Trends in Information Security

Topic Description: New Markets in CyberInsurance

Prof. Chris Johnson,
School of Computing, University of Glasgow.
Johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk

Introduction

It is impossible to guarantee that any complex system will be totally secure – new methods of attack are developed over time and new vulnerabilities are identified. Further problems stem from third party effects – where companies can suffer the knock-on consequences of cyber-attacks that focus on their suppliers or customers when they cannot directly affect the security of the computer systems operated by these external organisations. In consequence, there is a small but growing market in cyber-insurance. Companies can take out policies that will provide financial support during the aftermath of a cyber-attack. The policies can cover the costs of recovery; including any forensic analysis. They may also provide the income necessary for a company to remain in business until any threat is resolved. A host of questions remain to be addressed in this area – in particular it is hard for insurance companies to assess an appropriate premium given that they cannot easily quantify the risk of an attack on their customers – many previous incidents are not reported.

Different Perspectives

Some have argued that cyberinsurance increases the "moral hazard" that arises if companies decide not to invest in cyber security because they know they are covered by insurance. It is difficult to know if these fears are justified without further experience but it is an active area for research looking at the investment decisions that guide the technical implementation of mitigations. Other concerns focus on the role of government and private enterprise in the development of the insurance markets. There is a concern that a single attack could affect many different companies – this creates problems because insurance companies might be made bankrupt following such a "cyber storm". They might respond by raising premiums to the point where most companies could not afford them. In consequence, the Obama administration have discussed limiting liability – reducing the costs of cyber-insurance for companies that could demonstrate any breach or attack occurred in spite of following 'best practices'. Insurance companies could then be certain of the limit of their exposure for each claim. However, questions remain about who should pay for residual costs about the limit; the tax payers or by third party claimants? Others have argued that Governments might provide direct subsidies for cyber insurance premiums. This avoids artificial limits on liability. However, there are concerns that providers might raise the premiums they demand knowing that the increased costs will be borne by tax payers.

The introduction has argued that insurance companies find it difficult to set premiums because they cannot quantify the threat posed to their customers. One issue here is that there are few public reports on major attacks hence insurance companies cannot rely on the data about previous treats. In the US, the Obama administration has been urged by the Senate to create voluntary schemes for

reporting cyber attacks. In contrast, the 2013 proposals for a European Cyber Security directive favour more compulsory reporting schemes. Not only will this help the exchange of information about previous attacks it will also help insurance companies to understand their potential financial exposure to future attacks.

Open Research Questions

The cyber-insurance market is small but growing rapidly. There have been recent workshops organised by the US Department of Homeland Security and by the Generva Association of European insurance companies. These meetings have identified a host of research questions:

- Does cyberinsurance really increase the moral hazard of underinvestment in protection measures? What research methods might be used to help better understand the nature of the moral hazard?
- What tools and techniques might be used to assess the premiums to be paid by particular companies and how can these be linked to existing security threat assessment techniques?
- The Obama administration have argued that premiums should be reduced for companies that follow the state of the art in security practices, what are the appropriate audit techniques that might be used to demonstrate a company really did follow these leding practices?

References

European Commission, Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, 7.2.2013, JOIN(2013) 1 final.

European Network and Information Security Agency, Incentives and barriers of the cyber insurance market in Europe, June 2012, Heraklion, Greece.

J. R. C. Nurse, S. Creese, M. Goldsmith and K. Lamberts, Trustworthy and Effective Communication of Cybersecurity Risks: A Review, First IEEE Workshop on Socio-Technical Aspects in Security and Trust (STAST), Milan, Italy, Nov. 2011.

R. Raysman and P. Brown Computer Law: Drafting and Negotiating Forms and Agreements, Law Journal Press/ALM, New York City, USA, 2008.

US Department of Homeland Security, National Protection and Programs Directorate, Cybersecurity Insurance Workshop Readout Report, Washington DC, USA, November 2012.

US Securities and Exchange Commission, Division of Corporation Finance, Cyber Security: CF Disclosure Guidance: Topic No. 2, Washington DC, USA, October 13, 2011. Available on: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm