Cybercrime Insurance. A growing market. Are you covered?

Overview

It's estimated that cybercrime now costs the global economy more than USD $600 billion each year[1] – with no sign of slowing down. As the world continues its digital transformation, the threat landscape is becoming ever more complex – with a broadening footprint that includes cloud-based services, myriad mobile devices, and the internet of things. Organizations are increasingly reliant on the interconnectivity of systems, and hackers have become sophisticated at exploiting software vulnerabilities and networks. A combination of factors including high-profile security incidents, the mandatory requirement to report breaches, and legislation such as the EU's General Data Protection Regulation (GDPR), means there's a growing global interest in cyber insurance policies. And with Organization for Economic Co-operation and Development (OECD) figures predicting that the cost of cybercrime will reach USD $2 trillion by 2019, it's inevitable that insurance is now a key consideration for businesses.

"Cybercrime is a costly, hard to detect and difficult to combat threat. From an insurance perspective, while analogies are often made with terrorism or catastrophe risks, cyber risk is in many ways a risk like no other."

Insurance 2020 & beyond: Reaping the dividends of cyber resilience, PwC

The demand for cyber insurance is therefore growing at an unprecedented rate and recent reports indicate that the global market for policies will hit USD $14 billion by 2022.[2] Yet it's a market still in its infancy with penetration levels still relatively low in some countries, particularly in smaller businesses, and a recent report indicates that 62 percent of all organizations globally still don't have a dedicated cyber insurance policy in place.[3]

As with all types of risk, organizations often look for ways to minimize their financial exposure should the worst happen – and cyber insurance policies seem a logical step. But insurers are becoming less likely to impose blanket terms and conditions. Instead, they will require a much fuller assessment of the policyholder's vulnerabilities, processes, risk mitigation solutions and response plans.

This paper looks at the cyber insurance market, the need for expert advice and the steps that organizations can take to ensure that they fully understand their own data risks and security vulnerabilities before taking out a policy.

A complex threat landscape

Cyber criminals are continuously discovering new ways to exploit vulnerabilities and technology. Although researchers and companies are working hard to remain one step ahead of attackers, we will never prevent all potential attacks. We're living in a world where threats are developing faster than the technologies we use every day. As a result, many organizations take out cyber insurance policies to transfer the financial risks associated with attacks, and insurers are challenged to underwrite these policies and provide recommendations.

"99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident."

Gartner

Cyber insurance is growing. In fact it's said to be one of the few areas of growth and innovation in the insurance market these days[4], but it's still a relatively untapped opportunity for insurers with maturity levels varying across the globe. And there is no standard approach on which the industry underwrites cyber liability cover. Some markets are more mature than others – approximately 90 percent of all cyber insurance is purchased by US organizations[5], whereas only 2 percent of UK companies have taken out standalone cyber insurance.

It's a minefield of ambiguity and there are many examples of insurers failing to pay out, based on small print and complex policy interpretation. Inaccurate

1. McAfee and the Center for Strategic and International Studies (CSIS), Economic Impact of Cybercrime — No Slowing Down 2. Allied Market Research, Global Cyber Insurance Market Report 3,7. NTT Security Risk:Value 2018 Report 4. PwC, Cyber security insurance – how can insurers quantify the risk? 5. PwC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience

information can void a policy, and claims continue to be denied where the information supplied has proven to be inaccurate.

An organization must demonstrate to the insurer the protective steps it has taken – both to assess and reduce risk in the first place, the steps it is taking to continuously monitor and manage these risks, and the incident response plan it has in place should a breach occur. Only then can an insurance company begin to understand its exposure.

Organizations considering taking out cybercrime insurance should think carefully about what they expect the policy to deliver. How do you know if you are adequately covered? Could your policy be invalidated? And what cybercrime safety measures would insurers expect you to have in place?

The dawn of cyber resilience evaluation

In a recent announcement, one group of organizations has collaborated to offer enhanced cyber insurance coverage in conjunction with secure technology from Apple and Cisco and a cyber resilience evaluation from London-based Aon. Customers who deploy the relevant technologies and hardware after engaging in the evaluation can become eligible for enhanced cyber coverage from Allianz, including lower deductibles. It's an interesting move and one that raises a number of questions about the direction the insurance market is heading.

If similar 'enhanced' cyber coverage policies become the norm, will this mean that the insurer will dictate the choice of information security providers and what would happen to your contractual obligations to incumbent suppliers? And if insurers are providing their own incident response teams, how do these compare with experts working in the information security sector with whom you may already have a relationship?

Risk:Value 2018 research findings

- One third of respondents do not expect to suffer from a breach
- 47% believe that their organization has never been breached
- 62% of respondents do not have a dedicated cyber insurance policy
- 22% of organizations have company insurance that covers only data loss

Of those organizations with a cyber insurance policy in place:

- 47% think that failure to maintain or apply updates would invalidate their policy
- 36% believe that their lack of an incident response plan would invalidate their policy
- 29% think that lack of employee care and attention would invalidate their policy

Don't ignore the small print

For now, these collaborations are still the exception rather than the rule and, given the complexity of policies, the best advice for people seeking cyber insurance is to seek professional help to navigate the small print in the policies.

Far too often, organizations take out cyber insurance without checking the fine detail. Many policies are taken out without sufficient research into what's available, what the costs are and what is covered. Policy terms are not dictated by regulators and no standard language has yet been adopted by the industry. Policies vary too, with some very well publicized disagreements where insurance providers have rejected claims based on their own interpretation of the fine print.

For example, does the policy cover data if it's held by a third party or in the cloud? Will the policy pay out if your organization has failed to keep up with security updates? How about if former employees still have access to your systems? Are you covered if the breach came via an employee's own device? And what happens if the original breach predates your policy, yet you were unaware that your systems had been infiltrated some months previously? NTT Security research[6] reveals that nearly 21 percent of vulnerabilities detected in client networks were more than three years old and over 5 percent were more than 10 years old.

It's all but impossible to cover yourself 100 percent. If you're unsure about the fine print – seek legal counsel.

Protection is key – but whose responsibility is it?

Rather than relying solely on an insurance policy to cover all losses, businesses need a different game plan: by all means buy insurance to cover some of the losses, but at the same time, take measures to reduce the potential for loss. Many organizations will lay the responsibility firmly at the door of the IT department – yet NTT Security's Risk:Value 2018 report highlights that there is no single executive role that is surfacing as ultimately responsible. IT security should be about more than just the hardware and software. It needs to be embedded in the culture of the organization, championed by the CEO, designed and executed by the CISO and communicated effectively so that every employee takes responsibility for ensuring that good practices are followed. Again, Risk:Value 2018 indicates that 61 percent of employees are not fully aware of their company's information security policy. And if your organization relies on the services of third-party contractors and suppliers, you need clear guidelines to ensure that all third parties are aware or equally accountable for your security policies and practices.

This may not prevent a third-party related security incident, but it would be good practice to ensure that everyone is at least aware of what is expected of them.

"No insurance policy will protect an organization's brand or reputation."

Garry Sidaway, SVP Security Strategy & Alliances, NTT Security

Choose your policy with care

Businesses of all sizes will rely on their IT infrastructure to some degree, exposing themselves to the risks of business interruption, income loss, plummeting share prices and reputational damage if systems fail or are interrupted. Yet organizations are not adequately insuring themselves against attacks, and in recent years we've seen a number of high-profile court cases with insurers rejecting cyber-related claims under more traditional policies. When contested, the courts have, in the majority of cases, sided with the insurers. General professional indemnity policies don't generally provide any of the first-party cover offered by a cyber insurance policy and it's this first-party cover that will include loss of business income as well as crisis management support (PR, legal advice, forensic investigators, IT specialists) to minimize the impact of the breach. Don't assume that your public liability insurance will cover all the costs associated with a data breach – it almost certainly won't.

6. NTT Security Global Threat Intelligence Report 2017

Assess your risk exposure

What is important to insurers is that clients have a complete understanding of their risk exposure. Without this, it's impossible to create a policy that is relevant for your business. Our recent global survey[7] indicated that just 57 percent of organizations have an information security policy in place.

A first step in protecting your organization against potential threats is to fully understand your risk exposure across all areas of the organization, ensuring industry best practice is considered. There's a growing global shortage of cybersecurity skills, so if you don't have the skills in-house, take expert advice and consider a comprehensive evaluation of your company. This will highlight areas of risk, make recommendations, prioritize actions and help you build a strategic road map for continuous risk management. A full assessment would highlight gaps in your IT security armor and show you the critical areas that need immediate attention. And an evaluation summary would give a timeline for carrying out any remedial actions required. This could then be shared with your insurer as evidence that you are taking security seriously.

Are you ready for cyber insurance?

Threats are constantly changing and so should your defensive testing. Taking out insurance however, is not a substitute for ensuring that your organization is adequately protected – no more so than taking out home insurance and leaving all your doors and windows unlocked.

Our claims data showed that 67% of cyber claims in 2017 involved human error.
Hiscox

What is important is to understand the risk exposure of your organization and knowing how you will respond should a breach occur. In its annual Cyber Readiness Report, insurer Hiscox measured the cyber readiness of organizations based on the quality of their strategy. Nearly three-quarters of companies fell into the 'cyber-novice' category, suggesting they have some way to go before they are cyber ready. Only 11 percent qualified as experts.

Cybercrime protection, best practice

1. **Understand your risk** – conduct an annual risk assessment exercise to understand your current risk exposure. Maintain the board's engagement with cyber risk.
2. **Fix known vulnerabilities** – keep hardware and software protection up to date – persistence pays off for the cyber criminal. Stay on top of basic protection.
3. **Home and mobile working** – set robust guidelines for data access. User-owned devices are increasingly being used to for day-to-day business. Protect your network regardless of the device accessing it.
4. **Education and training** – ensure your employees know your policies and incident response processes by implementing a full security awareness program including, where practical, poster campaigns, regular advisory emails, new starter security inductions and annual computer-based training.
5. **Incident management** – establish, produce and routinely test incident management plans.
6. **Monitoring** – continuously monitor all ICT systems and associated logs to spot and act upon potential attacks.
7. **Secure network** – manage the network perimeter and filter out unauthorized access.
8. **Malware protection** – establish anti-malware defenses and continuously scan for malware.
9. **Manage user privileges** – limit user privileges and monitor user activity.
10. **Establish employee ground rules for use of social media** – social media is becoming a primary path for cyber criminals. Give your employees the ground rules for acceptable use at work and guidance on secure online behavior outside work.
11. **Perform security assessments** on third parties during the procurement process and at least annually, to monitor compliance to your organization's security requirements, as well as legislative and regulatory controls.
12. **Establish and maintain a formal risk management process** – ideally adopting an internationally-recognized standard.

Understanding your risk will mean understanding your security vulnerabilities relating to processes, people and technology, and is a first step in moving your organization towards cyber readiness and being ready for a conversation with an insurer.

Be proactive

The risk of attack will never diminish and the sophistication and frequency of attacks is growing.

Socially engineered malware, social media threats, APTs and phishing all continue to threaten organizations. However, the exploitation of known vulnerabilities is still the root cause of most information security breaches today. Gartner estimates that zero day vulnerabilities account for only 0.4 percent of all attacks over the past decade, whereas 99 percent of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident.

Proactively prioritizing patching will deal with the biggest cause of breaches and data loss and demonstrate to insurers that your organization understands the most effective approach to risk mitigation and prevention.

If you do decide to take out a cyber insurance policy, you are making a commitment to transfer risk and ultimately reduce any costs associated with as yet unknown attacks. Yet, underwriting these policies is still a challenge for insurers and organizations must do everything possible to understand their exposure and take appropriate steps to mitigate risk. This includes demonstrating to insurers that information security and risk management is top of the agenda.

Conclusion

Insurance policies are not a license to be reckless and it should not be a surprise that policies are written in such a way as to avoid covering high-impact scenarios that could be easily prevented. Similar to home insurance, coverage against cybercrime does not replace preventative measures to deter criminals and secure your home – such as setting your intruder alarm or keeping expensive items such as laptops, tablets and smartphones out of plain sight, away from windows.

A smart business will implement a security framework that includes both technological and process controls and better staff training to prevent breaches, and consider an insurance policy only as a supplement to its own solid risk-based security program, not a replacement for it.

Organizations need to invest in both protecting assets in the first instance, and also in transferring any risks via appropriate insurance cover should an attack occur. These are not mutually exclusive requirements: it's important to have prevention measures in place before you go on to insure your assets.

And perhaps more collaboration between insurers, third-party experts and companies that have been breached would help all parties. Due to the sensitivity of information, insurers are often reluctant to share details of their incident history and security measures. Unfortunately the industry learns nothing this way, meaning underwriting accuracy won't improve – and that's to nobody's benefit.

Companies that want to transfer some of the risk of a breach will increasingly turn to cyber insurance. Unfortunately, they will not always get what they think they're paying for.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.