Research briefing

Measuring the harm caused by cyber crime to UK businesses

February, 2016

Sabina Enback and Sam Mason, SfJ Research

SfJ RESEARCH

The cost of cyber crime to the UK is estimated at £27bn per year[1] with recent years having seen an increase in recorded instances of cyber crime[2]. Even though cases of cyber crime are increasingly being recorded it is believed that these crimes are still under-reported[3,4,5]. It is thought that one reason for this is businesses being reluctant to disclose breaches in cyber security which in turn can lead to reputational damage [4,6]. Even though reputational damage is one of the main factors for not reporting cyber crime, quantifying the impact of such damage has been largely ignored.[7]

Reputation is essential for the long term survival of businesses; it is vital to creating and maintaining confidence and can determine why a customer chooses a certain company or product above others[8]. As many businesses now allow customers to make purchases online, customers and employees expect a company to protect sensitive information such as personal information, trade secrets and bank or credit card details from being accessed by hacking [9].

Reputational harm as a result of a security breach has been increasingly cited by businesses as having the biggest impact; this is linked to the increase in businesses reporting that

[1] https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report
[2] Wall, David S., & Williams, Matthew L., Policing cybercrime: networked and social media technologies and the challenges for policing, Policing and Society, 23:4, 409-412, 2013.
Available at: http://dx.doi.org/10.1080/10439463.2013.780222
[3] Wall, David S., Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime (Revised Feb. 2011) (July 3, 2008). Information, Communication & Society, Vol. 11, No. 6, pp. 861-884, 2008 . Available at SSRN: http://ssrn.com/abstract=1155155
[4] Heinonen, J., Holt, T., and Wilson, J., (2012), *Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics*, International Criminal Justice Review, Vol. 22: 353-371
[5] Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M.L. (2015) 'The Implications of Economic Cybercrime for Policing', City of London Corporation.
[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
[7] http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf
[8] http://www.cimaglobal.com/Documents/Thought_leadership_docs/cid_exrep_corporate_reputation_june07.pdf
[9] http://www.pwc.com/us/en/it-risk-security/assets/high-risk-data-discovery.pdf

breaches led to varying levels of media scrutiny[10]. While there is no unique measure to quantify such reputation losses, the following would provide estimates of the damage:

1. Loss in sales and profits
2. Loss in customer satisfaction
3. Reduction in stock prices (for publicly traded companies)
4. Business relations and access to credit
5. Supply chain relations
6. Corresponding changes in competitors' indices as in 1-3.[11]

The total loss to a firm following a cyber attack is of course larger. It includes loss in business from disruption, delays in service/delivery of their product as well as the resources spent in strengthening security. There are also costs in terms of the cost of security to prevent breaches. It is clear that a framework is needed to measure various cost factors and harm typologies in order to describe how losses are inflicted on both the short and longer terms.

[10] https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

[11] https://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb