EURIM DIGITAL POLICY ALLIANCE
informing policy for a competitive, inclusive, networked society

Cyber Security Working Group - Primer

May 2019

Cyber Insurance as a Catalyst for Good Security Practice

Introduction

The digitalisation of virtually all productive activity in everyday life brings with it a wide array of social and economic benefits. However, digitalisation also creates large and poorly understood risks which have the potential to cause economic damage, threaten the rights and safety of individuals and harm national security.

Managing cyber risk is consequently one of the greater public policy challenges we face, as represented by its place in the national risk register.

Insurance is a central element in risk management by both private businesses and the public sector. The OECD has acknowledged that cyber insurance, which is maturing, will be an important contributor to any comprehensive strategy to improve cybersecurity[1]. Understanding of the role played by cyber insurance in managing cyber risk is however limited and, in the UK, take up of appropriate cyber insurance cover, at 25% by larger businesses and only 9% of all businesses, is inadequate.

The duty to protect personal data brought in by GDPR, coupled with the Government's determination to enhance cyber security as well as the security challenges created by the Internet of Things, point to the need to encourage much greater and rapid take-up of cyber insurance.

The cyber protection gap

Affordability of premiums may be less of a critical issue than the design of policies which, to deliver value, need to be more closely aligned to the needs of any given sector and of individual businesses. Figures suggest that 43% of businesses have experienced a cyber security breach in the past 12 months[2]. This suggests that coverage is currently low relative to the risk they face.

Insurance and risk management

Risk management is at the heart of cyber security. Cyber insurance does a great deal more than simply pay claims in the event of a breach or cyber incident. Insurance companies provide practical advice and support to prevent breaches from happening in the first place as well as assistance when they occur.

[1] OECD (2017) Enhancing the Role of Insurance in Cyber Risk Management

[2] Cyber Security Breaches Survey 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701840/CSBS_2018_Infographics_-_General_Findings.pdf

The exact support and policy coverage provided by insurers to their customers will depend on the provider and the type and level of cover purchased. Core parts of cyber insurance nevertheless have some elements in common which can include: [3]

- Access to a suite of supporting services including risk management consulting services and legal and technical cybersecurity advice;
- In the event of a breach, rapid access to experts to help minimise the impact and restore capabilities securely; and, potentially, additional legal or PR support to help firms in navigating the reputational and other sensitivities that can result from cyber incidents.

Preventative support of this kind begins during the underwriting process, when there is an opportunity for firms to consider and address major vulnerabilities within their business, leveraging the expertise of their insurer. Support will typically continue throughout the duration of the policy by means of the provision of services such as online risk management support.

Experience tells us that even the most robust strategies around governance, training, processes, and technical IT security cannot eliminate cyber risk – it can only ever be prepared for and mitigated. For instance, training staff in appropriate behaviour makes a material contribution to good cyber security but will not, of itself, prevent rogue staff engaging in malicious activities. Furthermore, a survey in 2018 by Ponemon found that while the majority of data breaches in firms were the result of known vulnerabilities, a substantial minority (40%) resulted from ones that were unknown[4] to them.

Thus, engaging with and receiving advice from insurers can serve as a catalyst for organisations to enhance their preparedness for and mitigation of cybersecurity threats. Importantly, insurance also plays its traditional role of dealing with the cost of the incidents. Even an unsophisticated cyber-attack, such as ones involving ransomware, can prevent businesses from being able to access data and key digital assets for days or even weeks, thereby causing huge interruption to trading and significant losses. Businesses could also be faced with the cost of notifying and compensating for breaches of personal privacy. These financial impacts can quite easily overwhelm firms without appropriate insurance cover.

Public guidance

The Government has committed itself to making the UK the safest place to be online[5]. In the context of the ever-increasing cost and long term risk posed by cyber-attacks to the country's national security and economy we would encourage the Government to cover cyber insurance in future guidance. Recent guidance such as the 2017 NCSC guidance for small businesses does not mention insurance, nor does the 2017 Home Office Cyber Aware campaign[6]. The later 2018 aviation cyber security strategy[7]is also silent on the matter. Given the potential of insurance not only to reduce substantially damages arising from successful attacks, but also to act as a catalyst for good practice in cyber security, endorsement by the government of the importance of businesses taking up appropriate insurance would be valuable.

We also believe this would help the Government deliver its objective of making the UK, "the safest place to be online".[8]

[3] ABI (2016) Making sense of cyber insurance: A Guide for SMEs

[4] https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465

[5] https://www.gov.uk/government/news/government-outlines-next-steps-to-make-the-uk-the-safest-place-to-be-online

[6] https://www.cyberaware.gov.uk/

[7]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726561/aviation-cyber-security-strategy.pdf

[8] https://www.gov.uk/government/speeches/matt-hancock-speaking-at-the-launch-of-tech-nation