2012 - EC Consultation on Improving Network and Information Security in the EU

This paper forms part of the response of the JNT Association, trading as Janet [1], to the Commission's consultation on Improving Network and Information Security (NIS) in the EU [2]. Janet is the UK's National Research and Education Network, connecting universities, colleges and research organisations to each other and to the Internet at very high bandwidths. Like most research networks our policy is to permit the wide range of network traffic needed to enable innovative research and to deal promptly and effectively with incidents that may occur. Our Computer Security and Incident Response Team (Janet CSIRT) has been a part of global information exchanges for nearly two decades, so has wide experience of coordinating the response to NIS attacks.

The great majority of these attacks come from end user computers that have been compromised by attackers, either as a result of risky behaviour by their users or, though this is now less common, through technical vulnerabilities. Often it seems that the legitimate owners are either unaware that their computers are compromised or do not perceive this as a problem, even though the personal and financial consequences to a user of a compromised device are becoming more apparent. Nonetheless Kaspersky still report that in some Member States more than 20% of computers are compromised [3]. The only way to reduce attacks using these computers is to enhance the security of end users and their devices by providing advice, motivation and support. Public services such as Get Safe Online [4]in the UK and Germany's Anti-Botnet Centre [5]seem the best way to achieve this on the required scale.

Unlike end-users, Internet-connected businesses generally do suffer direct harm from NIS incidents, so should already be motivated to take measures to prevent them. Advice to company boards – for example through recent publications [6]by the Department for Business, Innovation and Skills [6] – can increase awareness both of the problem and the areas where insecurity may need to be addressed. Many businesses already understand that exchanging information about NIS incidents and remedies can improve practice for everyone: it is striking that the vast majority of security breach reports [7] made to the UK's Information Commissioner are now voluntary, from sectors do not have a legal obligation to notify. It is therefore not clear either that regulatory compulsion to report is needed or, once good practice is available, that businesses will need to be compelled to implement it. Both are increasingly recognised as being in businesses' own interest.

The most important reason to exchange information about NIS incidents is to learn lessons and improve practice among all users of networked systems. However we note and share ENISA's concern [8]that legal duties to notify or exchange information about incidents must not divert organisations from first responding to and resolving the incidents. We have previously expressed our concern [9] that a requirement to notify within 24 hours could distort priorities in that way. The suggestion in the current consultation that mandatory reporting might be extended to CERTs seems even more dangerous: CERTs above all must not be

distracted from their primary task of responding to incidents and minimising their impact. Any requirement on European CERTs to disclose information could make organisations reluctant to share information with them, thus increasing both the likelihood and severity of incidents.

For information exchange to be effective in improving security practice it must be both easy and trusted. Reporting an incident must not harm the reporter. If those who report are 'named and shamed' there will be a strong incentive to remain silent: if reporting is too onerous then organisations will have economic reasons to avoid it. It is therefore concerning that ENISA report five different notification schemes [8] either in, or being considered for, European legislation (the Telecoms Framework Directive, the Telecoms Privacy Directive, proposed Regulations on Data Protection and Digital Identities, and this NIS activity). These require different information, different timescales, different reporting points and different national implementations. Because of overlaps in the laws and the activities they regulate, many organisations will be subject to multiple reporting requirements resulting in wasteful duplication of both information and reporting effort. Information exchange must be efficient if it is to be a benefit to organisations and confidence in the information society, rather than a burden on those who participate in it.

We therefore recommend that any action by the Commission or Governments should focus on promoting the development, dissemination and use of good Network and Information Security practice by network users, businesses and providers. Actions that create burdens rather than benefits, or that hinder the resolution of NIS incidents, must be avoided. An approach that facilitates information exchange, rather than one that mandates breach notification, seems more likely to achieve this.

Links
[1] http://www.ja.net/
[2] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/818&format=HTML&aged=0&langua
[3] http://www.securelist.com/en/analysis/204792231/IT_Threat_Evolution_Q1_2012
[4] https://www.getsafeonline.org/
[5] https://www.botfrei.de/
[6] http://www.bis.gov.uk/news/topstories/2012/Aug/cyber-security-for-business
[7] http://www.out-law.com/en/articles/2012/september/ico-reports-increasing-trend-in-self-reported-data-breaches-in-past-five-years/
[8] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
[9] https://community.ja.net/library/consultations/2012-ministry-justice-call-evidence-eu-data-protection-proposals