Shutterstock: Royalty-free stock vector ID: 1425918233

Nov 27, 2019 23:37 GMT

The do’s and don’ts of cyber security insurance

By Sourya Biswas, Technical Director

Cyber security does not exist for its own sake; it’s ultimate aim is to help businesses manage risk. Risk Management 101 tells us there are four possible ways to respond to a risk.

- Risk avoidance - avoid the risk by avoiding the associated activity
- Risk acceptance - accept the risk by depending on the risk and

cost to mitigate
- Risk mitigation - reduce the risk by implementing controls
- Risk transfer - shift risk to another party through a contract.

While the full responsibility for the risk cannot be transferred, its impact can be reduced. Enter cyber insurance. Last year, the global cyber security insurance market was valued at $5.5 billion, and is expected to grow at 26.5% every year for at least the next decade.

Read it again: 26% yearly growth for a decade. That translates to a potential valuation of an astounding $58 billion by 2028. But how effective is cyber insurance in reality?

In 1943, IBM Chairman Thomas Watson remarked, “I think there is a world market for about five computers”. We’ve come a long way since then. Today, computers connected to the World Wide Web are an integral part of every company in every industry. With cyber attacks becoming more and more common, it’s not surprising that the popularity of cyber insurance has increased in leaps and bounds.

Does insurance provide a false sense of security?

While there’s no clear regulatory requirement to be insured, companies have embraced cyber insurance as an additional layer of assurance to cover loss of business, regulatory penalties, and digital forensics costs. What cyber insurance truly amounts to is FUD protection—a way to alleviate fear, uncertainty, and doubt post breach.

So, how does cyber insurance work? And do they always pay out? In short, a cyber insurance policy is an insurance plan designed to protect from liability and losses related to IT (traditional policies usually don't include any kind of protection from digital threats). While insurers companies cite that 90% of claims are paid out, and most to full coverage amounts, there have been instances where claims have been contested.

Mondelez International. In June of 2017, the American confectionary giant was hit by the global outbreak of the NotPetya malware that froze its logistics software and ultimately shaved 0.4% off the company’s annual revenue of $25.9 billion, a $180 million loss. Mondelez filed a $100 million

claim with Zurich Insurance under their cyber insurance policy, a claim that was denied under the "war exclusion" clause.

Since US and UK researchers had identified NotPetya as a state-sponsored effort by Russia to undermine Ukrainian infrastructure, the insurer argued that the attack on Mondelez was an "act of war" and hence, not liable to be paid out under the terms of the policy. The matter is currently still being battled in court.

National Bank of Blacksburg. On May 2016 and January 2017 (yes, twice), the bank was targeted in a 'coordinated criminal enterprise and bank robbery' in which attackers gained access to bank computers using phishing emails, defeated security controls, and withdrew money at hundreds of ATMs for a total loss exceeding $2 million.

The insurer, Everest National Insurance, refused to pay out the claim under the bank's computer and electronic crime insurance, arguing that the incidents were covered under the insured's debit card policy (which had a significantly lower payout). The matter went to court and was confidentially settled in 2019.

Medidata Solutions. The data management company was hit by a social engineering attack in September 2014, when employees from Medidata's finance department were tricked (by emails purportedly coming from a company executive) into transferring $4.8 million to a fraudulent bank account in China.

The company's claim under their cyber insurance policy with Federal Insurance Company was declined because the insurer stated that there was no manipulation of in-house computers and the funds were transferred 'voluntarily'. After a four-year judicial battle, the court ruled in favor of Medidata, a decision that was upheld on appeal.

Navigating cyber security insurance at your organization.

In some cases, insurers may believe (and rightfully so) that they're being unfairly maligned; however it's safe to say there are some important lessons we can take from the incidents above.

Do involve both your Security and Legal teams.

Cyber security professionals are not lawyers and most lawyers don't have expertise in cyber security.

Security and Legal teams should work together to choose the right cyber security insurance, coming together to review their choices at least once every year.

Even better, consider employing the services of a cyber security lawyer, since they are hyperspecialized in dealing with cyber risk. This not the time or place to be picking from dropdown options on a website form.

Don't cheap out when choosing a cyber insurance provider.

I can't think of a situation where the popular adage of "you get what you pay for" applies more than with cyber security insurance. In other words, choose insurance coverage depending on your business needs and possible impact of a cyberattack, not on how low the premium is. Pay special attention to exclusions and riders.

Don't let cyber insurance make you complacent.

You might think that just because you've purchased cyber insurance, your company can become lax in implementing security programs. After all, you're covered, right? Wrong. Cyber insurance is a safety net that should ideally be employed only under the most difficult of situations.

Take car insurance, for example. You wouldn't start driving on the wrong side of the road just because you have excellent auto coverage, would you?

Do establish good security practices.

Using the previous example, there is not a single insurance company that would cover auto theft if they were to find out that you left your car unattended with the key in the ignition. Similarly, not responding to an evolving threat environment can actually put your company in violation of what cyber insurers refer to as 'due care' requirements.

Organizations must have the minimum cybersecurity programs and processes in place for standard blocking/tackling, as well as demonstrate they have been operating as intended. These include patching, monitoring, password strength, encryption, secure processes, and so forth.

Do supplement your security with external assessments.

Every organization has a unique risk profile for which cyber insurance should be leveraged, but only in combination with a solid cyber security program. At NCC Group, we help clients identify where their greatest threats lie and how to address them through the implementation of appropriate security mechanisms or controls.

We also provide insights from the perspective of the attacker via our penetration testing services. By simulating real-world exploitation of inherent weaknesses in the client's ecosystem, we help validate the effectiveness of existing controls and find gaps to remediate before an actual attacker gets in.

Instead of relying solely on cyber security insurance, focus on prevention, mitigation, and response.

You essentially buy cyber insurance to minimize the impact from a exploited gap in your cyber security posture. The Catch-22 here is that your insurance provider will demand you plug your cyber security gaps. Should we not just focus on simply establishing good security practices in the first place?

Cyber insurance is not a panacea to cyber security issues; in fact, it's a reactive mechanism that comes with several terms and conditions attached. That makes it less impactful than proactive measures like implementing security controls commensurate with applicable risks and then testing them in real-world scenarios. As any physician will tell you, 'prevention is always better than cure.'

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted

by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750