CHASE

J.P.Morgan

CYBERSECURITY & TECHNOLOGY CONTROLS

Cyber Insurance: What You Need to Consider Before Purchasing a Policy

INTRODUCTION

Many businesses, government entities and nonprofits depend upon information technology for their operations. This includes the internet, desktops, servers, e-commerce, cloud computing and more. Any disruption to the IT infrastructure or data breach caused by a cyberattack could cause significant harm to the organization's business and payment operations as well as its reputation.

Organizations have a responsibility to their clients, investors and employees to protect sensitive data, including personally identifiable information, protected health information and proprietary information. Failure to provide adequate data protection can result in a loss of competitive advantage, a drop in stock value, regulatory fines, civil litigation, and, in some cases, criminal prosecution.

In addition to having an incident response plan, conducting security audits and practicing proper cybersecurity hygiene, many organizations also purchase a cyber insurance policy. These policies are separate and distinct from general liability policies, which may exclude cyber events. But what is cyber insurance, and what do you need to consider before purchasing a policy?

The information provided here is intended to help inform clients about cyber insurance. It does not provide a comprehensive list of all types of cyber insurance considerations or identify all types of best practices. The client company or organization is responsible for determining how to best select cyber insurance products and for identifying the best practices that are most appropriate to its needs.

What is Cyber Insurance?

Cyber insurance, also known as cyber risk insurance or cyber liability insurance coverage, is designed to help an organization mitigate exposure through risk transfer by offsetting any costs associated with data recovery after a cyber-related incident.

A cyber insurance policy provides insurance coverage to the insured in the event of a cyberattack that results in the loss of data and/or the breach of confidential information. Depending on the terms and conditions of the cyber insurance policy, the insured could recover the cost of:

- Restoring personal identities of impacted customers
- Business interruption that results in the loss of income
- Communicating to clients, customers, employees and other stakeholders
- Civil fines and penalties
- Security and privacy liability
- Cyber extortion
- Network interruption

Insurance companies collect premiums from clients to pay for claims when an event occurs. To provide their customers with lower premiums and ensure sufficient funds to pay out a claim, cyber insurance companies group large numbers of customers together to minimize the cost impact of the highest-risk organizations; larger risk pools result in more predictable and stable premiums.

Why Purchase Cyber Insurance?

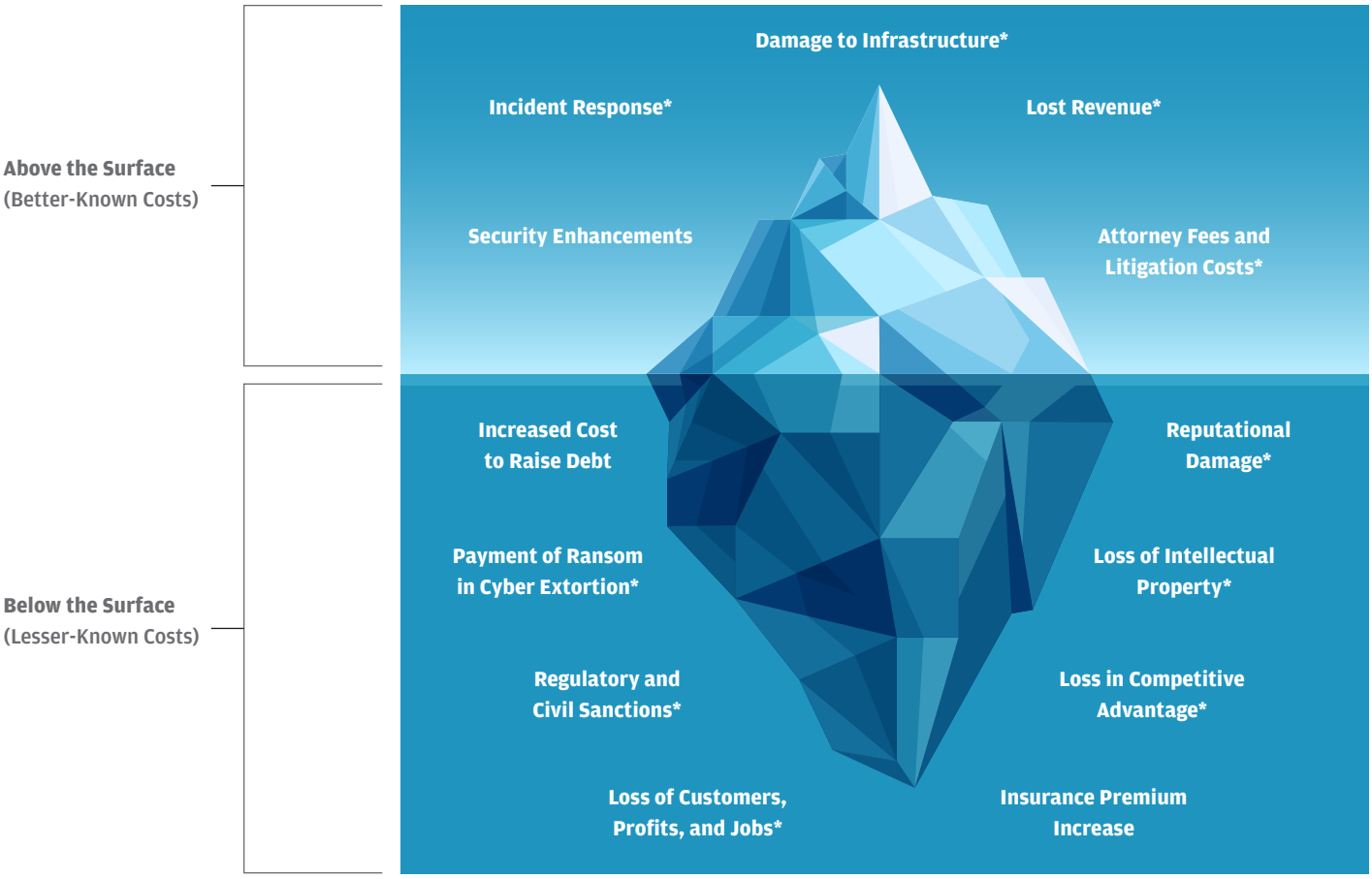
Cyber insurance, like traditional insurance, is designed to provide access to financial resources in the event of a disaster. Most organizations do not have the operating capital available to cover the types of losses caused by a cyberattack, such as those impacting a data center server or intellectual property.

Cybercrimes have escalated in recent years, particularly ransomware attacks against companies, governments and healthcare organizations. In 2019, the FBI's Internet Crime Complaint Center received 2,047 complaints of ransomware, with adjusted losses totaling over $8.9 million, according to its annual report. Since the COVID-19 pandemic began, cybercriminals have exploited the uncertainty and chaos in the business landscape to increase cyberattacks against all organizations.

As the rise in cybercrime is expected to continue, many organizations may choose to purchase a cyber insurance policy to transfer the risk from themselves to the insurance provider, who agrees to indemnify the policyholder up to a certain amount for losses incurred in exchange for an insurance claim recovery. Although an organization's cybersecurity controls help protect and defend against attacks, there are times when controls can fail or an organization may want additional protection. Organizations may consider cyber insurance to bridge the gap, particularly when it comes to the high costs associated with recovering from an incident (see Figure 1).

When evaluating whether to purchase cyber insurance, organizations should ensure they will receive value from a policy. The cost of insurance premiums and deductibles should fall below the annualized loss expectancy (ALE) for the company. ALE is determined by calculating the annual rate of occurrence (the likelihood of an incident occurring each year) and the single loss expectancy (the cost of a single incident).

Figure 1. The Costs of a Cyber Attack



*Covered by Insurance

How Does Cyber Insurance Help Manage Risk?

Insurance is a method of risk transfer that places specific risks on another person or entity for some or all of the associated financial loss. An insurance policy transfers risk through a contractual obligation from an insured to an insurance provider, subject to the terms and conditions of the insurance policy.

Any organization that is considering purchasing cyber insurance should consult with its technology and risk departments as well as other advisors, such as an insurance broker that specializes in cyber insurance coverage. Together they should assess the risk of cyber attacks and evaluate the value an insurance policy may provide. This evaluation would include the insurance policy's deductible, premium, limit of coverage and coverage terms.

What Cyber Trends May Impact My Decision to Purchase Cyber Insurance?

As the rate of cybercrimes increases, the rate of **cyber insurance claims has also grown by 39% over the past two years**. During 2Q 2020, cybercriminals requested an average of **$178,254 in ransom payments per incident, up 60% from the first quarter of 2020** with some requests exceeding $1 million. There are also the costs of lost revenue and infrastructure rebuilding, **with recovery taking over 16 days on average during Q2 2020**. The loss of business operations for days, weeks or months, the cost to hire incident response, and the cost of replacing infrastructure can also total several thousands of dollars, or more, depending on the size of the organization and complexity of the attack.

Approximately 40% of US based companies have a cyber insurance policy in place, according to Aon Cyber Solutions Senior Vice President James C. Trainor, and the number of new companies purchasing insurance is rising slowly. There are no mandates requiring cyber insurance; however, it is important to consult with your legal counsel for any regulatory or contractual obligations.

How Do I Determine the Expected Value of Cyber Insurance?

Each organization will have its own unique needs, which can include, but are not limited to, deductibles, coverage levels, and insurable events. Each of these variables can affect the final cost of insurance. It is important to keep in mind that the final cost of insurance is not merely the cost of the policy's premiums. It is imperative that organizations examine the expected value of the policy by considering the likelihood of an event occurring and the expected loss of such an event, and balance those costs with the cost of paying insurance premiums and deductibles. For example, if there is a 2% chance of an organization losing $1 million and the insurance premium costs $10,000 annually, here is how the organization can calculate the expected value of insurance to decide whether to transfer or retain the risk:

EXPECTED VALUE MATRIX

	No Loss	Loss	Expected Value
WITHOUT INSURANCE	$0 x 0.98 = $0	**($1,000,000)** x 0.02 = ($20,000)	$0 + **($20,000)** = **($20,000)**
WITH INSURANCE	**($10,000)** x 0.98 = **($9,800)**	**($10,000)** x 0.02 = **($200)**	**($9,800)** + **($200)** = **($10,000)**

EXPECTED VALUE MATRIX

	Cost	Expected Value
WITHOUT INSURANCE	**$1,000,000 loss** x 2% probability of incident	**-$20,000**
WITH INSURANCE	**$10,000 insurance premium**	**-$10,000**

In this hypothetical example, the cost of purchasing insurance with an annual premium of $10,000 shows a higher expected value than accepting the risk, as the ALE is $20,000. It may be more financially beneficial for an organization to purchase insurance than accept the risk.

Are There Other Considerations to Look for in a Cyber Insurance Policy?

When purchasing cyber insurance, keep in mind three guidelines:

1. Determine if the maximum loss is affordable for your organization

2. Consider the likelihood of losses

3. Ensure that the transfer risk is worth the premium you would be paying

A deductible must be paid for each loss incurred and a lower deductible can increase your annual premium. The cost of the deductible should be included in your expected value calculations when totaling the cost of an incident.

It is important to review the policy coverage with your insurance carrier and insurance broker to make sure your organization has appropriate coverage based on your specific needs and risk appetite. Additionally, the organization's management should also review with legal counsel the risk of a cyber attack and its impact on any regulatory or contractual requirements.

Insurance may not cover all cyberattacks, particularly incidents that originate from a nation-state actor. The insurance industry generally considers these types of attacks to be acts of war, so policies usually do not cover them.

Finally, purchasing more insurance than you need does not mean you will be better insured if an attack happens. Estimate your insurance policy coverage by using the expected value matrix to ensure you have adequate coverage to restore business operations quickly.