EPIC®
Insurance Brokers &
Consultants

CYBERSECURITY RANSOMWARE

WHAT IS RANSOMWARE?

Ransomware is malware hackers use to access and then lock down companies' networks. Once an attack infiltrates a network through phishing emails, malvertising, contaminated links, portable storage devices, or other means, the ransomware holds data hostage from its owners by encrypting the files. Organizations are then forced to pay a ransom or recreate data from clean backups, if available. In the interim, businesses are prevented from accessing any of their data and using computers for work.

EXAMPLES OF RANSOMWARE

- **SamSam:** This ransomware exploits vulnerabilities in servers in order to access victims' networks. The commonality in these attacks is the word "sorry" in ransom notes.
- **Ryuk:** Used for very customized attacks, hackers perform extensive research on their target before the breach. The infection tends to be small-scale but hits crucial assets or resources at a company.
- **LockerGoga:** Although relatively rare, LockerGoga uses targeted hacking techniques to not only gain control of system but of physical equipment as well. The results of these hacks can be both catastrophic and physically dangerous.

REDUCING THE RISK OF A RANSOMWARE ATTACK

Cybercriminals are advancing their techniques faster than we can defend against them. Here are some key elements of any Cyber Security protocol to mitigate this growing risk:

- **Employee Training:** While it may be impossible to eliminate exposure to human error, methods such as mandatory seminars, regular training, and phishing test emails are effective in mitigating the risk.
- **Incident Response Readiness:** Companies should create procedures to minimize business interruption and limit potential damages. In addition to ensuring you have a strong incident response plan, you should test the plan regularly, in the same way you conduct fire drills.
- **Insurance Coverage:** Today, many traditional insurance products include some cyber coverage. However, in most instances, the coverage provided in those products is very narrow in scope. Stand-alone cyber insurance policies offer a broad range of first and third party coverages intended to protect an organization in the event of a ransomware attack. A comprehensive cyber insurance policy is a key element of any cyber risk management program.

DON'T BE A STATISTIC

Companies surveyed by Allianz for its 2020 Risk Barometer ranked **cyber incidents** as their **#1 risk**

50% of cybersecurity professionals feel their **ransomware** security is inadequate[1]

Ransomware costs businesses over **$75 billion** each year[1]

Ransomware attacks have increased over **97%** from 2017 to 2019[1]

34% of businesses that experience malware attacks take a week or more to recover[1]

CLAIM EXAMPLE

In December 2019, New Orleans was hit with a ransomware attack, after a series of attacks during 2018 and 2019, on other municipalities including Albany, NY and Atlanta, GA. The damages are expected to exceed their $3M cyber insurance policy.

More recently, in January 2020, the foreign currency exchange company Travelex was infiltrated by ransomware. In response, Travelex was forced to shut down all of their systems in order to remediate and control the malware. As of the release of this advisory, Travelex is not disclosing the extent of the damage or the demands made by the cybercriminals.

[1] PhoenixNAP: Global IT Services 2019, 27 Terrifying Ransomware Statistics & Facts You Need to Read, 31 January 2019 https://phoenixnap.com/blog/ransomware-statistics-facts

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond procured by EPIC. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

© EDGEWOOD PARTNERS INSURANCE CENTER | CA LICENSE 0B29370

EPIC Insurance Brokers & Consultants

CYBERSECURITY

RANSOMWARE

INSURANCE SOLUTIONS FOR RANSOMWARE PROTECTION

CYBER COVERAGE

Cyber risk mitigation involves taking proactive steps to protect against and reduce the adverse effects of the key risks to your organization. Implementing network security defenses, incident response plans and employee training are all essential elements of cyber risk mitigation. Unfortunately, this is not enough. The reality is, no organization is immune from a cyber-attack, regardless of the strength of their defenses. This is where insurance can help. Comprehensive stand-alone cyber insurance will help protect the organization's balance sheet by transferring some of the costs associated with the inevitable breach.

Cyber insurance complements and supports active security measures by providing third-party regulatory and liability coverage as well as a host of first-party response, remediation and recovery insurance. In addition, most cyber markets also provide free or discounted pre-loss services to assist an organization in breach preparedness.

Specifically, in the case of ransomware, insureds should look for coverage which includes digital restoration and extortion coverage. As mentioned above, try to avoid "inadequate security exclusions".

RISK MANAGEMENT TIPS

- Develop, implement and regularly update and test a holistic incident response plan that includes IT, HR, Accounting Staff, Security and Management
- Appoint a Computer Information Security Officer
- Identify, contain and protect any Personal and Corporate Confidential or Sensitive Information.
- Continually maintain and upgrade computer systems and software
- Implement mandatory employee training to better prevent phishing, unauthorized transfer of funds, or unwitting data breach
- Encrypt all mobile devices

CRIME COVERAGE

Commercial Crime insurance provides first-party coverage intended to help an organization recoup losses due to employee dishonesty, theft of money or securities, robbery, burglary, forgery and alteration, and theft of client property. In addition, Commercial Crime policies also typically include coverage for Computer Fraud, Wire Transfer Fraud and Social Engineering Fraud. Today, many stand-alone cyber policies also include similar or identical coverage extensions. This means there is a potential for overlapping and/or redundant coverage. Organizations should strive to coordinate coverage between stand-alone cyber and crime policies in order to ensure they are able to maximize potential insurance recoveries in the event of an incident.

In addition to the above, most commercial crime policies also provide a limit for investigation costs for covered loss, assisting the insured in paying for the complex process of determining the extent of the loss once the fraud has been uncovered. Coverage is typically on a loss discovered basis, meaning that the cumulative loss over time, regardless of when it took place, is covered by the policy in place when the loss is discovered.

RISK MANAGEMENT TIPS

- Establish an anti-fraud policy and code of conduct, with a hotline for employees to call if they suspect fraudulent activity. Conduct anti-fraud training and procedures for employees, managers and executives
- Conducting external audits of internal controls used in financial reporting
- Maintain multi-person controls in accounting and inventory
- Vet, update and purge approved vendor lists at least annually

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond procured by EPIC. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

© EDGEWOOD PARTNERS INSURANCE CENTER | CA LICENSE 0B29370