security researchers and firms.