Information Security Now – 46

IT Risk Insurance

John Mitchell & Bee Kalsi

I was once discussing business continuity with the CIO of a large insurance company. When I identified that he did not have a viable plan he shrugged his shoulders and said that he had insurance for such an eventuality, he was, after all the CIO of an insurance business. I asked to see the policy and after a long wait it was eventually produced. He was covered to the tune of £50,000, but only for 'recovery of data'. In today's money, we are talking in the region of £250,000, but the point is that the policy covered him solely for data recovery and not the cost of interruptions that did not involve data loss. He admitted to never having read the policy, but defended this stance on the basis that his legal representative had said it was fine; thus, confirming the adage that a little knowledge is a very dangerous thing. Things may have moved on a bit in the last few years, but does your CIO and indeed your insurance company really understand the extent of the risks now faced by IT and the consequence to the business[1]? The challenges for both sides are the following: knowing what is to be covered; understanding the efficacy of the business's current IT security framework; the likely damage to be incurred; the recovery cost. It should also be noted that many of the recently reported security breaches were by companies that were accredited to the PCI/DSS[2], which indicates either a certain slackness in the standard itself, or non-compliance with it. Cyber insurance is the insurance industry's response to the growing global cyber threat. It is important to note that cyber insurance is not the answer to all security issues, but rather part of a toolkit which will allow a business to defend itself against the threats, and reduce the impact from such threats. Those of you with a knowledge of risk management's four Ts will recognise insurance as being in the Transfer/Treat areas[3].

What Cover?

Using risk management techniques is a good way to analyse what insurance cover you may require. Identifying your company's exposure to the standard confidentiality, integrity, availability and compliance threats and the efficacy of your controls will provide a solid framework for discussions with your insurance provider. Although insurance is viewed as a means of transferring risk, it does no such thing. The risk remains with you. All you have really done is to outsource dealing with the consequence side of the risk equation. As this is after the event it does not help you with the likelihood component, so the onus remains with you to take sensible precautions. It is also worth noting that you cannot get insurance for criminal acts, so the recent diesel-gate scandal, where software was written to fool the regulators, will not be covered. Your company is unique and you require a tailored policy to suit your needs. There is plenty of

---

[1] In 2016, 2.9 million British companies were hit by some sort of cyber-crime at a total cost of £29.1 billion (https://www.beaming.co.uk/press-releases/cyber-security-breaches-cost-businesses-30-billion/).

[2] Payment Card Industry/Data Security Standard

[3] Tolerate, Terminate, Treat, Transfer

choice when it comes to providers. Lloyds alone has over 70 cyber risk insurers and there are other large players in the field. Their websites are a useful starting point in understanding the level of cover you may need.

Should you have a cyber claim you should be covered for the costs of dealing with it. The question being how much will be covered? Ideally, this should include the costs that arise through dealing with a security breach, support against ransomware and loss of income if a cyber-attack interrupts your business operations. If your business suffers a data breach you should be covered for alerting your customers and protection against the costs of handling and investigating it. You should also expect to receive 24/7 support to help manage the impact of a cyber-related incident and have access to specialist support and advice for IT, legal, forensic and media relations handling. If a business has taking onboard the National Cyber Security Centre's 10 steps to cyber security[4], or is accredited to one, or more, of the relevant international standards such as ISO 20000[5] or ISO 27000[6] then it enhances the likelihood of obtaining a preferential premium.

Financial Risks

The financial risks to businesses are well documented. A cyber event can remove a business's access to essential information systems and crucial data. Some businesses, especially small ones, may be forced to close whilst dealing with the repercussions. Costly and time-consuming security overhauls may be required to prevent the attack from re-occurring and staff may need to be re-trained. Databases could be wiped and/or files corrupted to the point where a business can no longer operate. These financial risks are not restricted to the short term. A cyber-event can affect a business for a long period, with customers opting to choose a perceived more reliable provider. Some of the figures from recent cyber breaches are staggering. It is estimated that a recent hack of a telecommunications provider cost the company £60 million and reduced their customer base by one hundred thousand.

Non-Financial Risks

Cyber-events are not limited to financial losses. The impact is often far wider. Reputation is a key risk to those who have suffered a cyber-attack and significant short-term reduction in share price is to be expected. A successful invasion of a company's IT infrastructure leads to a loss of trust from both current and potential customers/partners. Customers will be concerned if their personal data and information is leaked and they could be affected by subsequent identity theft. Time must be spent investigating the breach to mitigate any immediate issues. This could be done by either internal or external parties, which could delay the implementation of other projects across the business.

What may not be covered

As with any insurance policy, it is crucial to review not only what is covered by your insurer but what is excluded under the agreement. Cyber related threats are complex and hard to predict, making the risk and its impact difficult to assess. The policy wording or structure can influence the outcome of a claim.

---

[4] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[5] Service Delivery

[6] Information Security Management

Most exclusions in cyber insurance are the same as those found in other insurance policies such as war and terrorism, although there is a fine line to be drawn between kinetic and cyber war/terrorism. Some exclusions to consider are: *Jurisdiction* **-** while policies purchased in the UK normally include territories in the European Union and much of the rest of the world, the United States and Canada are often excluded; *Claims by Related Entities* - whilst cyber insurance will protect your business from loss of customer data and any claims which arise because of this loss, policies do not normally include the claims for the loss of employees' personal information. This exclusion normally extends to contractors and even to partially owned subsidiaries; *Bodily Injury and Property Damage* - digital asset replacement clauses will cover losses in the digital sphere, but will not usually cover damage to physical property, or bodily injury which results from a cyber incident.

A final thought. What cover do your outsourced service providers have? Are you included in theirs and are they included in yours?

John is is currently Workshop Liaison for the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)7774 145638

Bee is an IT Risk & Compliance Analyst for an insurance company.