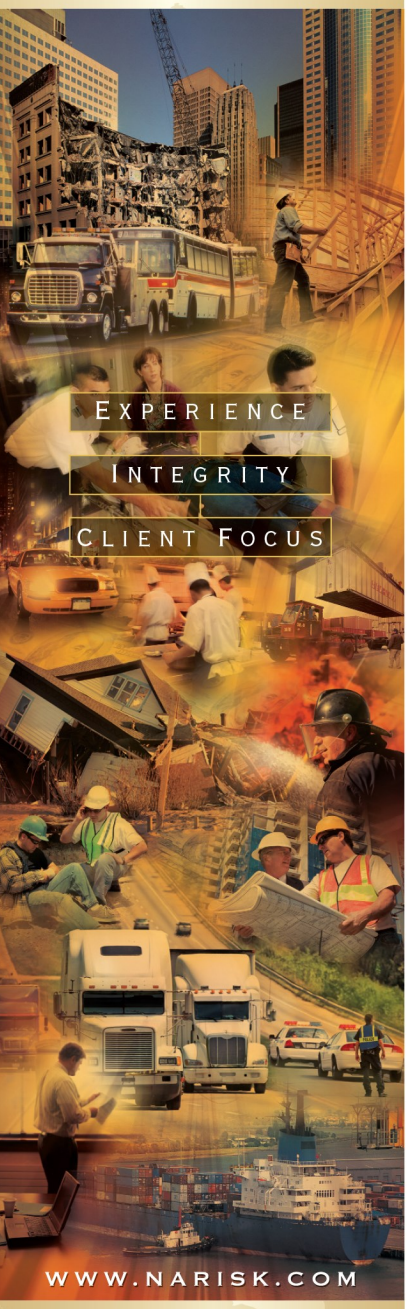
NARS
North American Risk Services



Cyber Security: Choosing Tailored Insurance Products & Proactive Cyber Risk Claims Considerations

Travis Allen
Senior Claims Adjuster, Liability

In today's increasingly sophisticated era of cloud computing and data driven business, cyber threats are an omnipresent risk faced by enterprises of all sizes with respect to the potential for electronic data breaches. These risks can be first party, whereby a company's own information is breached, or third party, whereby data belonging to a company's customers, with which a company has been entrusted, becomes compromised.

Consider the following scenarios:

- A hacker infiltrates a company's network, stealing sensitive data, proprietary business information and the credit card numbers of numerous customers
- An employee inadvertently disseminates private customer information, placing the company's clients at risk
- A server containing critical transactional information is wiped clean prior to cloud backup due to a virus.
- During business travel, a company laptop containing client billing data vanishes
- Ransom-ware is installed on the company server by way of a malicious email link, scrambling important documents

The reputational and economic damage posed by all of these situations hold the potential to ruin a business and the litigation that often results from such scenarios are typically not covered under most standard property and general liability policies.

The Solution

Commercial general liability policies now often include cyber exclusions, necessitating the purchase of specialized cyber insurance packages for larger enterprises. Some smaller businesses with lower revenue thresholds may also be able to endorse coverage into their existing commercial general liability insurance policies.

These policies and endorsements typically cover damages related to the management of incidents, investigation, remediation, legal costs and regulatory fines. Additional coverage parts also exist for cyber extortion incidents and data breach expenses that cover, among other things, credit monitoring services. As there are numerous options available, businesses should work with their respective

brokers to effectively customize coverage solutions most appropriate to fit their individual needs.

Cyber coverage is still in its relative infancy, having first debuted in the late 1990s, and as such, there is often little standardization between package policies. The sector is growing tremendously however; cyber insurance premiums are projected to burgeon from $2 billion in 2015 to upwards of $20 billion by 2025 and there are now 50+ carriers worldwide able to offer $500 million in capacity.

Once a business has equipped itself with the appropriate coverage and the peace of mind that comes with it, what additional steps can be taken to prevent the occurrence of cyber threats?

Prevention

During his 1962 State of the Union Address, John F. Kennedy astutely remarked, "The time to repair a roof is when the sun is shining." Consistent with this preparatory philosophy, a number of avoidance steps and preventative measures can be employed to minimize the potential for cyber risk. Applied within the parameters of a company's corporate security policy, as well as within compliance with state, federal and international privacy/data security laws, implementation of the following measures can serve to reduce the likelihood of a breach:

- Ensure portable media and devices are always encrypted with strong authentication measures
- Use up to date anti-virus, anti-spyware and firewall software and diligently work to make certain all operating systems and software platforms receive regular security patch updates
- Make sure passwords are changed routinely and are sufficiently complex, incorporating a combination of numbers, symbols, capital letters and lower case letters. Avoid dictionary words or combinations of dictionary words to prevent brute force cracks, programs that automatically try dictionary lists of user names and passwords to gain access
- Require network administrator privileges for the installation of new programs
- Employ a robust email filter to ensure malicious items are quarantined and direct all personnel to never click on embedded email hyperlinks of any kind received from unknown sources
- Closely scrutinize and vet any third party vendors entrusted with sensitive information
- Segregate machines tasked with handling confidential information from those utilized for routine services
- Consider enlisting the services of an ethical hacker from a reputable firm to check for security breaches, detect vulnerabilities and render recommendations for additional safe guards and fortification measures
- Develop and test incident response plans to be deployed in the event of a breach

Mitigation

Even with the most vigilant implementation of preventative best practices, cyber risk is not unlike any other risk in that it cannot be eliminated entirely and the potential for breaches invariably still exist. With this in

mind, in the wake of a breach-triggering a claim, what can be done to mitigate the severity of a loss, streamline its handling or expedite its disposition?

- Upon detection, take immediate steps to contain and neutralize the attack, re-secure the system and thwart further infiltration consistent with the pre-planned incident response protocol
- Assess the degree of damage and/or the nature and extent of potentially compromised data
- Promptly place the cyber liability carrier on notice
- Furnish to your adjuster and/or agent all pertinent activity logs. Assure that all such activity logs and historical network records and hardware are preserved to assure no spoliation of evidence in the event it becomes necessary for a forensic IT team to conduct a review
- In the event of a breach involving a non-technological failure (i.e. lost equipment, human error), also provide your adjuster and/or agent with the full name and contact information for the employee(s) involved while making advanced arrangements for he/she to provide a formal statement
- Consider residual damage control measures such as offering a credit monitoring services for affected customers
- If a loss involves a business interruption component, assemble pertinent documentation to submit to the carrier

In summation, selecting an appropriate cyber coverage, by way of standalone policy or endorsement, while an important decision, is only half the battle. Once this initial hurdle is cleared, adherence to the aforementioned operational guidelines can serve to reduce the frequency of claims and minimize the severity of losses if they do occur. These prevention and mitigation recommendations are not comprehensive and will often vary depending on the risk profile specific to a particular company, its employees and its clients.

ABOUT THE AUTHOR

Travis Allen is a Senior General Liability Claims Adjuster at NARS. Travis has over a decade of diverse claims and risk management experience, having presided over hundreds of high-exposure litigated liability cases for both carriers and self-insured Fortune 500 companies.