This content brought to you by Travelers

Travelers Cyber Academy – Cyber Insurance_ Protect and Prevent

(SPEECH)
[MUSIC PLAYING]

(DESCRIPTION)
Computer graphics twinkle behind the text, Access Key Required. A starred-out password is typed. A male figure holds an icon of a lock. Text, Travelers Cyber Academy - Cyber Insurance: Protect and Prevent.

(SPEECH)
SPEAKER 1: In today's challenging threat environment, cyber insurance provides important financial protections against a range of different risks. Lost or stolen data is just the start. Cyber insurance may also help to protect against fraud, extortion, and business interruption losses. A good cyber policy provides more than just financial protection, however, it also provides pre-breach services that can help a company prevent losses and post-breach services that can help minimize losses when a cyber incident occurs.

(DESCRIPTION)
Text, What we'll cover today.

(SPEECH)
In today's session of the Travelers Cyber Academy, we will review coverage provisions that are available in most cyber insurance products, including those offered by Travelers. Cyber insurance typically helps protect against first-party losses, such as expenses associated with conducting a digital forensic examination and complying with breach notification statutes, as well as third-party liability, such as responding to lawsuits or inquiries from regulatory agencies.

We will also describe different coverage scenarios to illustrate who needs cyber insurance and why. Finally, we will review pre-breach services that can help companies prevent losses, not just pay for them.

(DESCRIPTION)
Threat word cloud.

(SPEECH)
Cyber insurance helps to protect businesses and organizations in a complex and ever shifting threat landscape. If just one of these threats gets through a business or organization's defenses, the result could be a costly data breach, a disruption of business operations, regulatory inquiries, or lawsuits, or all of those.

(DESCRIPTION)
Insurance coverages.

(SPEECH)
Cyber insurance can provide both first-party coverages, which helps protect against losses that result from a cyber incident, as well as third-party coverages, which helps protect against liability claims, litigation, or regulatory inquiries that may follow from a cyber incident.

Let's start by reviewing some of the first-party coverage provisions that may be available.

(DESCRIPTION)
Remediation and Notification.

(SPEECH)
Data breach remediation and notification coverage helps to protect a business when a data breach occurs. There are different kinds of events that can trigger this coverage, including unauthorized access to confidential information of others, such as PII, PHI, or PCI that is being collected, stored, or used by the business.

When coverage is triggered, the policy responds by providing reimbursement for legal consultation with a breach coach as described in the earlier Traveler's Cyber Academy session-- "After The Breach, Whom to Call, What to Do." Where appropriate, the policy will also provide reimbursement for digital forensic investigations, which may be needed to determine the scope of the breach and the number and identity of affected individuals, and for notification expenses, including the cost to draft legally sound notification documents and to establish and maintain a call center to handle customer inquiries. The policy may also cover the cost of providing credit or identity monitoring services to the affected individuals.

The limits and deductibles for this coverage are typically expressed in dollar amounts, but coverage may also be available on a per affected person basis. In other words, a business could obtain remediation and notification coverage up to a specified number of affected individuals, rather than a specific dollar amount. Purchasing coverage on an affected individuals basis can be useful for businesses that would prefer to determine the potential number of affected individuals, rather than the potential cost of notification for those individuals.

(DESCRIPTION)
Coverage considerations.

(SPEECH)
Coverage for remediation and notification expenses is needed by businesses and organizations of every size and sector, if a business or organization has employees, for example.

The IRS recently warned about a scheme to steal W-2 information in order to commit tax fraud. The IRS described the scheme as one of the most dangerous email phishing schemes seen in a long time, one that has evolved beyond the corporate world and is spreading to other sectors.

(DESCRIPTION)
Alert quote.

(SPEECH)
In a hypothetical claim scenario involving a manufacturing company and 300 stolen W-2 forms, the net diligence data breach cost calculator estimated potential cost to the company in excess of $200,000.

Similarly, this coverage is important for any business or organization that accepts or processes credit or debit card payments, that collects or handles protected health information under HIPAA, or that collects, stores, or uses any personally identifiable information. A business or organization cannot simply assume that it has not suffered a data breach because it has not detected one. Most data breaches are discovered by a third-party, such as a law enforcement agency or an outside cybersecurity vendor.

(DESCRIPTION)
Cyber extortion.

(SPEECH)
As described in the Traveler's Cyber Academy session on ransomware, criminals have also turned to extortion as a way of profiting from the compromise of the computer system or computer network. Cyber extortion

coverage can help a business or organization that has fallen victim to ransomware by providing reimbursement for the costs of investigating a ransom demand, retaining legal counsel or other assistance in negotiating the ransom demand, and if necessary actually paying the ransom.

(DESCRIPTION)
Business interruption.

(SPEECH)
A business or organization may also suffer a loss of income when its computers and networks are attacked or compromised. This can happen, for example, when systems become infected with ransomware or through something known as a denial of service attack. In a denial of service attack, the business or organization servers are flooded with fake traffic in order to block legitimate traffic and impede normal business operations. Business interruption coverage helps protect businesses and organizations when their computers and networks are targeted by ransomware, denial of service attacks, and other malicious activity. Whereas, business interruption coverage addresses attacks against the business or organization's own network assets.

A related coverage known as contingent business interruption protects against attacks or outages relating to the network assets of third parties on which the business or organization depends. Examples of such third parties include website hosting providers or cloud service providers. Both business interruption and contingent business interruption provide reimbursement for extra expenses incurred in order to mitigate losses, for example, by temporarily transferring critical web applications to a different server.

(DESCRIPTION)
Coverage considerations - D.D.o.S. key.

(SPEECH)
Every business or organization that relies on data or computers in the course of its operations should consider obtaining business interruption and cyber extortion coverage. According to Symantec's 2016 Internet Security Threat Report, denial of service attacks are growing in number and intensity and are likely to continue increasing.

As to ransomware, hospitals and health care providers have been the most recent high-profile victims. But Symantec Special Report on ransomware in businesses found that almost every sector has been affected by ransomware in recent years.

(DESCRIPTION)
Pie chart.

(SPEECH)
The most frequently hit sectors in order were service industries, manufacturing, financial, public sector, and wholesalers. Ransomware, of course, may result in losses both from the extortion itself as well as business interruption loss.

As ransomware, denial of service attacks, and other cyber threats continue to evolve and become more sophisticated, prudent businesses and organizations can look to cyber extortion and business interruption coverage to help protect against those threats.

(DESCRIPTION)
Fraud coverage - payment screen on tablet.

(SPEECH)
Cyber insurance may also include coverage for computer fraud and funds transfer fraud. Computer fraud

involves the unauthorized use of a business or organization's computers to conduct a fraudulent transaction. Funds transfer fraud addresses fraud committed through spoofing, which does not necessarily involve the use of a business or organization's computers. In spoofing, a criminal poses as an employee and sends an email message or other electronic communication to a bank in order to conduct a fraudulent transaction. Coverage for social engineering fraud in which an employee of the business or organization is tricked or persuaded by a criminal to transfer money may be found in crime policies or other Travelers Insurance products.

(DESCRIPTION)
Claim scenario.

(SPEECH)
Fraud coverage is important for businesses and organizations that engage in business to business transactions involving wire transfers or other forms of electronic payment. Consider, for example, a scenario in which a criminal hacks into a company's accounts payable system and adds a new payee, causing a $350,000 payment to be sent without the company's knowledge. In this scenario, coverage for computer fraud could help protect the company from a potentially crippling financial loss.

(DESCRIPTION)
Restoration.

(SPEECH)
Finally, whether a cyber incident involves ransomware or some other malicious activity, there may be significant costs associated with recovering lost data, repairing damaged operating systems, and restoring applications and other important software files. Computer program and electronic data restoration coverage can help a business or organization defray these expenses, whether caused by a virus, a hacker, or even a disgruntled employee.

(DESCRIPTION)
Third Party.

(SPEECH)
In addition to protecting against their own first-party losses, businesses and organizations should obtain protection against third-party liability, such as lawsuits and regulatory investigations. The types of third-party coverages that are available include the following.

(DESCRIPTION)
Network and I.S. Security.

(SPEECH)
First, network and information security liability provides coverage against claims that allege a failure to prevent the transmission of computer viruses or other malware; a failure to protect confidential information of others, including PII, PHI, or PCI; a failure to provide access to authorize users; and a failure to comply with data breach notification obligations. This coverage also protects against claims that a business or organization failed to comply with its own privacy policy with respect to the protection of personally identifiable information.

(DESCRIPTION)
Media Liability.

(SPEECH)
Communications and media liability coverage helps protect against claims alleging copyright infringement, trademark infringement, trade dress infringement, and similar violations; infringements of an individual's right to publicity, including using an individual's likeness or appearance for commercial purposes without

authorization; and defamation, libel, slander, and other forms of reputational harm. Coverage can be obtained for all the communications of a business or organization or specifically for claims based on email communications, social media platforms, internet websites, or other forms of electronic media.

Finally, regulatory defense coverage provides protection in the event that a data breach results in a formal administrative or regulatory proceeding by, for example, the Federal Trade Commission or by the Department of Health and Human Services Office for civil rights. Coverage may also be available for resulting regulatory fines and penalties.

(DESCRIPTION)
Coverage considerations.

(SPEECH)
Nearly all entities that collect or store personally identifiable information should consider obtaining network and information security liability coverage to protect against the risk of being sued in the event of a data breach. According to the 2016 cyber claims study by Net Diligence, legal defense and settlement costs were included in approximately 10% of all cyber claims, with average total costs more than $900,000.

In addition, regulatory defense coverage is critical for businesses and organizations that handle the confidential information of others, such as PHI, PCI, or PII. In particular, the regulatory environment is fast-paced and constantly changing. In March 2017, for example, the New York State Department of Financial Services finalized cybersecurity regulations that establish comprehensive requirements for financial institutions and affiliates, changing how those companies will be affected by a cybersecurity event.

Also regulatory investigations can be costly in a hypothetical claim scenario involving a health care provider and 750 stolen patient files the net diligence data breach cost calculator estimated potential cost to the health care provider following a regulatory investigation in excess of $400,000.

(DESCRIPTION)
Fines and Assessments.

(SPEECH)
Coverage is also available for businesses and organizations that receive, handle, or process payment card information. As described in the Traveler's Cyber Academy session, "It's in the Cards, Payment Card Security," those entities may be required by contract to pay fines, fees, or assessments in the event of a breach of PCI data. This coverage helps to protect against the cost of conducting PCI forensic investigations, resulting fines, fees, or assessments as well as charge backs for fraudulent activity relating to stolen PCI. Depending on the extent of the breach, these costs can range into the millions of dollars.

In addition, if a business or organization systems are found to be non-compliant with the PCI data security standard after a data breach, coverage may be available for the costs associated with coming into compliance and for obtaining a qualified security assessment in order to establish compliance.

(DESCRIPTION)
Errors and Omissions.

(SPEECH)
Companies that produce or provide technology goods or services should also consider obtaining errors and omissions coverage or tech E and O. This coverage provides financial protection against third-party claims, which may include claims that relate to technology products that do not meet required specifications, software that is buggy and is not performing as expected, or technology services that are not meeting customer expectations, resulting in financial harm to the customer or other third parties.

(DESCRIPTION)
Exposure.

(SPEECH)
In determining what kind of coverage is needed by a business or organization, here are some of the fundamental questions to consider. What sensitive information does the business or organization collect or store? This can include information obtained from customers, from employees, and from other businesses or individuals. How sensitive is the data? Certain kinds of information are inherently more valuable or more likely to lead to lawsuits or regulatory inquiries than others.

How is sensitive data to be collected, used, shared, and disposed of? Data that is widely shared, for example, whether within a business or with outside parties, is obviously more vulnerable to compromise. And what systems or data does the business or organization depend on? If the operations of a business or organization rely on critical applications, data centers, or cloud services, there is likely a need for robust business interruption coverage.

(DESCRIPTION)
Good insurance provides a package of benefits.

(SPEECH)
The good cyber insurance policy will provide more than just financial protection. It will also provide access to other benefits, such as pre-breach services that can actually help a company prevent losses. According to the 2016 Cost of Data Breach Study by the Ponemon Institute, the average cost of a breach was lower for businesses that carried cyber insurance than for businesses that did not.

(DESCRIPTION)
Four pairs of hands work on laptops.

(SPEECH)
Here at Travelers we offer a range of cyber insurance products that fit the needs of businesses of all shapes and sizes. CyberFirst Essentials covers small businesses, including tech companies and professionals. CyberFirst focuses on mid to large technology companies and up, as well as public sector entities CyberRisk covers everything else, from private and non-profit entities financial institutions, going up to the largest publicly held companies.

Additional information about these products can be found at www.Travelers.com/cyber or from your local independent insurance agent or broker.

(DESCRIPTION)
Pre-Breach Services.

(SPEECH)
In April 2017, Travelers announced that it engaged Symantec, one of the world's leading cybersecurity companies, to provide an array of valuable pre-breach services for Travelers cyber insurance policy holders including one or more of the following, depending on the type of policy purchased.

Access to a cybersecurity assessment tool that can help businesses and organizations better understand their current cybersecurity posture, what is being done well, and where improvement is needed.

Cybersecurity awareness training. Employees who have been educated about cyber threats are the strongest defense against both internal and external attackers. Educating your entire organization not only helps to minimize potential attacks, but can reduce internal security accidents.

Discounts on cybersecurity products and services, such as Norton for small business software, DeepSight Intelligence, and Symantec Managed Security services.

Access to cybersecurity expertise, through white papers, cybersecurity updates, or live access to a cybersecurity coach.

(DESCRIPTION)
Policy, Protect, Business and Secure graphic.

(SPEECH)
In sum, cyber insurance is an important risk management tool for businesses and organizations to use when addressing cyber risks. This is especially so as other lines of insurance are more regularly excluding coverage for cyber related incidents. However, coverage terms and availability can vary widely. So it is important for a business or organization to work with a trusted independent insurance agent or brokers to obtain coverage appropriate to its specific needs.

(DESCRIPTION)
How a business can protect itself.

(SPEECH)
A business or organization can better protect itself by understanding the cyber risks that it faces, by working with a trusted independent insurance agent or broker to obtain cyber insurance with appropriate first-party and third-party coverages. A business an organization can also benefit from the valuable pre-breach services that a good cyber policy provides to help improve its cybersecurity.

(DESCRIPTION)
Contact email and information link.

(SPEECH)
Thank you very much for your time today. We hope you enjoyed this session of the Travelers Cyber Academy on "Cyber Insurance, Protect and Prevent." If you have any further questions, please contact us at TRVCyber@ems.travelers.com. Or for a replay of this session to share with your colleagues and find additional resources on this topic, please visit travelers.com/cyberadvantage.

(DESCRIPTION)