SANS

Analyst Program

Whitepaper

# Avoiding or Minimizing Ransomware Impact to the Bottom Line

Written by **John Pescatore** and **Benjamin Wright**

May 2021

Gigamon®

# Introduction

Although the mainstream media has only recently focused on ransomware, attacks date as far back as 1989. Ransomware attacks became more widespread in 2009, and they have continued to morph and cause damage (see Figure 1). In most ways, ransomware is simply another form of malware that requires well-known, essential security hygiene controls to avoid or minimize damage. However, the rapid DoS impact and accompanying extortion demands warrant a careful review of detection and incident response processes and controls.

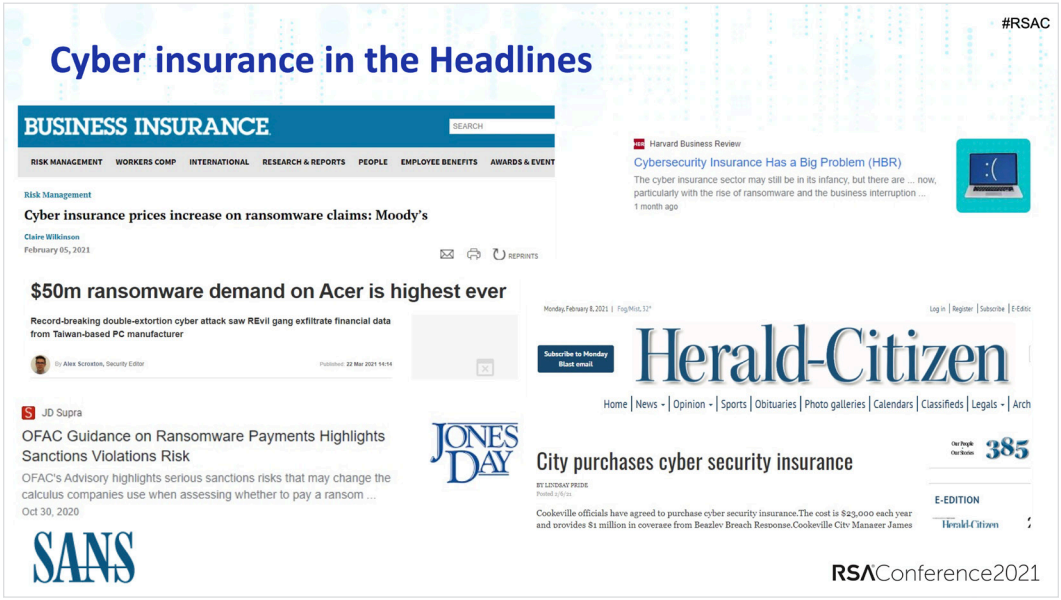


*Figure 1. Ransomware Attacks in the Media*

Kidnappers have been making ransom demands for hundreds of years, and standard law enforcement advice has always been, "Do *not* agree to pay a ransom, by wire or in person."[1] When ransomware began to be a common online attack, most cybersecurity agencies continued giving the same advice.

Since 2019, the FBI and the Department of Treasury Office of Foreign Assets Control (OFAC) has evolved federal guidelines and regulations around ransomware payoff, acknowledging that organizations are considered victims—even if they pay a ransom.[2]

Although there are many downsides to paying off a ransomware demand, the realities of the situation and the business impact require security managers to be able to make business-relevant risk recommendations to CEOs and boards if a ransomware event occurs. Most of the planning and effort to battle ransomware must take place well before an attack!

Investing in a mature, effective, and efficient cybersecurity program will always be the best way to minimize the risk of any attack succeeding. Cyber insurance policies are widely available and can reduce (but not eliminate or fully transfer) the financial impact of an incident. The extortion aspect of ransomware requires new looks at if and how cybersecurity insurance can play a role in reducing the financial impact of an incident.

This whitepaper provides the key facts and a decision model for CISOs to make informed recommendations on how to best reduce the impact of ransomware attacks, including how cyber insurance plays a role.

---

[1] Federal Bureau of Investigation, "Virtual Kidnapping: A New Twist on a Frightening Scam," October 16, 2017, www.fbi.gov/news/stories/virtual-kidnapping

[2] Dennis Fisher, "FBI Guidance Evolves on Ransomware Payments," November 18, 2020, https://duo.com/decipher/fbi-guidance-evolves-on-ransomware-payments

# Ransomware: Basics and Differences from "Normal" Malware

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency Ransomware Guide defines ransomware as "...a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."[3]

Early ransomware attacks (see Figure 2) fit this definition very well, because the impact of a ransomware incident was limited to denial or interruption of service. These simple attacks could be mitigated by mature disaster recovery or continuity of operations processes that included maintaining comprehensive backup files that were stored separately from active data.

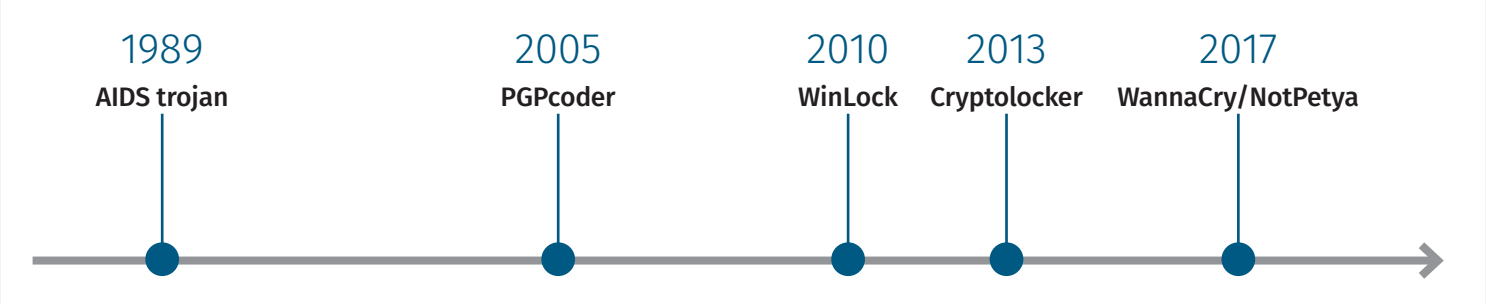


*Figure 2. Brief History of Ransomware*[4]

However, for an attacker to encrypt critical business information or executables, they first have to gain unauthorized access and control, *which means a breach has occurred*, and regulations and laws requiring various forms of public breach notification become relevant. In more recent ransomware events, attackers have threatened to expose the information they encrypted and have frequently done so. Also, ransomware attacks, like data exfiltration attacks, are often carried out without malware—phishing attacks are used to obtain user and/or admin credentials, and system internal capabilities are used to encrypt and/or export sensitive files.

For the purposes of this paper, we will use this definition: "A ransomware attack involves a threat actor obtaining access to and control of sensitive business files or executables, and then demanding a payoff to prevent business damage through denial of service or exposure of the captured information."

[3] Multi-State Information Sharing & Analysis Center, "Ransomware Guide," September 2020, www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

[4] Andrada Fiscutean, "A History of Ransomware: The Motives and Methods Behind These Evolving Attacks," July 27, 2020, www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html

## Mitigating Malware

The basic principles for preventing damage from malware apply to ransomware, as well. The CIS Critical Security Controls[5] and the NIST Cybersecurity Framework[6] are two commonly used frameworks.

The CIS Basic Controls are a necessary, minimal level of essential security controls. The CIS Controls also recommend incremental Implementation Groups (IGs) to add higher levels of controls after those essential controls are deployed.[7] See Figure 3.

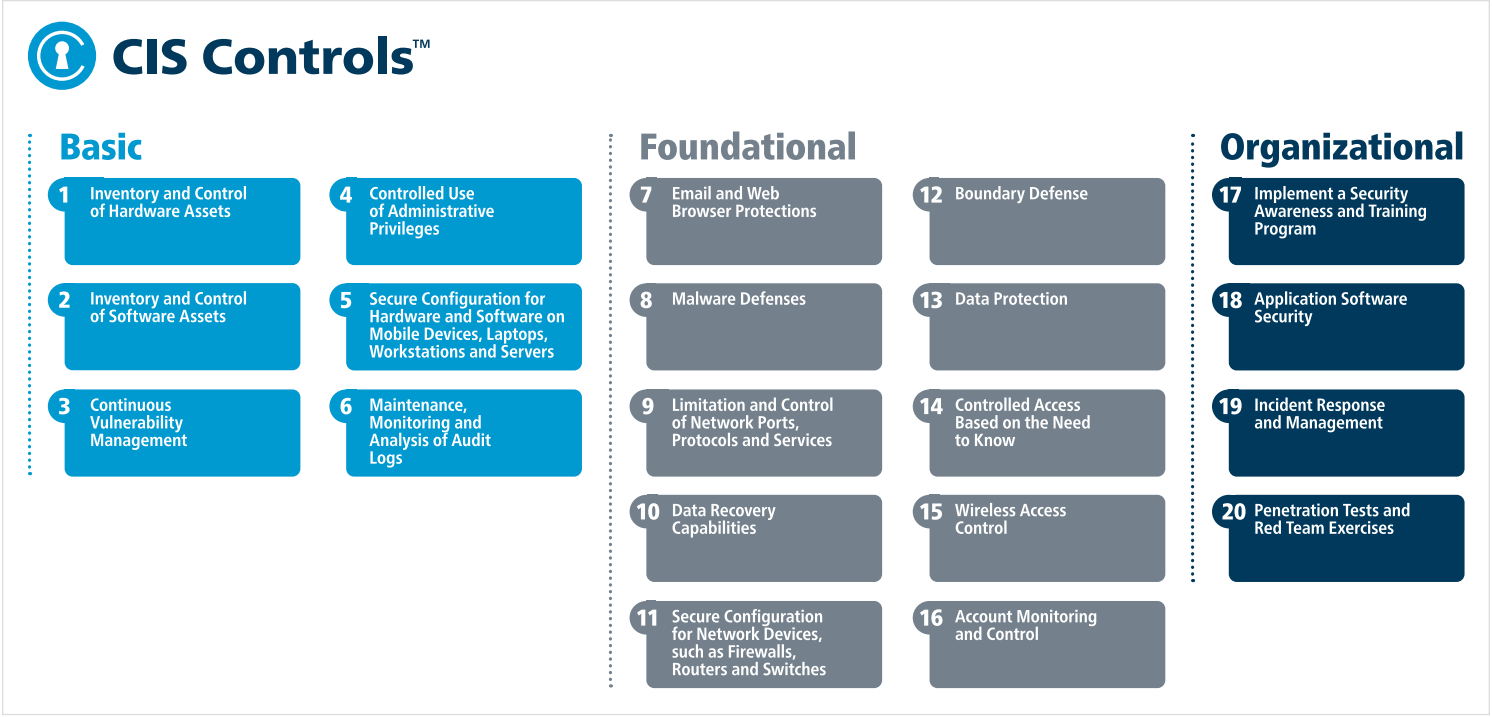


*Figure 3. The CIS Basic Controls*

The NIST Cybersecurity Framework (CSF) is a comprehensive collection of standards, guidelines, and practices for securing information systems and services.[8] The NIST CSF has allocated these across three phases of security processes, and there are five areas relevant to ransomware (see Figure 4), including:

- **Identify—**Know what critical files and executables ransomware actors may target and where they are stored. Critical Security Controls IG 1 (asset inventory, patch management, configuration standards/control, privilege management, and log management) with documented management and operational processes are key to accurate and up-to-date identification of sensitive files and executables.
- **Protect—**Stopping a ransomware attack early is not much different from stopping any other attack. Endpoint detection, response, and protection controls are required to mitigate malware used in ransomware attacks. User awareness education, strong authentication, and regular testing are needed to protect against phishing-based ransomware attacks.

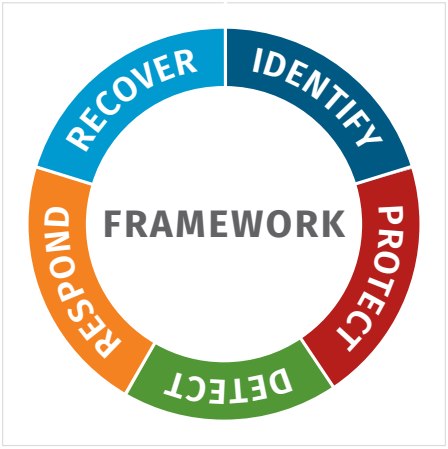


*Figure 4. The NIST Cybersecurity Framework*

[5] Center for Internet Security, "The 20 CIS Controls & Resources," www.cisecurity.org/controls/cis-controls-list

[6] NIST, "New to Framework," www.nist.gov/cyberframework/new-framework

[7] Center for Internet Security, "CIS Controls V7.1 Implementation Groups," www.cisecurity.org/white-papers/cis-controls-v-7-1-implementation-groups

[8] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018, https://doi.org/10.6028/NIST.CSWP.04162018

- **Detect—**The tactics, techniques, and processes (TTPs) used by ransomware actors do have some unique characteristics compared with common malware incidents. More file system activity and less data movement is often seen when network traffic monitoring is used to provide visibility.
- **Respond—**The extortion demand aspect of ransomware requires different or augmented response processes. This is the focus of the following section.
- **Recover—**If critical data or executables are encrypted, standard (but often overlooked) backup and recovery processes can be used. However, some ransomware attacks attempt to encrypt multiple times and wait long enough for incremental backups to also be encrypted and unusable.

## Dealing with a Ransom/Extortion Demand

In a ransomware event involving an insurer, many members of the insurer's team may show up quickly to participate. This can include staff of the insurer, a negotiator, incident responders specified by the insurer (rather than the insured's usual IR team), an OFAC compliance expert, the insurance broker who sold the policy, and others. One of the responsibilities of the security team is to assess all participants. Do they have the experience and technical competence necessary to do the job, and are they devoting their undivided attention to it? Are they helping the process or hindering it? Should executives rely on them or turn elsewhere as decisions are made?

Cyber insurance, especially as it pertains to ransomware, is not a fungible commodity that is standardized and interchangeable across companies or even different incidents. It is a service that can be more effective or less effective depending on circumstances. Beyond the financial aspects, another benefit of insurance is that the insurer may bring expertise in dealing with ransomware and retaining qualified experts. The detriment is that insurance adds layers of bureaucracy that can impede or complicate the response by the victim enterprise.

Tabletop exercises with the insurer can help the security team to assess the participants and think through issues and scenarios in advance.

### Accurate Information Is Imperative

In relation to ransomware, the involvement of insurance places additional demands on the security team to gather information, assess it, and deliver it to the right people. The security team must ensure its information is accurate and delivered reliably.

Failure to tell the full truth to the insurer could lead to denial of coverage under the insurance policy.[9] It might also lead to sanctions for violating OFAC rules.

[9] Cameron Argetsinger, "Cyber Insurance: 10 Tips and Traps," *Risk Management*, February 3, 2020, www.rmmagazine.com/2020/02/03/cyber-insurance-10-tips-and-traps

As insurers have expanded coverage to explicitly cover ransomware, they have sent new questionnaires to insureds asking more detailed questions about cyber hygiene, such as multifactor authentication (MFA).[10] Again, in answering the questionnaires, the security team must be careful to tell the full and candid truth. In the Cottage Health System case, the insurer denied coverage of a data breach by claiming the insured did not tell the truth in responding to an earlier questionnaire about cyber hygiene.[11]

The need to tell the truth requires security teams to choose their words carefully and accurately. If you do not always use MFA, then do not imply that you always do. Maybe you should say you "strive" to use MFA, in combination with other controls, or something like that.[12]

## Insurer May Have Its Own Priorities

The insurer may have priorities that do not align with those of the insured. For example, the insurer may prefer paying ransom whereas the insured prefers a different resolution to an attack.

The insurance policy may provide for payment of ransom as well as the cost of business interruption. The insurer may believe it can negotiate a ransom payment that is lower than the cost of business interruption as systems are recovered from backup. So the insurer may pressure the insured to approve payment of the ransom rather than going through the more arduous process of recovering from backup.[13]

The insurer might apply pressure by insisting, for example, the insurance policy required the insured to maintain good cyber hygiene and that requirement was not met.[14] The insurer may say that if you don't accept its offer to cover the ransom payment, then it will take the position you violated the policy and won't have to pay much under the business interruption coverage. The Cottage Health System case is an example of an insurer refusing to cover a cyber event because the insured failed to implement required cyber hygiene procedures.

Commercial insurance policies contain many exclusions of coverage. For example, insurers for two companies claimed the NotPetya ransomware was excluded under act-of-war clauses in policies, because NotPetya was linked to the Russian military.[15] Such exclusions give an insurer leverage as it steers the insured toward a decision preferred by the insurer.

Still, most insurers emphasize that the decision of whether to pay ransom rests entirely with the insured.

---

[10] Bethan Moorcraft, "Ransomware the 'Most Prominent Issue' for Cyber Insurers," Insurance Business America, January 11, 2021, www.insurancebusinessmag.com/us/news/cyber/ransomware-the-most-prominent-issue-for-cyber-insurers-243188.aspx

[11] Council of Insurance Agents & Brokers, "Columbia Casualty v. Cottage Health System Shows Importance of Reading Your Cyber Policy," www.ciab.com/resources/columbia-casualty-v-cottage-health-system-shows-importance-of-reading-your-cyber-policy

[12] Benjamin Wright, "Complying with Data Protection Law in a Changing World," SANS Institute, June 27, 2017, www.sans.org/reading-room/whitepapers/legal/paper/37835

[13] Renee Dudley, "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," *ProPublica*, August 27, 2019, www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

[14] Anecdotal statement from a knowledgeable witness who wishes to remain anonymous.

[15] Renee Dudley, "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," *ProPublica*, August 27, 2019.

From the insured's perspective, payment of the ransom may not be the best outcome. The attackers may not give a valid decryption key.[16] The attackers may attack a second time after they have been paid. Even after being paid, the attackers may still leak exfiltrated data to the public.[17] Moreover, the insured may not want to pay ransom for moral or political reasons.

### There Is No Cookbook Recipe for Public Communications

Public communications in a cyber crisis are always unique to the situation.

In the Southwire ransomware case, the victim refused to pay the ransom, even though the attackers had exfiltrated data and were releasing it on the web.[18] The victim sued a hosting company in an Irish court, and the court ordered removal of a website that was releasing the stolen data.[19] The victory in Ireland was more symbolic than substantive, because the attackers could release the data from some other place. Yet the victim went on a public relations campaign to persuade its corporate customers and other stakeholders that it was doing the right thing by refusing to pay the ransom. It emphasized to the stakeholders that it was ready to do whatever was necessary to fight the attackers, including bringing a lawsuit in distant Ireland.[20]

In a case like Southwire, the security team guides the effort to gather and analyze evidence of what is happening so executives and advisors can devise strategies for public response.

## Cyber Insurance Basics

Boards of directors are motivated to purchase cyber insurance.[21] Boards have a fiduciary duty to protect the financial interests of an enterprise and, to help fulfill that duty, boards have long turned to insurance. Cyber insurance does cover some financial risk. Plus, to help avoid that risk, the insurance underwriting process evaluates whether the enterprise is practicing appropriate cyber hygiene and using necessary security technology. (In the underwriting process, an insurer decides whether to approve an application for insurance and on what terms.)

---

[16] Andrew G. Simpson, "Putting Municipal Ransomware Attacks—and Cyber Insurance—in Context," *Insurance Journal*, September 3, 2019, www.insurancejournal.com/news/national/2019/09/03/538635.htm;
Renee Dudley, "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," *ProPublica*, August 27, 2019, www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

[17] Coveware, "Ransomware Demands Continue to Rise as Data Exfiltration Becomes Common, and Maze Subdues," November 4, 2020, www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[18] Tomas Meskauskas, "Stuck Between a Data Breach and a Ransom," Security Boulevard, June 17, 2020, https://securityboulevard.com/2020/06/stuck-between-a-data-breach-and-a-ransom

[19] Lawrence Abrams, "Maze Ransomware Publishes 14GB of Stolen Southwire Files," Bleeping Computer, January 10, 2021, https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files

[20] RVPro, "Southwire Warns Businesses of Ransomware," *RV PRO*, January 17, 2021, https://rv-pro.com/news/southwire-warns-businesses-ransomware

[21] William R. Denny, "Mitigating Your Business Risk: Board Responsibilities in Cybersecurity," *Business Law Today*, February 11, 2020, https://businesslawtoday.org/2020/02/mitigating-business-risk-board-responsibilities-cybersecurity

Whether an enterprise has cyber insurance is also of interest to lenders, investors, and corporate customers (including a prime contractor when the enterprise is a subcontractor). The attitude of these parties is that they are unable to evaluate cybersecurity themselves. It is hard for them to evaluate an audit report on cybersecurity. But they more readily understand insurance. With insurance, an independent institution puts its money on the table to show that it has undertaken an underwriting process to evaluate cyber risk, and it has determined the risk is acceptable.

Some regulated entities such as banks are required by law to purchase cyber insurance.

Accordingly, enterprises are motivated to purchase cyber insurance, even though the security team may believe money could better be spent directly improving security. The security team may further be wary of insurance, because it calls for assessments of security that the team may view as distractions from more important work.

Regardless of the motivation to purchase insurance, the leadership for procurement of the insurance typically comes from the chief financial officer or chief legal officer. In the procurement process, these officers then turn to the security team for support.

## What Does Cyber Insurance Cover?

Cyber insurance can cover many different risks, and insureds are often not well informed regarding what their insurance covers. Cyber insurance policies are not standardized. Each policy uses different language, and this language is often open to interpretation. Larger insureds have the leverage to negotiate bespoke language in policies.

Cyber insurance can cover the costs of business interruption, regulatory fines, and incident response. Increasingly, cyber insurers are explicitly covering ransomware, including the costs of negotiation and payment.

A security team should review insurance policies carefully with insurers and the brokers who sold the insurance before an incident occurs. Further, tabletop exercises with executives and the board of directors can help management understand what the insurance covers in practice, what it does not cover, and what the costs and benefits are.

## Coverage of Ransomware Under Property/Casualty Policies

Traditional property/casualty insurance policies can cover extortion or damage to property while not explicitly covering cyber risks. Sometimes, however, insurers interpret these policies to cover cyberattacks, including ransomware.[22] Coverage of cyber/ransomware when it is not explicitly stated in the policy is what insurers call “silent risk.”

Silent risk for ransomware rose to prominence in the NotPetya attacks. Losses from those attacks cost insurers $2.7 billion under traditional (silent) property/casualty policies worldwide.[23]

---

[22] New York Department of Financial Services, “Insurance Circular Letter No. 2 (2021), regarding Cyber Insurance Risk Framework,” February 4, 2021, www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02#_ednref9

[23] Jon Bateman, “War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions,” Carnegie Endowment for International Peace, October 5, 2020, https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819

So-called "silent" coverage of ransomware under a property/casualty policy is not likely to impact a security team much during its response to an incident. Silent coverage typically would not come with much in the way of services related to ransomware. After the incident is resolved, however, the security team would need to help document what happened in the incident and what the impact and losses were.

Since the NotPetya attacks, insurers have been progressively reducing their silent risk. They are explicitly excluding cyber/ransomware from renewed traditional policies and requiring insureds to purchase cyber/ransomware as a special rider or a special policy.[24]

## Practical Implications of Insurance for Ransomware

Cyber insurance that explicitly covers ransomware often includes services specific to ransomware, including payment, negotiation, and incident response. For a security team, the involvement of a cyber insurer makes management of a ransomware attack different from management of other cyber crises. The insurer becomes a player in the process of reaching the *technical* resolution, becoming more directly engaged than is common in many other cyber crises. The reason the insurer is more directly engaged is that it is at the center of a pivot point: Pay ransom or refuse to pay ransom.

The insurer may bring several of its own team members into the process. The insurer itself may have experience and desire to negotiate the ransom. Alternatively, the insurer may hire an outside negotiator. The insurer may want to have its own forensics experts directly involved to inform the insurer of what is happening.[25] The insurer may hire a payments facilitator.

The cumulative involvement of so many of the insurer's team members can detract from the value of insurance to resolve a ransomware event.

In a ransomware event, many parties could be seeking information and giving advice in a compressed time frame. In addition to the insurer and its team members, these parties could include lawyers, investigators working directly under the lawyers, and law enforcement. It falls to the security team to coordinate these people and manage their input and their access to resources and information. The security team needs tact and patience, the soft skills of diplomacy.

As the security team works through a ransomware event, it must advance numerous alternative approaches simultaneously. The insurer, for example, may be ready to pay ransom, and the security team must be ready to react to that payment and the release of a decryption key. But then the insurer may discover that OFAC requirements prevent the payment. The security team must then recover from backup or find some other method for defeating the encryption. A partial alternative to cyber insurance for ransomware is for an enterprise to retain a ransomware negotiator and payment facilitator, directly, in advance.

---

[24] PartnerRe, "Cyber Insurance—The Market's View," September 17, 2020, page 9. https://partnerre.com/wp-content/uploads/2020/09/Cyber-Insurance-The-Markets-View-2020.pdf

[25] Andrew G. Simpson, "Putting Municipal Ransomware Attacks—and Cyber Insurance—in Context," *Insurance Journal*, September 3, 2019, www.insurancejournal.com/news/national/2019/09/03/538635.htm

# Understanding the Cost and Payback of Cyber Insurance

Corporations have a lot of experience with various types of insurance. Corporate spending varies by industry and company size, but it averages less than 0.2% of revenue.[26] However, adoption of cyber insurance is still low, and the offerings and terms are still evolving.[27] For those reasons, the costs and benefits of cyber insurance policies are not well understood.

The previous section detailed some of the time and staffing impacts the cybersecurity team should expect when a cyber insurance policy is in effect. This section will focus on the hard costs of cyber insurance and the typical payoffs.

Often in restaurants, the menu for a certain dish will not show a price, but will say "market price." This generally translates to "highly variable and expensive"—if the boats didn't bring in a lot of lobsters recently, your lobster thermidor is going to cost a lot. Cyber insurance is generally market price—highly variable and often expensive compared with other forms of insurance.

The two major costs of cyber insurance are similar to those for many other forms of insurance:

- **Annual premium—**Premiums are based on the amount of coverage, but often also on the size of the company being insured.
- **Deductible—**Cyber insurance policies will pay nothing for any incident below the deductible value, and any payoff for larger incidents is reduced by the deductible value.

There may be other costs if the insurance carrier requires the company to demonstrate compliance with cybersecurity regulations or terms, or show results of security audits or penetration tests.

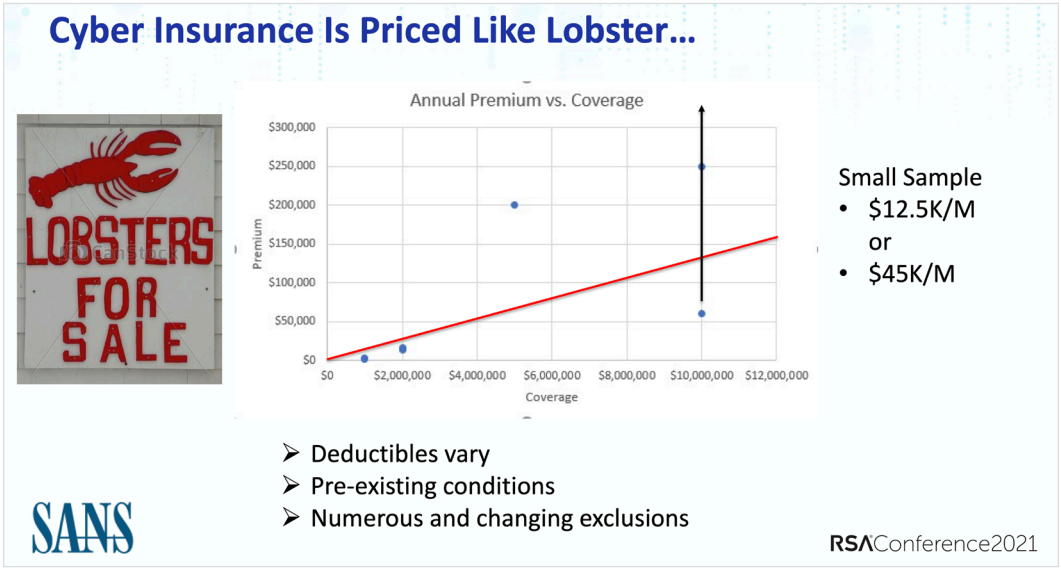


*Figure 5. Cyber Insurance Pricing*

The payoff from a cyber insurance policy is highly dependent on the contract language of the individual policy and is beyond the scope of this paper. However, payoffs are generally limited to invoiceable costs of restoration of services and documented business losses.

During 2020 and early 2021, there were a few publicly released pricing examples for cyber insurance policies. The data points in Figure 5 show that policy premium costs average out to somewhere between $12,000 and $20,000 per $1 million in coverage, but the pricing is lower for small companies and higher for large companies.

---

[26] Swiss Re Institute, "World Insurance in 2017: Solid, but Mature Life Markets Weigh on Growth, 2018, www.swissre.com/dam/jcr:a160725c-d746-4140-961b-ea0d206e9574/sigma3_2018_en.pdf

[27] Aon, "Why the Take-up of Cyber Insurance Is on the Rise," October 2019, www.aon.com/unitedkingdom/insights/why-the-take-up-of-cyber-insurance-is-on-the-rise.jsp

The cost to avoid an incident is similarly highly dependent on the maturity of the cybersecurity program and the company's diligence in maintaining essential security controls. Comparing costs to avoid estimates with cyber insurance costs and payoffs can provide valuable guidance to management. Some recent public examples of premiums and policy value give some idea of the cost and return and estimates of the cost to avoid the incident.

Let's drill down into two real-world examples.

## Midsize Company, Small Policy

A company with fewer than 500 employees and between $100 million and $200 million in annual revenue obtained a cyber insurance policy with $2 million coverage and a $25,000 deductible. The annual premium paid was $14,000.

The company was very proactive in security, but had an employee fall for a phishing attack that resulted in corporate email being forwarded to the attacker. One email had an attached spreadsheet that contained personally identifiable information about 28,000 customers, but no financial information was exposed.

Typically, the cost of breaches is in the range of $150 per record exposed, and lower for breaches where financial data is not involved.[28] Our estimate of the costs of a breach of this nature is approximately $3 million, but the company impacted estimated its invoiceable costs were $1.4 million with no business disruption costs. Most of those costs were for remedying deficiencies and improving processes and may not have been covered by the policy. The company decided not to make a claim on the policy, because payoff was uncertain and premium costs may have gone up.

There are several ways the company could have avoided this breach, but we include two simple examples here:

- Pay for a detailed penetration test, which would have discovered the vulnerability in email as a service configuration setting that enabled the attacker to covertly turn on email forwarding. Estimated one-time cost, including internal labor: $125,000.
- Require cellphone-based two-factor authentication for all email system logins. (This was done after the event.) Estimated one-time cost including increased support costs in the first year: $150,000.

In this case, at first glance, the cost to avoid equates to close to 10 years of premium payments and seems expensive. However, such measures would have avoided the $1.4-million direct financial hit, and *most importantly, if the policy ever paid off, the costs to avoid would be incurred anyway*.

[28] Chris Brook, "What Is the Cost of a Data Breach in 2019?," Digital Guardian, December 1, 2020, https://digitalguardian.com/blog/whats-cost-data-breach-2019

## County Government

In May 2019, Maryland's Baltimore County suffered a ransomware attack that shut down the county's network of 10,000 computers used by 22,000 employees and demanded a ransom payment of 13 bitcoins. At the time, that represented a demand of about $80,000—at today's bitcoin valuation, it would be $640,000!

The county had no cyber insurance at the time, but refused to pay and incurred $10 million in recovery costs and $8 million in revenue interruption or delay. In order to avoid this impact, the county would have had to upgrade its patch and configuration management practices, maintain reliable backup systems, and invested in user awareness education and strong authentication to prevent phishing attacks. SANS estimates this would have cost $3 million to $5 million, and many of those costs were incurred by the county after this incident occurred.

After the incident, the county obtained two $10-million cyber insurance policies with a total deductible of $1 million at an annual cost of $800,000. If these policies had been in place at the time of the ransomware attack, the county's financial exposure would potentially have been reduced to $1.8 million, the cost of the premium and the deductibles. However, as discussed earlier, in order for the insurer to pay off the full $18 million, the county would have had to meet all requirements, been completely accurate in all information provided to the insurer, and not been in violation of any clauses of the policy. Equally important, the county would still have to incur the $3 million to $5 million of mitigation costs to establish essential asset management, change control, endpoint protection, and network traffic and log event monitoring processes.

In 2020, the county's mitigation spending resulted in no successful attacks and no claims on the policy, but when it recompeted the policies in 2021, the lowest prices totaled $950,000 for the same level of coverage and deductible.

These two examples show the benefits and weaknesses of typical cyber insurance policies. Cyber insurance can reduce, but not cap or fully transfer, the cost of an event, but it does not reduce the level of prevention, detection, and response the security program needs to maintain in order to meet the needs of the business and customers. Almost invariably, the cost to avoid a ransomware event will need to be incurred after the event, whether or not cyber insurance policies are in effect.

## Summary

Most companies have many years of experience in obtaining various forms of insurance. However, cyber insurance is a new and still-evolving offering, and CXOs and boards may have misconceptions of how much financial mitigation of incident impact such policies will provide compared with investing the same amount in security improvements to increase the odds that an incident will *not occur*. The extortion element of ransomware has increased board risk and liability committee interest in cyber insurance.

CISOs should make sure they are involved in cyber insurance decisions and are aware of the requirements and terms of all insurance policies in effect that are relevant to ransomware in particular and cyberattacks in general. Some key points to convey include:

- Remedying gaps in essential security controls, such as asset inventory, configuration management, endpoint protection, and network traffic and log event monitoring, should be done *before* considering cyber insurance because it will avoid most incidents and will be required after a damaging incident occurs.
- MFA is the only highly effective way of preventing phishing-based ransomware attacks. Simple text message, two-factor approaches reduce successful phishing attacks by more than 99% and are now widely used by CXOs and board members for their personal financial accounts.
- The costs of cyber insurance include premiums and deductibles, but also may increase the workload of the security team when policies are obtained and renewed, as well as during ransomware incident response. Further, an insurer may require the insured to purchase and deploy technology the insurer deems necessary, such as a SIEM system or additional endpoint detection and response capabilities.

A tabletop exercise with management is an excellent way to get these points across and to obtain buy-in for strategies that will reduce cybersecurity risk overall, as well as impact decisions on cyber insurance.

A security team is wise to understand its cyber insurance policy before a ransomware event happens. A step in this direction is a tabletop exercise involving the insurer's representatives. The security team should be prepared to work with them, ensuring they have access to accurate information. Further, the security team should assess the insurer's team so executives are better prepared to make decisions. As a ransomware event unfolds, the security team needs to advance multiple possible resolutions simultaneously.

# Resources

SANS Webcast: How to Negotiate a Cyber Insurance Policy,
www.sans.org/webcasts/negotiate-cyber-insurance-policy-101192

DHS/CISA Cyberinsurance Resources,
www.cisa.gov/cybersecurity-insurance

Federation of European Risk Management Associations,
www.ferma.eu/app/uploads/2019/02/preparing-for-cyber-insurance-web-04-10-2018.pdf

"The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks,"
www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

"US Treasury Warns of Sanctions Violations for Paying Ransomware Attackers,"
www.darkreading.com/risk/us-treasury-warns-of-sanctions-violations-for-paying-ransomware-attackers/d/d-id/1339066

SANS Webcast: Cyber Insurance: What Is Its Role in Your Security Program?,
www.sans.org/webcasts/cyber-insurance-role-security-program-101012

## About the Authors

**John Pescatore** joined SANS as director of emerging security trends in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008, and is an NSA-certified cryptologic engineer.

**Benjamin Wright** is a practicing attorney based in Dallas, Texas, focused on technology law. He serves as a senior instructor at the SANS Institute, teaching its five-day course, LEG523 Law of Data Security and Investigations. By means of that course, Ben has taught thousands of students from throughout the world. Ben advises diverse clients, both in the United States and outside of it, on privacy, electronic commerce, and data security law. He is the author of many compliance modules in the SANS Security Awareness program. http://benjaminwright.us

## Sponsor

**SANS would like to thank this paper's sponsor:**

Gigamon®