JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CYBER INSURANCE AS A CORNERSTONE OF ENTERPRISE RISK MANAGEMENT

Sikha Haritwal

Next Move Strategy Consulting, Assam, India

Abstract

Cybersecurity insurance, commonly referred to as cyber insurance, serves as a critical product for businesses to mitigate risks associated with cyber crime activities such as cyberattacks and data breaches. This manuscript explores the definition, importance, functionality, coverage areas, exclusions, and broader implications of cyber insurance based on detailed examinations of its components. It discusses how cyber insurance operates similarly to traditional insurance, covering first-party and third-party losses, and emphasizes its role in financial protection, legal support, and remediation following cyber incidents. Key risks covered include customer notifications, data recovery, system damage repair, ransom demands, and attack remediation, while exclusions encompass poor security processes, prior breaches, human error, insider attacks, preexisting vulnerabilities, and technology system improvements. The manuscript highlights that cyber insurance is not a substitute for robust cyber defense strategies and outlines steps to reduce cyber risk through assessment, implementation, and insurance procurement. Benefits such as forensic support, coverage for data breaches and cyber extortion, affordability, and protection against various cyber threats are detailed. Requirements for obtaining cyber insurance, including multi-factor authentication, cybersecurity training, data backups, identity access management, and data classification, are examined. The discussion extends to why cyber insurance costs are justified, factors influencing costs, average pricing, market dynamics, and major loss drivers like ransomware, business email compromise, data breaches, and supply chain vulnerabilities. This comprehensive overview underscores the necessity of integrating cyber insurance with proactive cybersecurity measures to enhance organizational resilience in a digitized economy.

Keywords

Cyber insurance, cybersecurity insurance, data breach, cyberattack, ransomware, cyber extortion, multi-factor authentication, data recovery, business interruption, cyber risk management, cyber defense, insurance exclusions, cyber insurance requirements, cyber insurance costs, cyber threat landscape, supply chain vulnerabilities, business email compromise, forensic support, cyber insurance market, governmental cyber protection.

1. Introduction

Cybersecurity insurance (cyber insurance) is a product that enables businesses to mitigate the risk of cyber crime activity like cyberattacks and data breaches. It protects organizations from the cost of internet-based threats affecting IT infrastructure, information governance, and information policy, which often are not covered by commercial liability policies and traditional insurance products.

Cyber insurance coverage works the same way as businesses would purchase insurance against physical risks and natural disasters. It covers the losses an enterprise may suffer as a result of a cyberattack.

Cyber insurance is increasingly becoming essential for all companies as the risk of cyberattacks against applications, devices, networks, and users grows. That is because the compromise, loss, or theft of data can significantly impact a business, from losing customers to the loss of reputation and revenue.

Enterprises may also be liable for the damage caused by the loss or theft of third-party data. A cyber insurance policy can protect the enterprise against cyber events, including acts of cyber terrorism, and help with the remediation of security incidents.

The cybersecurity insurance process works in a similar way to other forms of insurance. Policies are sold by many suppliers that provide other forms of business insurance, such as errors and omissions insurance, liability insurance, and property insurance. Cyber insurance policies will often include first-party coverage, which means losses that directly impact an enterprise, and third-party coverage, which means losses suffered by other enterprises due to having a business relationship with the affected organization.

A cyber insurance policy helps an organization pay for any financial losses they may incur in the event of a cyberattack or data breach. It also helps them cover any costs related to the remediation process, such as paying for the investigation, crisis communication, legal services, and refunds to customers.

2. What Risks Does Cyber Insurance Cover?

Insurance for cybersecurity typically includes first-party coverage of losses incurred through data destruction, hacking, data extortion, and data theft. Policies may also provide coverage for legal expenses and related costs. Although policies may vary by provider and plan, the main areas that cyber insurance covers include:

1. **Customer notifications**: Enterprises are usually required to notify their customers of a data breach, especially if it involves the loss or theft of. Cyber insurance often helps businesses cover the cost of this process.
2. **Recovering personal identities**: Cybersecurity insurance coverage helps organizations restore the personal identities of their affected customers.
3. **Data breaches**: incidents where personal information is stolen or accessed without proper authorization.
4. **Data recovery**: A cyber liability insurance policy usually enables businesses to pay for the recovery of any data compromised by an attack.
5. **System damage repair**: The cost of repairing computer systems damaged by a cyberattack will also be covered by a cyber insurance policy.
6. **Ransom demands**: Ransomware attacks often see attackers demand a fee from their victims to unlock or retrieve compromised data. Cyber insurance coverage can help organizations cover the costs of meeting such extortion demands, although some government agencies advise against paying ransoms as doing so only makes these attacks profitable for criminals.
7. **Attack remediation**: A cyber insurance policy will help an enterprise pay for legal fees incurred through violating various privacy policies or regulations. It will also help them hire security or computer forensic experts who will enable them to remediate the attack or recover compromised data.
8. **Liability** for losses incurred by business partners with access to business data.

Many entry-level cybersecurity insurance policies only cover first-party losses; more extensive policies cover third-party liability losses. Expenditure covered by cyber insurance typically includes costs associated with the following:

- Meeting extortion demands from a ransomware attack.
- Notifying customers when a security breach has occurred.
- Paying legal fees levied because of privacy violations.
- Hiring computer forensics experts to recover compromised data.
- Restoring identities of customers whose PII was compromised.
- Recovering data that has been altered or stolen.
- Repairing or replacing damaged or compromised computer systems.
- Providing credit monitoring services for customers affected by a data breach.

3. Cyber Risks Excluded from Cyber Insurance Coverage

A cybersecurity insurance policy will often exclude issues that were preventable or caused by human error or negligence, such as:

1. **Poor security processes**: If an attack occurred as a result of an organization having poor configuration management or ineffective security processes in place
2. **Prior breaches**: Breaches or events that occurred before an organization purchased a policy
3. **Human error**: Any cyberattack caused by human error by an organization's employees

4. **Insider attacks**: The loss or theft of data due to an insider attack, which means an employee was responsible for the incident
5. **Preexisting vulnerabilities**: If an organization suffers a data breach as a result of failing to address or correct a previously known vulnerability
6. **Technology system improvements**: Any costs related to improving technology systems, such as hardening applications and networks

The following are among the exclusions and issues cybersecurity policies don't cover:

- Preventable security issues caused by humans, such as poor configuration management or the mishandling of digital assets.
- Preexisting issues and prior breaches and cybersecurity events, such as incidents that occurred before the policy purchase.
- Cybersecurity events initiated and caused by employees or insiders.
- Infrastructure failures not caused by a purposeful cyberattack.
- Failure to correct a known vulnerability, such as when a company that knows a vulnerability exists, fails to address it and then has a compromising situation related to that vulnerability.
- The cost to improve technology systems, including security hardening in systems or applications.
- The loss of intellectual property value, such as proprietary information, trade secrets or other priceless intangible assets.

4. Does Cyber Insurance Mean Cyber Defense?

Cyber insurance should not be considered in place of effective and robust cyber risk management. All companies need to purchase cyber insurance but should only consider it to mitigate the damage caused by a potential cyberattack. Their cyber insurance policy needs to complement the security processes and technologies they implement as part of their risk management plan.

Cyber insurance suppliers analyze an organization's cybersecurity posture in the process of issuing a policy. Having a solid security posture enables an enterprise to obtain better coverage. In contrast, a poor security posture makes it more difficult for an insurer to understand their approach, resulting in ineffective insurance purchases.

Furthermore, failing to invest in appropriate or effective cybersecurity solutions can result in enterprises either failing to qualify for cyber insurance or paying more for it.

Cyberdefense and cyber insurance aren't synonymous terms. Cyberdefense is a broad term that refers to any arrangement of security tools and policies a business chooses to implement to address cyberthreats. A cyber insurance plan is one policy a business acquires to provide remediation and financial reimbursement in the wake of a cyberattack. Cyber insurance complements other security tools and procedures.

Setting up a cybersecurity infrastructure precedes buying cyber insurance. A business that lacks security tools and policies might pay more for cyber insurance because it would be deemed to be at higher risk. However, if an infrastructure is set up prior to purchasing, risks are reduced and insurance plans have less to cover. Cyber insurance is just one component of a business's full cyberdefense strategy.

5. Why Cyber Insurance Isn't a Substitute for Strong Cybersecurity Measures

In today's digital landscape, cyber threats are more sophisticated and damaging than ever before. Businesses across industries face risks such as ransomware, data breaches, phishing attacks, and supply chain vulnerabilities. To mitigate financial losses from cyber incidents, many organizations turn to cyber insurance. However, relying solely on cyber insurance without implementing strong cybersecurity measures is a critical mistake.

Cyber insurance is not a proactive security solution—it does not prevent cyberattacks, nor does it eliminate the operational, reputational, and regulatory consequences of an incident. Instead, it should be seen as a financial safety net that complements robust cybersecurity practices. In this blog, we will explore why cyber insurance is not a replacement for effective cybersecurity and why businesses must prioritize proactive security strategies.

5.1 Cyber Insurance Provides Financial Relief, Not Protection

Cyber insurance is designed to cover financial losses resulting from cyber incidents, including legal costs, data recovery expenses, and business interruption losses. However, it does not prevent cyberattacks from happening. Businesses without strong security measures remain vulnerable to breaches, and no insurance policy can restore lost data, protect customer trust, or fully recover reputational damage.

Furthermore, some cyber policies have limitations on what they cover. For example, if a ransomware attack encrypts your entire database but the policy excludes ransom payments, your business may still face catastrophic losses despite having coverage.

5.2 Stringent Policy Requirements and Exclusions

Insurance companies are becoming increasingly strict about the cybersecurity posture of organizations before issuing policies. Many insurers require businesses to implement baseline security measures such as:

- Multi-Factor Authentication (MFA) for critical systems
- Regular software patching and vulnerability management
- Endpoint detection and response (EDR) solutions
- Secure backup and disaster recovery plans
- Employee cybersecurity awareness training

Failure to meet these security requirements may result in denied claims or higher premiums. Additionally, cyber insurance policies often contain exclusions for incidents caused by inadequate security practices, insider threats, or nation-state cyberattacks.

For instance, after the NotPetya ransomware attack, many insurers refused to pay claims, arguing that the attack was an act of war. This left many businesses stranded with no financial assistance, further highlighting the importance of a strong cybersecurity foundation.

5.3 Business Disruption Costs Go Beyond Financial Compensation

The aftermath of a cyberattack is not limited to immediate financial losses. A successful attack can result in long-term business disruption, loss of competitive advantage, and diminished customer trust. Even if an insurance policy covers direct financial damages, it cannot:

- Restore lost business opportunities
- Rebuild customer relationships and brand reputation
- Compensate for intellectual property theft
- Address legal and regulatory scrutiny

Take the example of a major e-commerce company that experiences a data breach. Even with insurance, the long-term consequences—such as loss of customer confidence and legal battles—can far exceed any policy payout.

5.4 Regulatory and Compliance Obligations Remain

Many industries are subject to strict compliance and regulatory frameworks, including:

1. **General Data Protection Regulation (GDPR)** – Requires businesses to implement appropriate cybersecurity measures and report breaches within 72 hours.
2. **Health Insurance Portability and Accountability Act (HIPAA)** – Mandates secure handling of healthcare data and imposes heavy fines for security lapses.
3. **Payment Card Industry Data Security Standard (PCI DSS)** – Requires businesses processing credit card transactions to meet stringent security standards.

Cyber insurance does not exempt organizations from these legal responsibilities. If a business fails to comply with regulatory requirements and experiences a breach, it may still face significant fines and penalties, even if insured.

5.5 The Rising Cost of Cyber Insurance and Coverage Gaps

As cyber threats grow more frequent and severe, cyber insurance premiums have surged. According to industry reports, cyber insurance premiums have increased by over 50% year-over-year due to the rising costs of ransomware attacks and data breaches. Many insurers now demand detailed cybersecurity audits before issuing policies and may impose:

- Higher deductibles for businesses with weak security postures
- Reduced coverage for ransomware-related incidents
- Strict policy limitations on social engineering fraud and business email compromise (BEC) attacks

This means that businesses without robust cybersecurity frameworks may struggle to obtain comprehensive coverage, leaving them exposed to significant risks despite paying for insurance.

5.6 The Role of Proactive Cybersecurity in Risk Management

A well-rounded cybersecurity strategy should include:

5.6.1 Risk Assessment and Vulnerability Management

Regularly assess security risks, identify vulnerabilities, and apply patches to reduce attack surfaces.

5.6.2 Employee Training and Awareness

Human error remains a leading cause of cyber incidents. Educating employees on phishing, social engineering, and password hygiene is crucial in preventing breaches.

5.6.3 Zero Trust Security Model

Implementing a Zero Trust framework ensures that no user or device is trusted by default, minimizing the risk of unauthorized access.

5.6.4 Incident Response and Business Continuity Planning

A well-defined incident response plan can help mitigate damage in case of an attack. Regularly test and update response strategies to improve resilience.

5.6.5 Advanced Threat Detection and Response

Leverage AI-driven security analytics, intrusion detection systems (IDS), and Security Information and Event Management (SIEM) solutions to detect and mitigate threats proactively.

Businesses should adopt a proactive cybersecurity approach that includes robust risk management, employee training, advanced threat detection, and regulatory compliance. By integrating cyber insurance with a strong security posture, businesses can build a resilient defense against evolving cyber threats while ensuring financial protection in case of an attack.

6. How to Choose the Right Cyber Insurance Policy?

Pricing cyber risk will typically depend on an enterprise’s revenue and the industry they operate in. To qualify, they will likely need to allow an insurer to carry out a security audit or provide relevant documentation courtesy of an approved assessment tool. The information accrued from an audit will guide the type of insurance policy the provider can offer and the cost of any premiums.

Policies often vary between different providers. Therefore, it is best to review any details carefully to ensure the required protections and provisions are covered by the proposed policy. The policy also needs to provide protection against currently known and emerging cyber threat vectors and profiles.

To qualify for cyber insurance coverage, an individual or entity typically must submit to an insurer's security audit or provide documentation from an approved assessment tool, such as one offered by the National Institute of Standards and Technology's Cybersecurity Framework. The results from a security audit or the documentation from approved assessment tools can factor into the types of coverage the insurance carrier provides, as well as the cost of the premiums.

7. Three Steps To Reduce Cyber Risk

Cyber risk is a significant concern for companies of all sizes and across all industries. Organizations need to take decisive action to strengthen their cyber defenses and manage their cyber risk through the combination of cyber insurance, secure devices, domain expertise, and technology.

1. **Step 1—Assess**: The first step in reducing cyber risk is to assess cyber readiness with a respected professional services organization. This process includes carrying out a security audit before providing appropriate cyber insurance.

2. **Step 2—Implement**: The next step is to implement technology that protects the elements an organization intends to take out cyber insurance against. This can include an anti-malware solution to protect the enterprise against the threat of malicious software.

3. **Step 3—Insurance**: The first two steps enable an organization to prove they have the necessary processes and technologies in place to qualify for cyber insurance from a provider.

8. Benefits of Cyber Insurance

Cyber insurance provides the following benefits:

- **Protection against cyber-risks**. Cyber liability coverage is important to protect businesses against the risk of cyber events, including those associated with terrorism. Cyber insurance can provide network security coverage and assist in the timely remediation of cyberattacks and other incidents.

- **Financial protection**. Cyber insurance offers financial security against damage caused by cybersecurity incidents. This includes expenses for investigations, credit monitoring services and legal responsibilities, among other costs associated with data breaches. In addition, it can provide compensation for business interruption, loss of revenue and computer system restoration.

- **Legal support**. Cyber insurance frequently includes legal assistance, which helps businesses navigate the complicated legal system around cybersecurity events. It can pay for the costs of legal counsel, legal compliance with regulations and prospective lawsuits resulting from data breaches and privacy violations.

- **Peace of mind**. Cyber insurance provides businesses and individuals with a sense of security by guaranteeing their financial stability in a cyber crisis. This lets businesses concentrate on their core business operations without having to worry about the possible financial and reputational consequences of a cyberattack.

- **Commitment to security**. Cyber insurance coverage highlights an organization's dedication to safeguarding client data and being proactive with its cyberdefense. A commitment to cybersecurity can boost a business's reputation and confidence in it among customers, stakeholders and partners.

Here are the 10 benefits of cyber insurance that can help protect your business when things go wrong:

Forensic Support

Whenever a cyber attack happens, it’s very important to understand how it occurred and who did it. Forensic experts help trace the source of the attack, figure out what data was compromised, and assist with the investigation.

Imagine discovering a data breach but not knowing how the hackers got in or what information they hacked.

Coverage of Data Breach

Any unauthorised disclosure of private or sensitive data is called a data breach. This may involve the disclosure of financial information, personal data, or company information, as a result of phishing, hacking, or system weaknesses.

Activities such as notifying affected customers, offering credit monitoring services, and handling legal fees, are all covered by cybersecurity insurance.

Defence Against Cyber Extortion

When hackers demand money in return for not committing a cybercrime (such as a ransomware threat), this is known as cyber extortion. Whether it means paying the ransom or financing the recovery attempts, cybersecurity insurance handle the expenses of dealing with such incidents.

Regaining control of your company following a cyberattack is more important than the money.

Affordability

The most prevalent misunderstanding is that cyber insurance is costly. Most people believe that only big businesses need to get cyber coverage. However, in practice, the price of cyber insurance has decreased over time, particularly for small and medium-sized enterprises.

It’s frequently a little investment to pay for the security and peace of mind it offers in comparison to the monetary losses from a cyberattack.

- For example, The University of California experienced a data breach, which impacted approx. 547,000 individuals. The exposed data includes dates of birth, names, phone numbers and social security numbers of students and staff. With the help of their cyber insurance, the university was able to manage the situation more effectively, leading to less financial and reputational damage.

- Also, Travelex, one of the foreign exchange service provider, was hit by a ransomware attack, which lead to major disruption to their operations for weeks. The attackers started demanding a massive ransom to decrypt their files. With the help of their travelex smart cyber insurance they were able to cover the ransom, the recovery process, and the loss of business during that particular period. While the attack resulted in significant setbacks, their insurance helped them recover swiftly and minimize the impact.

8.1 What are the strengths of cyber insurance?

Cyber insurance offers financial protection against today’s most common cyber threats, such as ransomware, phishing, and data breaches. Its key strength lies in helping businesses recover quickly and affordably from such incidents. It supports legal defense, regulatory compliance, and access to cybersecurity resources that reduce future risk.

9. How Does Cyber Insurance Work?

Most insurance providers that offer business insurance, such as E&O, business liability and commercial property insurance, also sell cyber insurance. Policies typically include first-party coverage, which applies to losses that directly affect a company. They also can have third-party coverage, which applies to losses others suffer from a cybersecurity event or incident, based on the third-party's business relationship with that company.

As part of cybersecurity incident response efforts, cyber insurance policies can cover the financial losses that result from cybersecurity events. In addition, cyber-risk coverage often covers costs associated with remediation, including payment for legal assistance, investigators, crisis communicators, and customer credits and refunds.

10. Who Needs Cyber Insurance?

While every organization's risk profile is unique, most companies could benefit from purchasing cyber insurance as part of their overall risk management strategy. A range of industries are good candidates for cyber insurance:

- **Businesses of all sizes**. Organizations that create, store and manage electronic data online -- such as customer contacts, customer sales, PII and credit card numbers -- could benefit from cyber insurance. In addition, e-commerce businesses can benefit from cyber insurance, since downtime related to cybersecurity incidents can cause a loss in sales and customers. Similarly, any organization, including small businesses, that stores customer information on a website can benefit from the liability coverage provided by a cyber insurance policy.
- **Healthcare providers**. Healthcare companies handle a range of sensitive information and patient data and are frequently targeted with data breaches and cyberthreats. According to IBM's annual data breach report, the average annual cost of a healthcare breach is nearly $10 million. To reduce the financial and legal risks connected to data breaches and Health Insurance Portability and Accountability Act violations, cyber insurance is essential for healthcare organizations.
- **Financial institutions**. Banks and credit unions are prime targets for cybercriminals because of the sensitive data they deal with, such as social security numbers, account numbers and other PII. Cyber insurance can help these institutions recover from financial damages caused by cyberattacks.
- **Government agencies**. Government agencies handle a huge amount of private information. Cyber insurance can help government institutions guard against cyberattacks and ensure the continuity of public services.
- **Educational institutions**. Educational institutions, such as schools, colleges and universities, store large amounts of personal and academic records for both employees and students, making them good candidates for cyber insurance.
- **Companies with high revenue**. Companies with significant revenue streams are hacker targets. To guard against the financial damages from cyberattacks and data breaches, these organizations should consider cyber insurance.

11. What Is Covered and Not Covered by Cyber Insurance?

Many major U.S. insurance companies offer customers cyber insurance policy options. Depending on the price and type of policy, the customer can expect to be covered for extra expenditure resulting from the physical destruction or theft of IT assets.

11.1 What's typically covered?

Many entry-level cybersecurity insurance policies only cover first-party losses; more extensive policies cover third-party liability losses. Expenditure covered by cyber insurance typically includes costs associated with the following:

- Meeting extortion demands from a ransomware attack.
- Notifying customers when a security breach has occurred.
- Paying legal fees levied because of privacy violations.
- Hiring computer forensics experts to recover compromised data.
- Restoring identities of customers whose PII was compromised.
- Recovering data that has been altered or stolen.
- Repairing or replacing damaged or compromised computer systems.
- Providing credit monitoring services for customers affected by a data breach.

11.2 What's not typically covered?

The following are among the exclusions and issues cybersecurity policies don't cover:

- Preventable security issues caused by humans, such as poor configuration management or the mishandling of digital assets.
- Preexisting issues and prior breaches and cybersecurity events, such as incidents that occurred before the policy purchase.
- Cybersecurity events initiated and caused by employees or insiders.
- Infrastructure failures not caused by a purposeful cyberattack.
- Failure to correct a known vulnerability, such as when a company that knows a vulnerability exists, fails to address it and then has a compromising situation related to that vulnerability.
- The cost to improve technology systems, including security hardening in systems or applications.
- The loss of intellectual property value, such as proprietary information, trade secrets or other priceless intangible assets.

12. How Much Does Cyber Insurance Cost?

Typically, cyber insurance pricing is based on the insured entity's annual revenue, industry, extent and type of coverage, and the size of the organization. Organization size matters because more employees mean a larger attack surface for malicious actors, and more insurance coverage is required. Industry is an important factor, because industries such as healthcare and finance manage large amounts of sensitive data and deal with more risk.

The past few years have seen a surge in cyber insurance premiums and payouts, a trend attributed to the expanding attack surfaces and evolving adversary techniques. A typical policy can cost from $500 to $5,000 or more a year according to Progressive Casualty Insurance Company.

The most prevalent misunderstanding is that cyber insurance is costly. Most people believe that only big businesses need to get cyber coverage. However, in practice, the price of cyber insurance has decreased over time, particularly for small and medium-sized enterprises.

It’s frequently a little investment to pay for the security and peace of mind it offers in comparison to the monetary losses from a cyberattack.

In 2021, U.S. businesses paid an average of $132 per month for cyber insurance, with 38% securing premiums under $100. The cost of cyber insurance varies widely depending on your business’s profile. For small businesses, premiums can start at $1,500 annually for basic coverage. Larger enterprises, especially those in high-risk industries, may pay upwards of $7,500 annually.

12.1 Why Cyber Insurance Costs Are Worth the Investment

Cyberattacks are a growing threat, with businesses suffering a cyberattack every 39 seconds. This reality underscores why cyber insurance costs are no longer optional for businesses of any size.

As businesses store sensitive customer data and rely on interconnected systems, the risks of financial and reputational damage increase dramatically. To mitigate these risks, investing in cyber insurance has become essential. Cyber insurance helps protect against the financial fallout of a cyberattack, providing a safety net for recovery and resilience.

But how much does cyber insurance cost? Let’s explore what impacts these costs and how you can ensure your investment is worthwhile.

12.2 Factors Influencing Cyber Insurance Costs

Understanding how much cyber insurance costs requires analyzing several factors. Insurers assess risk based on your business's size, operations, and security posture.

12.2.1 Business Size and Industry

Smaller businesses often have fewer resources to secure their systems, increasing their perceived risk. Certain industries, like healthcare and finance, face higher premiums because of the sensitive nature of the data they handle.

A healthcare organization storing patient records will pay higher premiums than a retail store. This is due to strict regulations like HIPAA, which increase the liability exposure for insurers.

12.2.2 Type and Volume of Data Handled

The more sensitive data you handle, the higher your cyber liability insurance costs. Hackers prioritize businesses that store financial information, Social Security numbers, or trade secrets.

If your company manages significant volumes of personal data, insurers may consider you a high-risk client. Ensure you're investing in security measures that protect this information to mitigate your costs.

12.2.3 Existing Security Measures

Businesses with robust cybersecurity frameworks often see reduced premiums. Multi-factor authentication (MFA), endpoint detection tools, and regular penetration testing demonstrate your commitment to reducing risk.

Insurers reward businesses with these safeguards because they lower the likelihood of costly incidents. For example, implementing employee cybersecurity training programs can decrease how much cyber insurance costs over time.

12.2.4 Policy Coverage and Limits

The extent of your coverage affects your premiums. Comprehensive policies that include legal fees, ransom payments, and PR crisis management cost more but offer greater peace of mind. Assess your risks carefully to avoid overpaying for unnecessary coverage.

12.3 How Much Does Cyber Insurance Cost on Average?

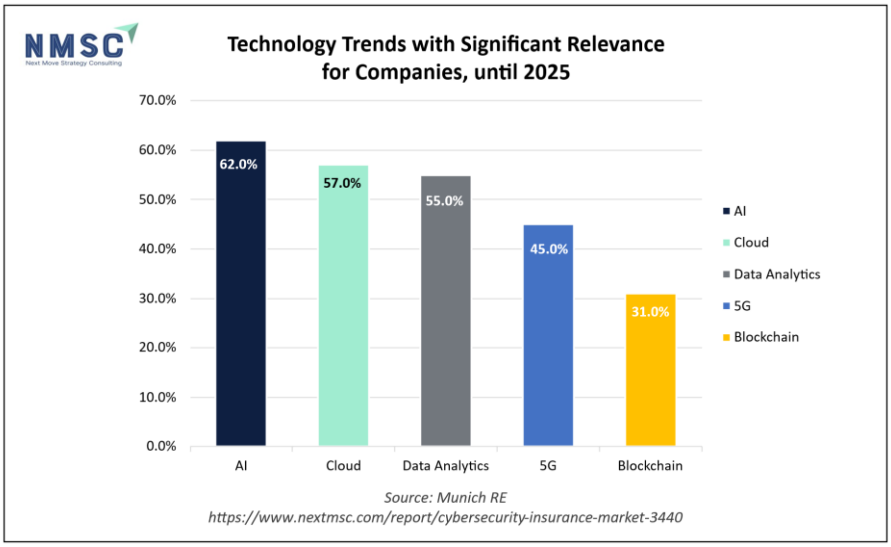
In 2021, U.S. businesses paid an average of $132 per month for cyber insurance, with 38% securing premiums under $100. The cost of cyber insurance varies widely depending on your business's profile. For small businesses, premiums can start at $1,500 annually for basic coverage. Larger enterprises, especially those in high-risk industries, may pay upwards of $7,500 annually.

13. Market Dynamics

The global Cybersecurity Insurance Market size is estimated at USD 21.37 billion in 2024 and is expected to be valued at USD 25.69 billion by the end of 2025. The industry is projected to grow, reaching USD 64.49 billion by 2030, with a CAGR of 20.21%.

The cyber insurance market has further matured. Looking to the future, the focus remains to meet increasing demand and manage dynamic risk exposures, while focussing on the sustainable insurability of cyber risks and market functionality.

Cyber risk continues to increase, driven by rapid technological advances such as (generative) artificial intelligence or cloud technology. Global industries are increasingly dependent on IT, IoT (Internet of Things), OT (Operational Technology) and digital services, such as cloud computing, each of which represent a critical part of the supply chain for many risk owners. Furthermore, the advancing sophistication of cyber criminals and the tense geopolitical situation shape the cyber threat landscape and pose a threat to global societies and democracies.



Source: Munich RE
https://www.nextmsc.com/report/cybersecurity-insurance-market-3440

In a digitalised global economy, insurers contribute significantly when protecting businesses against the cyber risks they face. Through its expertise, strong collaborative networks and clear focus on data analytics, risk quantification and accumulation modelling, the insurance industry has a deep understanding of the threat landscape and a discernment of the limits of insurability. Despite the fact that today's value chains are largely dependent on digital assets, the level of protection appears to remain inadequate.

According to the Munich Re Cyber Risk and Insurance Survey 2024, 87% of global decision makers say their company is currently not adequately protected against cyber-attacks. Cyber insurance penetration and associated resilience need to be further increased. This report provides an outlook on the cyber risk landscape and the surrounding dynamics affecting cyber insurance.

Experts and authorities face challenges in compiling adequate statistics on cybercrime and it is likely that the data represent only a small proportion of total cybercrime. For example, the German Federal Criminal Police Office (BKA) estimates that up to 91.5% of criminal cyber incidents go unreported. Past trends may not always be indicative of future ones. Nevertheless, lessons learned from attack patterns, vulnerabilities and losses are important for future cyber readiness. Equally, it is essential to anticipate major impacts of potential threats on all levels - from private individuals to single companies to nation-states.

14. Major Loss Drivers in Cyber Insurance

Munich Re loss data and experience paint a clear picture of cyber risks and their impact on cyber insurance. This is particularly true for ransomware, business email compromise and business communication compromise, data breaches and supply chain vulnerabilities.

14.1 Ransomware

Ransomware will continue to be the dominant risk and loss driver for cyber insurance. Advances in applied technological progress and tactics point to a more complex and damaging ransomware landscape, where more and stronger ransomware groups will shorten their dwell times, including through the use of prompt injection tactics. Ransomware-as-a-Service (RaaS) models will become even more competitive in dark web markets, partly because AI can drive or enhance them. AI will encourage a high degree of automation in hacking processes and lead to a strong individualization of attacks - with tailored phishing or email extortion that can be easily translated into multiple languages in high quality by AI and thus scaled in many regions simultaneously.

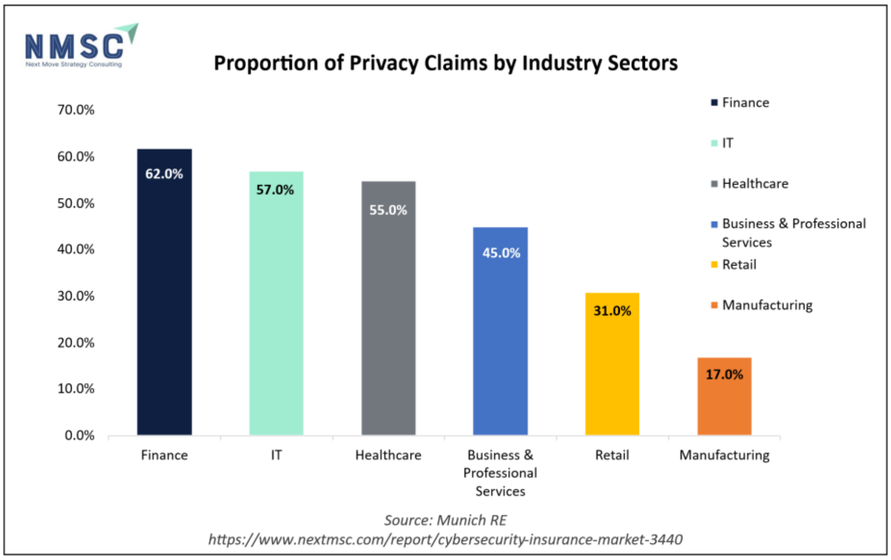
14.2 Business Email Compromise (BEC) and Business Communication Compromise (BCC)

For 2024 and beyond, Munich Re experts anticipate a sharp increase in BCC and BEC attacks. These will deceive people within companies into performing harmful actions, such as making unauthorized payments or sharing sensitive data externally. As scammers seek to harvest comparatively low-hanging fruit, BEC remains a top attack vector, especially since it is easy to carry out and requires virtually no technical knowledge while reaping very high rewards. It is not only email that is used as a gateway, but also all communication platforms and social media channels. Needless to say, BEC and BCC attacks not only cause high financial losses, but also lead to an erosion of trust and reputational damage.

Examples include CEO fraud attacks, where hackers pose as executives and instruct employees to transfer money. Since AI tools and deepfake technologies have become part of the mainstream criminal's toolbox, convincing fake phone calls or digital meetings as well as videos are broadly and cheaply available for scams. In early 2024, a Hong Kong based employee of a multinational company transferred nearly $26 million to scammers after attending a video call with deepfakes of their co-workers, including the company's CFO. The employee was the only human being who attended the video call, while fake participants were impersonated with AI-driven technology.

14.3 Data Breaches

By the end of 2024, privacy regulation will cover three quarters of consumer data worldwide, but 60% of all regulated global entities will struggle to comply with intensifying data protection regulation and privacy requirements (Gartner), given the high rates of data growth driven by technology. 5G will continue to be the driving force behind mobile data growth: By 2029, 5G's share of mobile data traffic will have surged to 76%. Video traffic will account for the majority of mobile data, escalating from currently slightly above 70% of all mobile data traffic to 80% by 2029 (Ericsson).



Source: Munich RE
https://www.nextmsc.com/report/cybersecurity-insurance-market-3440

Amidst all technological developments, one factor should not be forgotten when discussing data breaches or other cyber incidents: The value and criticality of data, together with governing data regulation and underlying issues regarding liability, will further push the emergence of more groups offering hack-for-hire and data theft services. Nevertheless, even the most advanced data breaches with AI enhanced spear phishing will still involve the human element in approximately 90% of instances (Forrester). Multifaceted efforts to create awareness and implement proper defence that goes beyond technology are and will be a must.

14.4 Supply Chain Vulnerabilities

Dependencies on software and hardware supply chains and digital services will continue to rise tremendously. As the obvious Achilles' heel of organizations, the supply chain consequently attracts attackers. Munich Re experts expect hacks across networks of suppliers, manufacturers and providers within digital supply chains (IT/OT/IoT) to increase further. Organizations will also witness a greater number of "supply chain attacks as a service", opening up this field to other less tech savvy hacker groups.

To put the potential impact in perspective: According to a World Economic Forum study (WEF 2024), 41% of companies surveyed have been affected by a third-party cyber incident. Small and medium-sized suppliers are being increasingly targeted with the aim of later hacking into their larger customers' systems.

15. 5 Essential Cyber Insurance Requirements

Cyber attacks and other malicious activity reached unprecedented levels in 2021, impacting all kinds of U.S.-based small businesses. Over the course of the year, the FBI's Internet Crime Complaint Center (IC3) received almost 850,000 complaints. It also recorded over $6.9 billion in potential losses due to cyber incidents.

As cyber threats continue to spread, organizations should take every precaution available to lower their overall cyber risk. Cyber insurance can provide an effective stopgap for cyber risk. Comprehensive cyber insurance covers everything from indemnification for legal fees to incident recovery costs.

However, to qualify for such coverage, an organization must meet certain security requirements. These requirements also align with overall cybersecurity best practices and controls to protect a business.

Insurance companies typically look for five essential cyber insurance requirements before agreeing to provide cyber insurance coverage. Chances are that your clients lack these security controls across their computer systems and IT infrastructure. In that case, the following security controls can reduce the likelihood and impact of a cyber incident while helping to qualify the business for coverage.

15.1 Multi-factor authentication

Multi-factor authentication (MFA), also known as two-factor authentication, is one of the best security controls available for securing user accounts and preventing unauthorized logins. MFA requires users to log into an account to validate their identity with a username and password. An additional layer of security authenticates users by way of a second factor," such as a one-time code sent to their mobile device, email, or from a token.

Internally, when required for every login, MFA adds an additional layer of protection, making it more difficult for threat actors to access unauthorized resources. It's also a necessity in an increasingly remote workforce, when users can log into almost any work device from almost anywhere.

Externally, MFA can reduce the number of internet-facing accounts threat actors may attempt to break into, such as work email accounts. It can also limit the impact of cyber attacks like social engineering. Even if a threat actor obtains a password, they would still need the additional level of authentication to access the account.

15.2 Cybersecurity training

Cybersecurity training is one the most cost-effective security methods available. Routine training can help educate team members about the latest threats and remind them to stay vigilant against potential malicious activity. It also matters because the majority of breaches come from human error.

According to Verizon's 2022 Data Breach Investigations Report, 82% of breaches this year were initially caused by human error. This includes the use of stolen credentials after someone fell for a phishing email and social engineering attempts. Cybersecurity training can teach employees to avoid these mistakes, potentially minimizing data breaches.

15.3 Maintain good data backups

A good data backup can mean the difference between a complete loss or a full recovery after a cyber attack. Maintaining data backups may also be a recommendation for your cyber insurance policy, depending on your organization's data.

Redundancy is critical in a good backup strategy. Businesses should use both on- and off-site backups for storing essential data. It's critical that at least one form of backup be stored completely separate from the primary network, such as in an external drive or tape. Store one copy on an off-site device, like a cloud server.

Test your backups by frequently conducting a full recovery. All too often, organizations only test their backups when they need them, and find out that their restoration has failed or backups were inadequate. In the case of increasingly common ransomware attacks, backups are the key determinant of whether a ransom payment is made or not. Without backups, a business is at the mercy of threat actors.

15.4 Identity access management

While there are numerous ways of applying identity access management (IAM) across networks, the basic focus is on assigning and managing digital identities for users that require it. This helps ensure that only certain users can access certain data, depending on their role within the organization.

15.5 Enforcing data classification

This means that users should only have enough digital rights to perform their job functions. Data classification or “need to know” access helps organizations to ensure they are enforcing this principle across all devices to meet cyber insurance requirements.

In a strict application of least privilege, users would not have the right to install or modify software on a company-issued device. They would only be able to access data and resources pertinent to their role.

15.6 Additional cyber insurance requirements

In addition to the essential cyber insurance requirements, there are some other components that are less critical but still important. Following these requirements can help an organization secure more favorable rates on a cyber policy and ensure that its security controls are effective.

- **Strong password policies**. Passwords are at the forefront of security controls. Businesses should ensure that all employee and network passwords are unique, strong, and regularly changed.
- **Antivirus or Endpoint Detection and Response (EDR) software**. Your clients should install and regularly update antivirus or EDR software on all user devices. This can increase the chances of identifying a potential vulnerability before it turns into a claim.
- **Firewalls**. Through firewalls, your clients can block incoming and outgoing traffic on devices according to rules that the system administrator sets. A firewall can block incoming malicious traffic and outgoing threat actor communications from a compromised device.
- **Incident response plans**. All organizations should have a cyber incident response plan in place in case of a cyber incident. These plans lay out a series of concrete steps and stakeholders the business should initiate to prepare for, and respond to, an incident.
- **Security risk assessments**. These assessments can help your clients identify any vulnerabilities within their networks and processes. They give businesses clearer insights into the concrete steps they can take to improve their overall cybersecurity.

16. Cyber Insurance Cornerstones

In the space of a decade, cyber insurance has become an essential important component of cyber risk management for organizations and households. Against an extremely dynamic threat landscape, where geopolitical and technological stressors are setting new priorities, tackling insurability challenges and managing accumulation risk is key to the long-term sustainability and functionality of a still maturing market. Insurers and risk modelers continue to explore the limits and possibilities of insurability. Prudent further development of the market is necessary, with anticipated future global demand requiring sufficient capacity from insurance and alternative capital markets.

Cyber risk must be managed properly and collectively. This is also true of those risks that cannot be managed, or at least not fully, by the private sector.

16.1 Governmental cyber protection

Cyber insurance has undoubtedly helped to build an effective layer of resilience. However, the insurance industry’s risk-bearing capacity has natural limitations. The damage from catastrophic systemic events like cyber war or outage of critical infrastructure would far exceed the industry’s capacity. Such scenarios pose a threat to macroeconomic stability which is why societies need the involvement of governments to manage these potentially catastrophic cyber risks. Munich Re can and will support the development of solutions and clearly advocates for the implementation of economic cyber protection as a precautionary measure of last resort. The dialogues on so-called "governmental backstops" have already begun.

Insurers face a major challenge in their endeavors to close the gap between economic losses and insured losses. Given the very dynamic growth of risks in a digitized economy, higher insurance penetration for cyber risks is the paramount aim. By helping to safeguard the digital world, insurers will once again demonstrate the industry’s relevance to the resilience of the economy and society. The insurance industry offers a variety of attractive solutions which continue to convince the uninsured. At the same time, the focus lies on ensuring that insurance cover is sufficient and offered on a sustainable basis.

17. What Is Cyber Insurance and Why Is It Essential?

Cyber insurance protects your business from financial losses caused by cyber incidents. These could include hacking, ransomware, or data theft. With the increasing sophistication of cyberattacks, traditional insurance policies no longer offer sufficient protection against digital risks.

Choosing the right cyber insurance ensures you are prepared to recover from a range of scenarios. From covering the cost of breach response to compensating affected customers, these policies address critical gaps.

Without this coverage, businesses face significant financial exposure that could threaten long-term survival.

18. Conclusion

This manuscript has provided a thorough examination of cybersecurity insurance, encompassing its definition, operational mechanics, covered risks, exclusions, benefits, requirements, costs, and integration with broader cyber risk management strategies. By adhering to the outlined steps for risk reduction and understanding the major loss drivers, organizations can better position themselves to leverage cyber insurance effectively.

Ultimately, cyber insurance serves as a vital financial tool but must be paired with proactive cybersecurity measures to achieve comprehensive protection in an evolving threat landscape. The growing market and governmental involvement further emphasize its importance for future resilience.

References

1. https://www.fortinet.com/resources/cyberglossary/cyber-insurance
2. https://www.techtarget.com/searchsecurity/definition/cybersecurity-insurance-cybersecurity-liability-insurance#:~:text=Cyber%20insurance%20offers%20financial%20security,among%20customers%2C%20stakeholders%20and%20partners.
3. https://mitigata.com/blog/top-benefits-of-cyber-insurance/#:~:text=Cyber%20insurance%20offers%20financial%20protection,resources%20that%20reduce%20future%20risk.
4. https://www.coalitioninc.com/topics/5-essential-cyber-insurance-requirements
5. https://www.secopsolution.com/blog/why-cyber-insurance-isnt-a-substitute-for-strong-cybersecurity-measures#:~:text=Cyber%20insurance%20is%20a%20useful,in%20case%20of%20an%20attack.
6. https://www.systems-x.com/blog/cyber-security-insurance-costs
7. https://www.nextmsc.com/report/cybersecurity-insurance-market-3440
8. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html#:~:text=AI%20and%20related%20technologies%20can,data%20analytics%2C%20telematics%20&%20predictive%20modelling
9. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html#:~:text=AI%20and%20related%20technologies%20can,data%20analytics%2C%20telematics%20&%20predictive%20modelling
10. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html#:~:text=AI%20and%20related%20technologies%20can,data%20analytics%2C%20telematics%20&%20predictive%20modelling
11. https://www.nextmsc.com/report/cyber-insurance-market
12. https://www.nextmsc.com/report/cyber-security-market
13. https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx
14. https://cybersecurityguide.org/resources/cyber-defense/
15. https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
16. https://www.ibm.com/think/topics/intrusion-detection-system
17. https://www.nist.gov/cyberframework
18. https://www.nextmsc.com/report/us-insurance-market
19. https://www.hhs.gov/hipaa/index.html
20. https://en.wikipedia.org/wiki/Operational_technology
21. https://www.bka.de/EN/Home/home_node.html
22. https://www.ibm.com/think/topics/ransomware-as-a-service
23. https://www.nextmsc.com/report/5g-technology-market
24. https://www.weforum.org/
25. https://www.nextmsc.com/report/consumer-identity-and-access-management-iam-market