Oct. 8, 2013 | NO. 72

ISSUE BRIEF
The Asan Institute for Policy Studies

Information Sharing for Cyber-Security: Evidence from Europe

Neil Robinson
Research Leader
RAND Europe

Recent cyber-attacks witnessed in the Republic of Korea on March 20th and subsequently on 25 June 2013, which affected financial institutions and newspapers, have highlighted the need for a well organised response to cyber-attacks. Cyber-attacks (and their response) cross the boundaries of public and private sector. Depending on the likely motivation attacks may require a response from: the police; regulatory authorities or, in the most serious cases, military and intelligence. The sharing of information between such entities is increasingly seen as important.

Concerns about cyber-security are widely held. In its 2012 survey of senior decision-makers in the public and private sector the World Economic Forum (WEF), found that cyber-security was ranked especially high by respondents as a technological risk being of global importance.[1] In 2011, Norton, part of the Symantec multi-national cyber-security firm, estimated the total cost of cyber-crime to be worth US$338bn per year.[2] Outages in the submarine infrastructure off the coast of Egypt resulted in a severe degradation of internet speeds across many countries in the Middle East and parts of Asia.[3]

In this issue brief[4] the results of three research projects gathering empirical evidence regarding information sharing[5] are discussed, drawing lessons relevant to the situation in the Republic of Korea.

Policy Mechanisms in the Republic of Korea

Perhaps understandably, the approach taken by the Republic of Korea is of a top down nature with the Blue House taking the lead in efforts since the attacks earlier in 2013. The Blue House has responsibility for response whilst he NIS (National Intelligence Service) co-ordinates the actual response.[6] The 2008 Korean Defence White Paper identified cyber-security as an essential component of national defence,[7] a theme which was reflected in the 2010 Defence White Paper where cyber-attack was identified as one of several non-traditional security threats that the government needed to address.[8]

Alongside the seeming increasing urgency of attacks and evolving cyber-risks, the South Korean government has been making efforts to expand its policy framework and capabilities. The National Cyber Security Management Regulation (Presidential Directive No. 141) as the main policy instrument guiding official South Korean response, sets out roles and responsibilities of various organisations. It is supported by the National Intelligence Agency Act and various other regulations on security.

Discussions over a proposed new bill that is intended to encompass many different aspects of cyber security are understood to be underway in the South Korean Parliament which will mean that South Korea joins an increasingly long list of countries with such broad omnibus national level frameworks: either in formal legislation or through cyber-security strategies and action plans. It remains to be seen, however, the extent to which information sharing is reflected as a key element in this draft legislation.

Presidential Directive 141 created the National Cyber Security Response Center (NCSC) which is the central government point for identifying, preventing and responding to cyber-attacks.[9] Other organisations of note include the national Cyber Security Strategy Council and a National Cyber Security Countermeasure Committee (playing a role as a crisis management committee). In order to further allow for more

efficient communications, efforts are also underway to develop information dissemination systems and joint action teams between civilian, government and military stakeholders.[10]

Concerning information exchange between public and private sectors, the 2008 Act on Information and Communications Infrastructure Protection provides a framework for Critical Infrastructure (CI) owners and operators in regulated sectors to create effective information security arrangements.

The Informatization Office of the Ministry of Science, ICT and Future Planning (MISP) reported that it was working on building a system of information sharing on the cyber-threat" by the end of 2014.[11]

Finally, the quasi-public model espoused by the Korean Internet Security Centre and its parent agency, the Korean Information Security Agency hold promise for effective exchange of information between Internet service providers and government).

For such frameworks to be as effective as possible in addressing cyber-security, some sharing of information must take place. We now turn to an analysis of the nuances of this requirement.

Types of Information Being Shared

In the context of this paper, a distinction is made between the type of relevant transaction involving cyber-security information. Information sharing is understood to concern a one way transmission to a known group without an expectation of reciprocation; information disclosure concerns a broader transmission of information to an unknown audience (for example the general public); notification implies transmission to a specific entity and finally information exchange concerns the transmission of information with an expectation of reciprocity.

Such transactions may include different types of information. Examples include:

- Technical information such as IP addresses, security telemetry, network traffic or

Indicators of Compromise (IoC) describing technical aspects about an incident;

- Threat relevant data: involving either a possibility of the type of attacker (nation state; criminal enterprise) or the type of attack vector used;[12]

- Vulnerabilities can cover: either a specific product or service or an organisation's policies and procedures;

- Experience of attacks; incidents and mitigations: anecdotal evidence from examples suggested that in a trusted forum, organisations may be willing to inform each other of security incidents affecting their operations; the impacts and what was done to resolve it (for example specific technical or procedural steps taken).

Why Does It Help to Share Information?

The sharing of some types of information between peers is commonly understood to be useful for two reasons: companies are able to learn from each other's mistakes to improve their own levels of cyber-security and secondly, if the government can access such information then it provides a 'window' into the level of security of critical infrastructures, further informing long term policy intervention.[13]

Within an organisation, reliance upon other information sources for security information (especially from peers operating in the same sector) may be seen as a useful way to triangulate understanding especially applied to mitigation measures and best practice on the basis that if something was reportedly successful for one organisation then there is the possibility that it might also be the case for others. Such activities can be useful in both the current and future efforts: firstly, by allowing the organisation to reduce vulnerabilities on deployed systems and secondly, by highlighting to the recipient that risks could be avoided in the future by not implementing a specific technology with which another party has reported problems.

Theoretical Barriers to Sharing Information

Neo-classical economic theory suggests that information will only be shared in an

Information Exchange (IE) when the benefits of doing so outweigh the costs. Particularly, economic theory suggests two ways in which economic incentives can be misaligned when individuals act in groups: externalities and free-riders.[14]

When a participant to an information exchange weighs up the benefits and costs of information sharing there is potentially a problem of externalities. The participant only takes into account the direct benefits to himself of information sharing, and not the wider benefits which may accrue to other members of the group.

A second barrier suggested by the economics literature, and stemming from misaligned economic incentives, is the problem of free-riding. A participant to an information exchange may be tempted to 'free-ride' and under-invest in information sharing in the hope of obtaining helpful information from other members for little or no cost.

Away from neoclassical economics, there are a host of other barriers that have been identified, including those concerning technical credibility (e.g. whether a technical specialist views his peers as technically credible); trust in the organisation receiving information; complex socio-behavioural issues[15] and in many different areas, laws, rules and procedures. For example, in regard to the latter, the European legal framework governing privacy and data protection prohibits the widespread sharing of data that is considered to be able to identify a person (such as Internet Protocol addresses) unless one of a number of conditions is met.

Three examples of how barriers and incentives work in practice are presented below using illustrative evidence from recent European cyber-security research studies.

Example 1: Information Sharing in Critical Infrastructure Protection

In 2009 the European Network and Information Security Agency (ENISA) published research into the exchange of information amongst owner-operators of critical information infrastructure. The research identified a host of incentives and barriers which operated either prior to or during participation in an IE. An IE is a specific type of trusted forum where peers gather to exchange information about incidents;

mitigation and effects of cyber-security with peers. Although this concept has its origins in the United States, IEs are increasingly seen as popular in Europe. Thirty representatives of companies participating in IEs were consulted as part of this research.[16]

The top three identified incentives were:

The first incentive was identified as cost savings. As security is very often seen as a cost centre with a difficult to prove return on investment (until it is too late), participants regarded that IEs were an important mechanism to reduce the costs of running and managing their cyber security operations.

The second most important incentive concerns the quality, value and use of the information derived from an IE. Participants were more motivated to either join an IE or volunteer information if they were already in one and if the value to them of the information obtained in an IE was something which was above and beyond what they could get from other sources.

The third most important incentive or encouraging factor was in relation to the existence of a clear playing field or set of rules and processes for participation. Those either thinking of joining an IE or participating in one considered that such a common framework or level playing field that all were aware of was especially important in managing expectations amongst their peers.

Perhaps unsurprisingly, the barriers or inhibitors to information sharing in an IE were something of a mirror image of the incentives.

The most important barrier in the top three was poor quality information. This was seen as being a barrier for two reasons. If the participants were receiving information which they could easily obtain elsewhere (especially either from free or paid for sources) then they would question participation, especially since IEs can occupy a lot of time for staff members. The second consequence was that the information obtained in an IE must be trustworthy, since the recipient must know that by implementing something he or she learnt in an IE won't make the situation in their

home network any worse.

The second most important barrier was in regard to reputational risks and that participants were concerned about whether the types of information would leak, exposing their firm as being incompetent or subject to cyber-attacks. This was particularly important with regards to publicly listed firms whose reputation is a key component of their stock market price.

Finally, the last most important barrier concerned poor management. If the running and administration of the IE was inept, then participants thought that they would quickly become disillusioned and not consider the meetings as being less or not valuable.

Example 2: Legal Barriers Affecting CERT Co-Operation

The second example presented here concerns information sharing between Computer Emergency Response Teams (CERTs). CERTs may be considered as fire brigades for cyber-space, having the priority for finding and fixing (remediation) of security incidents and restoration of service. ENISA's 2011 study into legal and operational barriers affecting CERT co-operation ran an online survey of 20 CERTs in Europe to gather evidence as to their frequency of information exchange. Knowledge of legal and regulatory factors and the extent to which these factors represented a barrier in real practice.[17]

Cross border information exchange between peer CERTs in Europe is not a rare phenomenon: just over half of those participating in the research reported participating sharing information with peers more than once per month.

One of the key challenges with regards to CERT co-operation in Europe is the conflicting demands imposed upon CERTs who are acting to maintain security following an actual or detected incident. To effectively co-ordinate a response and mitigate the effects of an incident, CERTs may need to impinge upon fundamental rights, especially given the somewhat unique nature of European legal framework, the right to the protection of personal data (given that the processing of IP address

data must respect certain legal obligations).

The research found that CERTs in general do not have access to legal expertise and thus, are confronted with a great deal of uncertainty regarding what they can and cannot do, not least because of the uneven implementation of European law in many areas. This uncertainty could lead to a number of consequences: ignoring the need to respect certain legal obligations; being overly restrictive in their response (ie. being extra cautious by withholding more information) or inefficient in response and co-ordination where a response may be delayed due to the need to seek definitive legal advice.

CERTs reported a number of legal frameworks as having a positive or negative effect upon information sharing including:

- The definitions of computer and network misuse (for example, not everyone used the 2001 Council of Europe Cybercrime Convention as a definitional framework).

- Privacy and data protection legislation might require in Europe one of a number of conditions to be met before exchanging certain types of relevant data for example IP addresses. Examples of these conditions might be that the consent of the person needs to be obtained or that they need to be informed.

Other specific frameworks could be involved such as public sector re-use of information (which imposes some obligations upon countries to publicly disclose certain types of information upon request). Laws relating to working with law enforcement (for example, certain forms of criminal procedural law imposing certain time-limits upon co-operation) and a range of others could apply.

Although many participants in this research reported familiarity with their own national frameworks, the level appeared less so with international legal frameworks (such as the aforementioned 2001 Council of Europe Cybercrime Convention) or the EU's 1995 General Data Protection Directive.

Example 3: Exchange of Cybercrime Related Information

The final example consists of evidence from law enforcement co-operation. Law enforcement units frequently collaborate on investigating, detecting cross border crimes such as different types of cyber-crime (fraud or scams, circulation of child exploitation material; credit card fraud and attacks against banking institutions). Many countries have a national level cyber-crime or high-tech crime unit but each has a varying approach to tackling cybercrime ranging from prosecuting as much as possible to more strategic approaches involving targeting particular suspects or operations. However, in order to identify, investigate and prosecute suspects, law enforcement needs to co-operate with a range of other types of organisation including CERTs; businesses (like financial institutions, Internet Service Providers) and citizens. As has been shown previously, CERTs may be trying to achieve different objectives after a cyber-attack: rather than preserving the scene of the crime they are more concerned with re-establishing service. The private sector may be reluctant to share information with law enforcement for fear that it will be disclosed, adversely affecting their reputation whilst citizens (who may be victims or witnesses) might be confronted with a wealth of potentially confusing ways to report incidents and co-operate with the police: either through online reporting mechanisms; a standard crime report or via intermediaries such as an Internet Service Provider.

To investigate these issues, as part of a feasibility study for a European Cybercrime Centre, research was carried out on the operation of police cyber-crime units across 15 European Union Member States.[18]

Amongst all of this, then, information sharing between peers in the law enforcement community can be fraught with difficulties. There are many different national interpretations of what constitutes cyber-crime – each country defines cyber-crime differently and may focus on specific phenomena. There are also difficulties in obtaining a truly pan European intelligence picture (since some countries are reluctant to contribute to a shared intelligence overview) because those being asked to contribute may consider there to be little return benefit or there might need to be attribution of results to the originating country: a complex issue in cross border investigations. Finally, the role of the public prosecutor is different in many countries. In some

countries the public prosecutor is responsible for actually deciding how the information may be used and so, if the case gets to court, the information obtained informally through a trusted mechanism may end up being publicly disclosed in a courtroom.

A number of barriers to the private sector co-operating with law enforcement were identified: not least the uncertainty that for many companies they felt that they were putting their reputation in the hands of the police (who in some cases were seen as less technically competent) when sharing information on cyber-crimes that they had fallen victim to. There is also a perception that they could fix the problem internally rather than alerting law enforcement – a decision seen as having little value overall.

From a consumer perspective as well as the multiplicity of reporting avenues a number of issues were identified in their co-operation with law enforcement, not least free riding and the ease in which some reporting mechanisms enable spurious or unimportant reports to be submitted causing further inefficiencies for law enforcement.

Conclusion

Each case study presents a textured picture of the realities of information exchange to address cyber-security, whether they be in the context of Critical Information Infrastructure Protection (CIIP); cross border co-operation between CERTs or law enforcement working to tackle cybercrime. When crafting responses to cyber-security issues and galvanising operational co-ordination, policy-makers need to be aware of a range of broad factors which may enable or inhibit information. To maximise the chances of these enablers being further supported and the problems caused by the barriers inhibited, policy-makers should take a multidisciplinary approach to understanding the phenomena of information exchange, bringing insights from economics, sociology, law, behavioural sciences and psychology.

Recommendations for the Republic of Korea

As we have seen, evidence from these three case studies could shed light on how evolving arrangements in the Republic of Korea might be most effectively organised to tackle the complex domain of cyber-security. In particular, the sharing of information through formal but also informal trusted networks is a key characteristic that would appear to be necessary. The success of the proposed "system for information sharing on cyber threats" will be driven by socio-economic factors as much as mere technical capability. Such mechanisms should be supported by appropriate incentives to encourage sharing, such as confidentiality agreements. These are especially important with regard to the private sector. Finally, within public administrations, the different cultures and working methods (across police; military; intelligence for example) may serve to encourage or inhibit information sharing: therefore effort should be focused on ensuring that any legislation takes account of these characteristics.

1. World Economic Forum (2012) Insight Report: Global Risks 2012 Seventh Edition: An Initiative of the Risk Response Network http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf.
2. ZDNet (2011) Cybercrime costs $338bn to global economy; More lucrative than drugs trade http://www.zdnet.com/blog/btl/cybercrime-costs-338bn-to-global-economy-more-lucrative-than-drugs-trade/57503.
3. Slashgear (2013) Three arrested for trying to cut undersea Internet cable http://www.slashgear.com/three-arrested-for-trying-to-cut-undersea-internet-cable-27275579/.
4. A version of this was also presented to staffers in the United States Congress in May 2012.
5. Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (Heraklion, Greece : European Network and Information Security Agency (ENISA), 2012); Robinson, Neil, Emma Disley, Dimitris Potoglou, Anais Reding, Deirdre May Culley, Maryse Penny, Maarten Botterman, Gwendolyn Carpenter, Colin Blackman and Jeremy Millard. Feasibility Study for a European Cybercrime Centre. Santa Monica, CA: RAND Corporation, 2012. http://www.rand.org/pubs/technical_reports/TR1218 and A Flair for Sharing - Encouraging Information Exchange Between CERTs (Heraklion, Greece : European Network and Information Security Agency (ENISA), 2011).
6. Blue House http://www.president.go.kr/activity/today.php?mode=view&uno=238.
7. *2008 Defense White Paper,* Ministry of National Defence, Republic of Korea, pp.192–219, 222.
8. *2010 Defense White Paper,* Ministry of National Defence, Republic of Korea, pp.8–10.
9. Woonyon, K (2005) Protection of Critical Information Infrastructure in Korea Presentation given to 13th ASEAN Regional Forum http://aseanregionalforum.asean.org/files/chive/13th/2nd%20ARF%20Seminar%20on%20Cyber%20Terrorism%20Cebu%20City,%20Philippines,%203-5%20October%202005/Annex%20H-Republic%20of%20Korea%20Country%20Report.pdf.
10. Blue House: http://www.president.go.kr/activity/today.php?mode=view&uno=238.
11. Blue House: http://www.president.go.kr/activity/today.php?mode=view&uno=238.
12. ENISA (2012a). *Threat Landscape Responding to the Evolving Threat Environment*. As of 29 July 2013: www.enisa.europa.eu/activities/risk.../ENISA...download/fullReport.
13. Dependability Development Support Initiative (2002) *Roadmap for Warning and Information Sharing* http://www.ddsi.org/htdocs/Documents/final%20docs/DDSI_D4_WIS_roadmap_f.pdf Leiden: Netherlands: RAND Corporation.
14. Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research,* 16(2) .
15. Messenger, M. (2006) Cyber-security: Why Would I Tell you? Research Briefing report version 0.3 February 2006.
16. ENISA, (2009). *Barriers and Incentives for Information Sharing for Critical Information Infrastructure Protection*. As of 19 July 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing.
17. European Network and Information Security Agency (2011b) *A flair for sharing - encouraging information exchange between CERTs.* Heraklion, Greece: ENISA. Retrieved 1 January 2012, from: http://www.enisa.europa.eu/act/cert/

support/legal-information-sharing/legal-information-sharing-1.

18. Robinson, Neil, Disley, Emma, Potoglou, Dimitris, Reding, Anais, Culley, Deirdre May, Penny, Maryse, Botterman, Maarten, Carpenter, Gwendolyn, Blackman, Colin and Millard, Jeremy, (2012). Feasibility Study for a European Cybercrime Centre, Santa Monica, CA: RAND Corporation, http://www.rand.org/pubs/technical_reports/TR1218.

Neil Robinson is a research leader at RAND Europe, working in such areas as European cybersecurity policy, cyber defence capabilities, and the broader socioeconomic implications of the Information Society. Robinson is presently leading a study for the European Defence Agency (EDA) taking stock of European military cyber defence capabilities. In 2012, he worked on a study for the European Commission into the feasibility of a European Cybercrime Centre (ECC), which informed the Commission decision to establish the ECC at Europol. In 2011 he worked on a project investigating the security, privacy, and trust implications of cloud computing and has also undertaken work into identity theft, cyberinsurance markets, and computer and network misuse. Robinson is leading RAND Europe's contribution to the PACT FP7 project, a pan-European empirical research project that aims to understand, measure, and monetise how individuals make privacy/security trade-offs. Robinson has also worked extensively on projects for the European Network and Information Security Agency (ENISA) in the domains of information sharing and exchange between Computer Emergency Response Teams and other stakeholders. Nationally, Robinson has advised a number of European government organisations including the UK Office of Cyber Security and Information Assurance (OCSIA) and Defence Science and Technology Laboratory, the French Interagency Joint Doctrine Centre (CICDE), and the Swedish Centre for Asymmetric Threat Studies (CATS). Robinson received his B.A. in war studies and history from King's College London and his M.Sc. in information systems and technology from City University London, where he studied the physical and logical vulnerability of fibre optic Metropolitan Area Networks.

MEMO

94340
9 791155 700150 비매품
ISBN 979-11-5570-015-0
ISBN 978-89-97046-06-5(세트)