TRAVELERS

Building Resilience to Cyber Risk

The five steps you need to know

Building Resilience to Cyber Risk

Cyber Security + Cyber Insurance = Cyber Resilience

Cyber risk has emerged as one of the most important risks facing businesses in the 21st century. In 2009, there were 2.4 million new pieces of malware created. In 2015, more than 430 million new pieces of malware were discovered—over a million new pieces of malware each day.[1] Targeted attacks increased by 55% in 2015, and adversaries increasingly targeted smaller businesses, which were subjected to 43% of all spear phishing attacks.[2] Data breaches and business interruptions due to cyber attacks have become a key concern for businesses, when their systems and networks are hit.

Part of the solution is better cyber security, but when hackers can penetrate the networks of Fortune 500 companies and high-profile government agencies, no ordinary business or organisation can presume that it cannot be breached. For the unprepared, the cost of a breach can be crippling. In 2015, the global average per-company cost of a data breach reached $3.5 million.[3] Cyber insurance provides a way for businesses and organisations to spread risk and, consequently, to be more resilient than they otherwise would be. By combining cyber security and cyber insurance, businesses and organisations can achieve greater cyber resilience against emerging cyber threats. A business or organisation is cyber resilient if: (1) it has implemented a cyber security programme that reasonably protects its information assets (taking into account the value of those assets and the surrounding threat environment), and (2) it has obtained cyber insurance that is reasonably sufficient to protect against residual cyber risks. Here are five critical steps towards achieving cyber resilience.

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[3] https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

Five Steps Towards Cyber Resilience

1. Know your data, systems, and network

The first step towards cyber resilience is to "know thyself." Know what (and where) data are being created, collected, and stored; maintain an accurate inventory of computer systems and software; and understand your network infrastructure. This will enable you to better identify and prioritise appropriate security controls, patch and maintain existing systems and software, and respond more effectively when an incident occurs.

Email remains the medium of choice for cyber criminals. Phishing attacks were more targeted, and malicious emails grew in number and complexity.[4]

2. Focus your cyber security efforts

Once you understand the data, systems, and network that you are trying to protect, you can focus on implementing (or improving) the security controls that would be most effective in light of your specific needs and resources. In doing so, you may want to consider the following:

- **What are your crown jewels?**
  If you have adopted a data classification scheme, you may want to implement stronger security controls for the storage and transmission of data that are classified as more sensitive.
- **What are your vulnerabilities?**
  A vulnerability assessment can help identify weak spots in your cyber security. If your organisation permits systems or network access to outside parties, such as contractors or vendors, understand that their vulnerabilities become your vulnerabilities.
- **What are the most likely threat scenarios?**
  If you understand the threats that are most likely to impact your business or organisation, you can focus on meeting those threats.

Compliance with a particular cyber security standard is not a prerequisite to achieving cyber resilience, but it can be important in determining which security controls to implement. Businesses that handle payment card information, for example, must comply with the PCI Data Security Standard.

3. Educate your employees

Many cyber security incidents can be directly attributed to inadequate security awareness training. A training programme designed to empower employees to recognise common cyber threats and to notify the IT staff is a cost-effective way to reduce these threats.

A comprehensive training program should:

- Emphasise the importance of cyber security to the business or organisation's success.
- Train employees to avoid information security risks.
- Explain how to protect laptops, mobile devices, and digital storage media.
- Encourage employees to report suspicious activity.

Employees should also receive training on policies and procedures that relate to cyber security. In many instances, explaining the rationale for restrictive "system use" policies will help to promote greater compliance.

[4] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

4. Plan for incident response

Every business or organisation should plan for the unexpected, including a data breach or cyber incident. In fact, without an incident response plan, there is a greater likelihood of making mistakes in responding to the breach or incident—for example, by failing to comply with applicable laws and regulations. Such mistakes can cause damage to the business or organisation that goes beyond the damage directly caused by the attack. A well-designed incident response plan will make it easier to launch a rapid and coordinated response.

The incident response plan should provide a framework for action so that important decisions have been considered ahead of time and are not made under pressure. In particular, it is important for the incident response plan to provide procedures and guidelines on difficult issues, including identifying lines of authority and internal reporting obligations. The team should be focused on making the best possible decisions, not on figuring out how and by whom the decisions need to be made.

Once you have an incident response plan in place, it is important to test it regularly—annually, if possible. These "tabletop" exercises should involve the full incident response team, and the results of the exercise should be made available to senior management. It is better to address issues that might be raised by senior management about the incident response plan in connection with a tabletop exercise — not in the midst of an actual incident response effort.

> The last five years have shown a steady increase in attacks targeting businesses with less than 250 employees.[5]

> Not only can cyber insurance products help transfer some of the risks associated with cyber threats, but the insurance underwriting process can help identify cyber security vulnerabilities and improve cyber security.[6]

5. Insure against residual risk

Strong cyber security is just one part of the equation; obtaining cyber insurance is the other. According to UK Government's Cyber Security Breaches Survey[7], only 11% of all UK businesses have specific cyber insurance. This figure does increase for medium and larger firms, but only to 31% and 35%, respectively. According to the Association of British Insurers, "The rise in the number of large and medium sized firms having cyber insurance reflects greater awareness of the value of this cover, as insurers play a vital role in supporting customers to recover from an attack, and in helping them manage the cyber threat. But we need to do more to promote this insurance to smaller firms, who are often the least protected against cyber criminals."[8]

Once a business or organisation knows its systems and data and understands its exposures, it will be well-positioned to work with an independent insurance agent or broker to evaluate its cyber insurance needs and to obtain coverage in this fast-growing insurance market.

Visit **www.travelers.co.uk/cyber** for more cyber security tips for your business.

[5] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[6] http://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf
[7] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019
[8] https://www.abi.org.uk/news/news-articles/2019/04/abi-responds-to-dcms-cyber-security-breaches/

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

TRAVELERS

Cyber insurance

Protecting a client's technology investment means reacting fast to a constantly changing landscape.

First, you have to know what's coming. Make sure they're covered and prepared for every stage of an incident – before, during, and after.

Second, you'll need to know the right people. Cyber risk isn't a simple subject. But it's simple enough to get in touch with the experts.

Third, know what they need. From indemnity for 1st and 3rd party losses across data and regulatory, to extortion, work interruption, and fines and penalties.

We're here to help your clients safeguard their digital technology and celebrate its power. Are you ready?

Insuring Ambition

travelers.co.uk/cyber | 01737 787787

Travelers operates through several underwriting entities through the UK and across Europe.
Please consult your policy documentation or visit the websites below for full information.
travelers.co.uk | travelers.ie