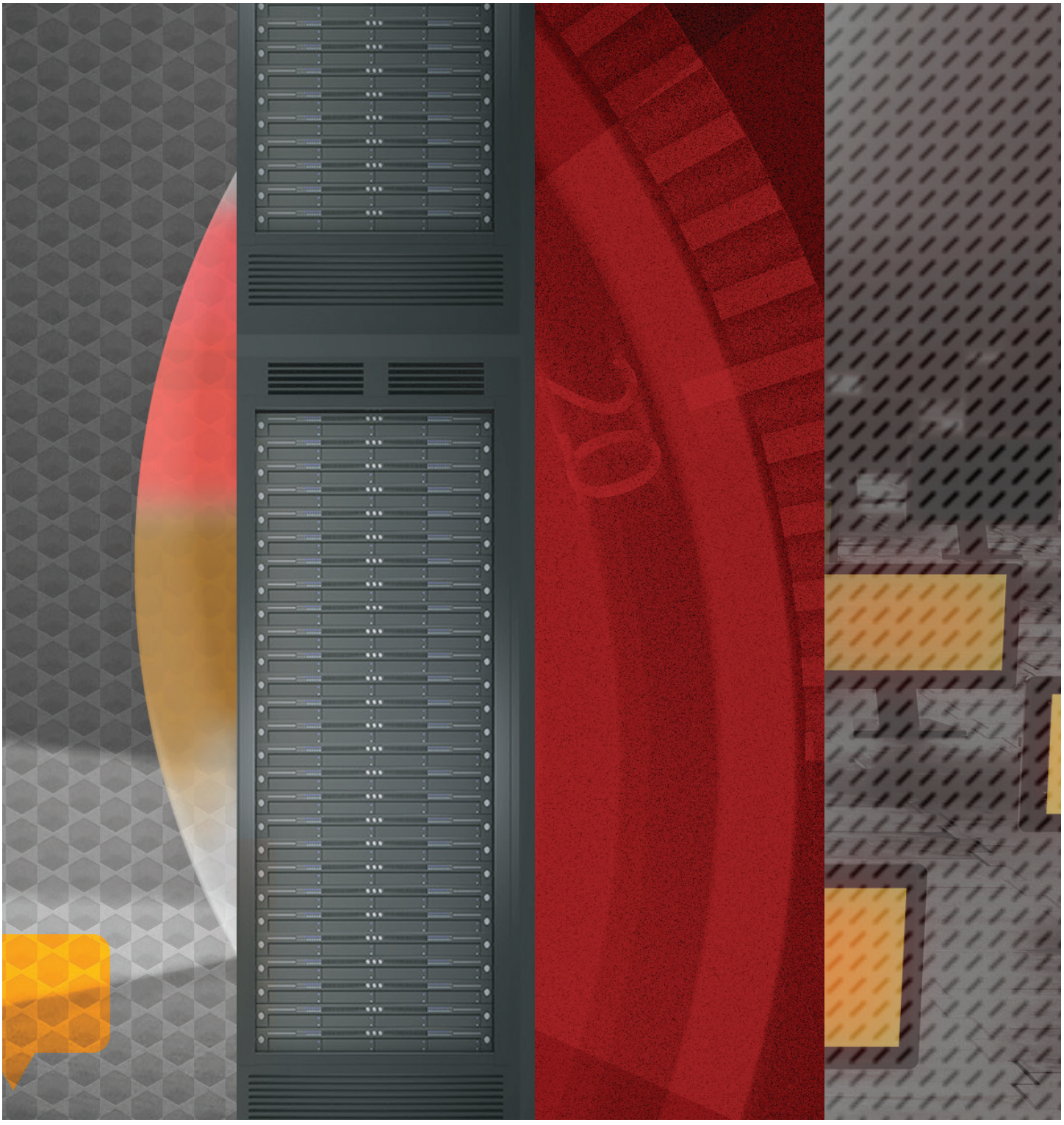
Symantec

TRAVELERS

Building Resilience to Cyber Risk



BUILDING RESILIENCE TO CYBER RISK

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 organization can presume that it cannot be breached. For the unprepared, the cost of a breach can be crippling. In 2015, the average per-company cost of a data breach reached $3.5 million.[3] Cyber insurance provides a way for businesses and organizations to spread risk and, consequently, to be more resilient than they otherwise would be. By combining cyber security and cyber insurance, businesses and organizations can achieve greater cyber resilience against emerging cyber threats. A business or organization is cyber resilient if: (1) it has implemented a cyber security program 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.

Cyber Security + Cyber Insurance = Cyber Resilience

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 prioritize appropriate security controls, patch and maintain existing systems and software, and respond more effectively when an incident occurs.

[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

2) Focus your cybersecurity 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 organization 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 organization, you can focus on meeting those threats.

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

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 program designed to empower employees to recognize common cyber threats and to notify the IT staff is a cost-effective way to reduce these threats.

A comprehensive training program should:

- Emphasize the importance of cyber security to the business or organization'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 organization 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 organization 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.

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

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.

5) Insure against residual risk

Strong cyber security is just one part of the equation; obtaining cyber insurance is the other. According to the American Bankers Association: "As cyber risks grow, the senior management and boards of directors of companies have increasingly focused on a holistic response to cyber threats that includes risk mitigation, risk transfer, and response/recovery. This holistic approach necessarily includes insurance."

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]

Once a business or organization 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.

[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

TRAVELERS AND SYMANTEC: HELPING BUSINESSES BECOME CYBER RESILIENT

Travelers has engaged Symantec, the global leader in cyber security, to provide an array of valuable pre-breach risk management services to CyberRisk, CyberFirst® and CyberFirst Essentials® policyholders. While the exact services will vary depending on the policy, businesses and organizations can use these services, combined with existing pre-breach services already offered by Travelers, to become more cyber resilient.

Symantec™ Cyber Resilience Readiness Assessment and Cyber Security Professional Consultation

This unique online assessment tool was created to help businesses and organizations move towards greater cyber resilience. It allows a business or organization to quickly assess its current cyber security posture, which will be documented in a written report with benchmarks against other organizations. In addition to the report, Travelers policyholders are eligible to receive up to a 1-hour consultation with a Symantec™ cyber security professional that will help explain the results of the assessment and address areas of weakness or vulnerability.

By taking advantage of this service offering, a business or organization can better understand its data, systems, and network, and can focus its cyber security resources where they will be most effective in protecting against cyber threats.

Symantec™ Cyber Security Awareness Training Videos

This collection of innovative security literacy and role-based training videos are specifically designed to help businesses and organizations educate their employees about cyber security. Businesses and organizations can reduce vulnerabilities while creating an informed corporate culture and influencing employees to protect critical information assets from exploitation, cyber-attacks, unauthorized access, and fraud.

Symantec™ Security Coach Helpline

The Symantec™ Security Coach Helpline provides professional cyber security advice to aid businesses and organizations in strengthening their cyber security programs. The helpline allows policyholders to schedule a consultation with a Security Coach who will provide guidance to a business or organization that is preparing or testing an incident response plan. The Security Coach can also answer general questions about cyber security, such as “What types of data should be encrypted?” or “What are some best practices for securing mobile devices?”

Symantec™ Service Discounts

Symantec™ is also providing discounted rates on a variety of products and services that can substantially improve the cyber resilience of a business or organization.

A business or organization that has identified a need for improved security controls, for example, may benefit from one or more of the following:

- Norton™ for Small Business Software offers a comprehensive, easy-to-manage security solution for up to 20 devices, including workstations, laptops, smartphones, and other mobile devices.

- Phishing Readiness service, which helps educate employees to identify and avoid falling victim to the latest social engineering attacks by launching and tracking the results of phishing simulations launched against employees of your firm.

Finally, businesses and organizations may find that they are already generating a significant volume of alerts and other security-related data, much of which is not being adequately monitored and analyzed. In that case, the most pressing need may be to improve incident detection capabilities. By using Symantec™ Managed Security Services, businesses and organizations will benefit from 24 x 7 x 365 security monitoring and real-time security analytics, equipping them with the strategic insights needed to prioritize and respond to the most critical incidents and to build strategies to protect their assets and reputation.

ACHIEVING CYBER RESILIENCE

The impact of a significant cyber attack can be devastating to any business or organization. Unfortunately, no silver bullet exists to prevent attacks, and breaches can occur in spite of a business or organization's best efforts at preparation and protection. By adopting a holistic approach to cyber risk management that includes cyber security with cyber insurance, businesses and organizations will improve their cyber resilience and their ability to respond and recover quickly from an attack.

Certain services are being provided to you by Symantec and in using them you must agree to Symantec's terms of use and privacy policy. Travelers Casualty and Surety Company of America and its property casualty affiliates ("Travelers") make no warranty, guarantee, or representation as to the accuracy or sufficiency of any such services. The use of the services and the implementation of any product or practices suggested by Symantec or NetDiligence is at your sole discretion. Travelers disclaims all warranties, express or implied. In no event will Travelers be liable in contract or in tort for any loss arising out of the use of the services or Symantec's or any other vendor's products.

Coverage provided by Travelers Casualty and Surety Company of America and its property casualty affiliates. Hartford, CT 06183.

This paper is for general informational purposes only. It is not designed to be comprehensive and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or other professional adviser. This material does not amend, or otherwise affect, the provisions of any insurance policy issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy provisions, and any applicablelaw. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.