Journal of Human Security | 2025 | Volume 21 | Issue 1 | Pages 35-42
DOI: https://doi.org/10.12924/johs2025.210107
ISSN: 1835–3800

Journal of Human Security

Research Article

Compensation for Damage from Cyberattacks

Ahmed Jaafar Shawi

Ministry of higher education and scientific research/Baghdad/Iraq

***Correspondence:** ahmed.j.shawi@mohesr.gov.iq

Submitted: 11 January 2025 | Revised: 29 March 2025 | Accepted: 09 May 2025 | Published: 30 June 2025

Abstract: Cyberattacks are very dangerous for humans and businesses, so there needs to be a way to compensate them that works well to lessen their effects on operations and finances. The study gives a thorough look at cyberattack compensation, going over the different types of dangers and their history, as well as what they mean for the people involved. The frameworks related to legal are presented at both the international and national levels, with an analysis of each's effectiveness regarding the risks concerning cyber. This study presents a case study analysis in this report, examining the role of cyber insurance, coverage types, emerging challenges, and private and governmental sector compensation models. The discussions of the economic implications involved include cost-benefit analysis and financial sustainability. The present research explores the advancement of technologies, including blockchain and smart contracts, that could benefit compensation progressions. The review culminates with policy recommendations, and the emphasis is placed on future research areas- integration of innovative technologies and dynamic regulatory frameworks toward strengthening resilience in the face of cyber threats.

Keywords: Cyberattacks, Compensation Mechanisms, Cyber Insurance Legal Frameworks, Economic Implications, Blockchain Technology, Risk Management, Policy Recommendations

1. Introduction

1.1 Background on Cyberattacks

Cyberattacks are intentional attacks on information systems aimed at disrupting, damaging, or gaining unauthorised access to data. These attacks have increased in numbers and sophistication over time and become a serious threat to individuals, businesses, and governments. Common types are malware, phishing, DoS/DDoS, and SQL injection. Recent trends indicate an increase in ransomware, supply chain attacks, and targeted critical infrastructure. All the above have been known to have wide-ranging impacts, such as economic losses, data breaches, or even national security threats. Understanding these evolving and emerging threats and their adoption to proper cybersecurity measures is crucial to mitigate their impact on society and ensuring data security [1].

1.2 Importance of Compensation Mechanisms

Compensation mechanisms play a key role in reducing the financial and reputational damages resulting from cyberattacks. The world can expect to lose $10.5 trillion annually by 2025 due to cybercrime, which includes data destruction, theft, and disruptions to business operations [2].

Effective compensation strategies, such as cyber insurance and robust security controls, help organizations recover losses and maintain stakeholder trust. Implementing compensating controls addresses vulnerabilities, ensuring compliance with security standards and reducing incident impact [3].

These mechanisms are important for organizational resilience and continuity in the face of escalating cyber threats.

1.3 Scope and Objectives of the Review

This review aims to cover compensation mechanisms for damages generated by cyberattacks based on recent developments and challenges. The current state of effective compensation strategies for cyber insurance and legal frameworks in addressing financial and reputational losses will be evaluated [4]. Besides this, the paper shows policy development and international cooperation in reinforcement mechanisms. This paper draws from recent studies to synthesise findings on compensation approaches that can be optimised to build organisational resilience against cyber threats [5].

2. Overview of Cyberattacks

2.1 Types of Cyberattacks

Cyberattacks are attacks intended to harm computer systems with the intent to steal, alter, or destroy data. Among the most common types are:

•Malware: Malicious software that includes viruses, worms, spyware, and ransomware which enter systems for malicious purposes [6].

Phishing: Phishing is instigated by false communications. it is especially observed in the form of email. It dupes the email receivers by giving away confidential information [6].

Denial-of-Service and Distributed Denial-of-Service (DDoS) Attacks: Overwhelming a system's resources, which prevents it from responding to legitimate requests .

Man-in-the-Middle (MitM) Attacks: An attack where an attacker secretly intercepts and possibly modifies the communication between two parties [7].

SQL Injection: Introducing malicious code into a server through Structured Query Language in order to gain access to unauthorized data [8].

Knowledge of these attack types will help to devise the proper cybersecurity strategy.

2.2 Historical Incidents and Case Studies

Historical cyberattacks show how the threat environment has changed over time. For example, the 2017 Equifax breach, in which hackers stole the data of about 147 million people, showed how weak data protection was. [9].

In the same way, in 2016, an attack on the Korean Cyber Command exhibited risks even within the cyber infrastructures of military [10].

The above incidents prove the necessity for strong cybersecurity measures and constant alertness [11].

2.3 Impact of Cyberattacks on Organisations and Individuals

The cyberattacks make significant damage to individuals and

organisations, resulting in financial losses, operational disruptions and reputation damage. For industries, the cyberattacks result in significant financial losses from theft, liability to lawsuits and the cost of recovery. Reputation loss causes a loss in consumer confidence and loss of customers. Operational disruption may even pause business activities, leading to further economic losses. There is a risk to privacy and security due to identity theft, financial fraud, and credential theft. Cyber threats are widespread nowadays, and thus cybersecurity requires control measures to ensure trust with assets [12].

3. Legal Frameworks for Compensation

3.1 International Laws and Regulations

There are still emerging international laws concerning compensation for damages from cyberattacks, and existing frameworks present notable challenges. Specifically, the UN Charter forbids using force against sovereign states while its application regarding cyberattacks remains ambiguous, especially regarding non-state actors [13]. The Tallinn Manual provides guidelines on the application of international law to cyber operations but does not have binding authority. Moreover, the duty to prevent and redress transboundary harms is recognized, but its enforcement in cyberspace is limited [14]. It reflects a need for incorporating comprehensive international legal frameworks to handle compensation for damages from cyberattacks.

3.2 National Legislation and Policies

National laws on compensation for cyberattack damages differ across jurisdictions, reflecting diverse legal frameworks and policy approaches. In the United States, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires immediate reporting of cyber incidents, thereby strengthening the government's ability to respond and, in turn, possibly enable compensation mechanisms [15].

The United Kingdom's upcoming Cyber Security and Resilience Bill is intended to bolster cyber defenses, and the bill will also have provisions for cost recovery mechanisms that allow regulators to ensure essential cybersecurity measures are implemented [16].

As provided under the General Data Protection Regulation, individuals have the right to claim compensation for damages resulting from data protection breaches, which includes both material and non-material harm [17].

However, the Court of Justice of the European Union clarified that no compensation would be awarded just because the GDPR is infringed; actual damage needs to be proven [18].

3.3 Comparative Analysis of Legal Frameworks

A comparative analysis of legal frameworks for compensating cyberattack damages reveals significant disparities among jurisdictions. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 in the United States says that cyber incidents must be reported right away. This makes the government's response better and the process for getting paid easier. On the other hand, the EU's General Data Protection Regulation lets people who have had their data stolen get paid for both material and non-material damages, putting individual rights first [19]. The EU Court of Justice has made it clear, though, that breaking the GDPR does not automatically mean you are entitled to compensation; you must show that you suffered actual harm. Some countries don't have specific laws about how to pay for cyberattacks, so they use general tort law instead. This may not work well for the specific problems that come up in cyber incidents. This kind of difference makes it necessary for countries to have the same laws so that victims are treated fairly and get the same amount of money [20].

4. Insurance and Cyber Risk Management

4.1 Role of Cyber Insurance

4.1.1 Role of Cyber Insurance

Cyber insurance is a special type of policy that protects businesses from losing money due to cyber incidents like cyberattacks, data breaches, and other digital attacks [21]. This is an important part of managing cyber risk because it includes costs for data recovery, lawyer fees, notification costs, and any damage to your reputation that happens [22]. Additionally, the cyber insurance policy covers access to resources like public relations help and credit monitoring services for people who have been affected by cyber attacks as part of a full response to the attacks.

Though coverage specifics differ, and some exclusions apply (e.g., pre-existing breaches or events initiated by inside sources), such as those explained in [21; 22].

By way of cyber threats continue to evolve, the market related to cyber insurance has emerged. The partnership of public-private is discussed in addressing large-scale, "uninsurable" events, displaying how the risk management of dynamic cyber is [23].

4.1.2 Types of Coverage and Policies

The insurance on cyber policies covers monetary loss due to cyber incidents by offering different types of coverage as appropriate to any risks related to cyber. A general cyber insurance policy would contain:

The Coverage of First-Party helps to cover actual losses suffered directly by the protected organisation due to the attack. For example, recovery of data or systems, lost business, or notification costs; it covers some of the necessary expenses for rebuilding operations and taking care of direct consequences [22; 23].

Third-Party Coverage: This refers to claims against the insured by third parties who suffered from the cyber incident. These include legal fees, settlements, and regulatory fines resulting from data breaches or failures in network security that affect clients or partners. For instance, if customer information is leaked in a data breach, third-party coverage would help manage the legal liabilities and regulatory penalties that ensue [24].

Some policies also contain specialized coverages, including:

Regulatory Liability: It insures legal expenditures for defending an organization against regulatory violations of its privacy regulations in addition to fine and penalty arising from the event [24].

PCI Fines: It pays fine and penalty for the Payment Card Industry Data Security Standard (PCI DSS) for the covered members [24].

It is important to note that the specifics of coverage may differ from one insurer to another, and there may be certain exclusions applicable, like pre-existing breaches or insider-initiated events. Organizations should thus take the time to understand their unique risk profiles and work with insurance professionals to craft policies that meet their needs [25].

4.1.3 Challenges in Cyber Insurance

Cyber insurance is a vital part of managing cyber risk, but its development has been hindered by the following:

Lack of History: Cyber risks are relatively recent phenomena, and the exact amount of history is not available to model or estimate risks for proper underwriting and coverage options [26]. This lack of history complicates the process of underwriting and creating suitable coverage options [27].

Underreporting of Incidents: The majority of cyber incidents are underreported, with an estimated 91.5% of cases not reported. This underreporting does not allow for comprehensive data collection to be used in the determination of risk and premium setting [28][29].

Aggregation Risk: Cyber attacks may result in massive, simultaneous losses across various policyholders, especially when systemic attacks are involved. Aggregation risk is, therefore, one of the greatest challenges facing insurers in terms of capital allocation and risk diversification [30].

Ambiguity in Policy Terms: Differences and ambiguities in policy wording can lead to misinterpretation and disputes over coverage after cyber incidents. The absence of standard terms complicates the claims process and may leave policyholders uncertain about their scope of coverage [31].

Insurers, policymakers, and organisations must work together to address such issues, improve data sharing, and craft policy language and innovative solutions for emerging cyber risks.

5. Compensation Models and Mechanisms

5.1 Governmental Compensation Schemes

Governmental compensation mechanisms are schemes offered by governments to financially compensate victims or affected bodies for losses resulting from specific events, including cyberattacks. These generally address situations when the victims, in their quest to get compensation legally, do not have enough redress avenues; or they were not covered or compensated by traditional insurance.

For example, the Australian Government's Scheme for Compensation for Detriment Caused by Defective Administration (CDDA) provides an avenue for compensation when a person suffers detriment because of

defective administration. Although not specifically created for cyber incidents, such schemes can be applied to losses resulting from governmental lapses in cybersecurity [32].

However, implementation challenges often characterize such schemes. For instance, according to the National Audit Office, a report indicates that, in the absence of a central strategy in developing compensation schemes, it tends to cause inefficiencies and delay, hence hurting public trust [33].

Besides, with the dynamic nature of cyber threats, public-private partnerships have become increasingly essential in dealing with large-scale cyber incidents. According to the U.S. Government Accountability Office, there is a need to consider potential federal responses to catastrophic cyberattacks, considering that existing insurance mechanisms may be inadequate to address widespread losses [34].

In a nutshell, although government compensation schemes have been important for addressing cyber-related damages, their effectiveness hinges on timely implementation, clear guidelines, and collaboration between public and private sectors to adapt to the dynamic nature of cyber threats.

5.2 Private Sector Compensation Models

Main cyberattack damage private sector compensation models mostly involve cyber insurance policies, aiming to reduce any resulting losses in terms of finance due to cyber incidents. These policies tend to cover almost all expenses for data restoration and legal fees to recoup business loss.:

Evolving Threat Landscape: The rapid evolution of cyber threats necessitates that insurance policies continually adapt to new vulnerabilities and attack vectors. This dynamic environment complicates the underwriting process and the development of comprehensive coverage [35].

Aggregation Risk: Cyber events can cause the loss of many insureds at a single point in time, primarily due to systemic attacks. It is an important challenge for the insurers in the context of allocating capital and spreading risks [36].

To overcome these challenges, public-private partnerships are increasingly being needed in dealing with large-scale cyber incidents. Cooperative efforts between governments and the private sector increase the sharing of data, standardize policy language, and develop new innovative solutions for emerging cyber risks [37].

In summary, private sector compensation models such as cyber insurance play a critical role in reducing financial losses from cyberattacks; however, their effectiveness depends on continuous adaptation to the evolving threat landscape and collaboration between public and private entities to address systemic risks.

5.3 Case Studies of Effective Compensation Mechanisms

After a cyberattack, an organization needs good ways to pay its employees in order to recover and stay strong. Looking at case studies can help you learn about successful strategies.

Cyberattack on Saudi Aramco: In 2012, Saudi Aramco was hit by a major cyberattack that disrupted operations. The company's response included detailed plans for handling incidents and compensating victims, with a focus on combining threat intelligence with real-time response systems. These strategies not only helped limit the damage right away, but they also helped the organization become more resilient to cyberattacks in the long run [9].

Colonial Pipeline Ransomware Attack The ransomware attack on Colonial Pipeline in 2021 resulted in significant operational disconnections. Coordinated efforts towards restoring services and allaying the concerns of stakeholders marked compensation mechanisms of the company. Strong incident response plans and communication strategies are a prerequisite for the response to cyber crises [38].

5.4 Economic Implications of Cyberattack Compensation

5.4.1 Cost-Benefit Analysis of Compensation

Companies rquired to do a cost-benefit analysis of cyberattack compensation to find the best ways to limit the damage from a cyberattack that are also the most cost-effective. This analysis weighs the costs of putting in place protections against and stopping different types of cyberattacks against the possible financial losses from cyber incidents.

A complete CBA should include both direct and indirect costs:

Direct Costs: These are the costs of recovering data, paying lawyers, paying fines to regulatory bodies, and giving money to people who were hurt. The total cost of recovering from ransomware, for instance, has gone up a lot: from $761,106 in 2020 to $1.85 million in 2021 [39].

Indirect costs include things like losing customers' trust, damaging your reputation, and problems with operations. Intellectual property theft, lost productivity, damage, and destruction of data, stolen money, and damage to reputation are some of the other costs of cybercrime [2]. Companies can figure out the return on investment [40] for cybersecurity by putting numbers on these things. Investing in strong cybersecurity can greatly lower the chances and effects of cyberattacks, which in turn lowers the amount of compensation costs that may come up. The best way to get the money you need to deal with major cybersecurity threats is to do a cost-benefit analysis [41].

A thorough CBA helps businesses make smart choices about how much money to spend on cybersecurity by weighing the cost of preventive measures against the cost of cyber incidents.

5.5 Economic Impact on Businesses and Economies

Cyber attacks have a big effect on businesses and economies because they cost a lot of money in both direct and indirect ways:

Costs that are direct: Cyber events will usually cost a company a lot of money in a direct way. Equifax, for instance, had to pay more than $1 billion in fines after its data breach in 2017. This shows that the attack has a very bad effect on a business's finances [42].

Disruptions to operations: A cyberattack could shut down a business, which would cost more time and money to get it back up and running. A study of Japan's cyberattack losses found that problems in one area could quickly spread to others, making the economy even worse [43].

Damage to your reputation. Customers would lose trust if there were violations, which would eventually cause them to leave or lower sales. The National Bureau of Economic Research says that companies that own high-value intangible assets are the ones that are most affected. Their market value goes down a lot when their reputation is hurt [44].

Wider Effects on the Economy On a larger macroeconomic scale, cybercrime is thought to cost the world economy almost $600 billion each year and make up almost 1% of global GDP [45].

This huge amount is a sign of how dangerous cyber attacks are to economies all over the world.

5.6 Funding and Financial Sustainability of Compensation Mechanisms

A major problem for both businesses and economies is how to make sure that compensation systems for cyberattack victims are financially stable. The International Monetary Fund says that cyberattacks are one of the biggest threats to global financial stability, so strong governance frameworks are needed to keep these risks under control [46].

Organizations in their quest to overcome these difficulties are embracing the cybersecurity factor as part of their ESG strategies. The business value of ESG underscores the importance of maintaining a level of operational resilience and ensuring long-term sustainability [46; 47].

Aside from that, the financial sector's interdependence during a cyber incident at one institution can have terrible effects on other institutions and make the system as a whole more risky. So, we need to come up with long-term ways to pay people that focus on:

Strong cybersecurity: Security measures are taken ahead of time to stop attacks and lessen any damage they may cause [48].

Sufficient Financial Resources: Setting aside specific funds or insurance coverage to offer prompt compensation to the affected parties [49].

Compliance: This implies observing the new standards of laws for accountability and transparency in compensations (Khalid et al., 2024).

Through such strategies, organizations can boost their resilience towards cyber threats while making compensation mechanisms financially sustainable [50].

By adopting these strategies, organizations can enhance their resilience against cyber threats and ensure the financial sustainability of compensation mechanisms.

5.7 Technological Considerations

5.7.1 Role of Technology in Assessing Damage

It plays a very important role in damage assessment, especially post-

disaster situations. Traditional approaches were usually very time-consuming, and prone to errors, relying on manual data collection. The advancement of technology has changed the process, which is now much more efficient and precise [51].

The first major development is the use of mobile application development that enables uploading information to residents and responders regarding structural damages. For example, following the 2012 Emilia earthquake, a mobile app was developed to facilitate initial damage evaluations. This approach was helpful, especially since there weren't many expert resources, and it improved the quality of emergency response by making quick and accurate information available [52]. GIS has been very useful for managing and analyzing spatial data. GIS makes detailed maps and models of the areas that were affected by using data from sources like remote sensing images. It helps keep an eye on changes, come up with plans for recovery, and make resources last [53].

The UNDP is also moving away from paper-based assessments and toward digital tools. With technology, disaster damage assessment can now figure out the best way to put resources in the right places so that public officials can use them where they are needed most [54].

In short, using technology in assessment processes has made it much easier to get, analyze, and respond to damages in disasters, which helps people make better decisions about how to recover and what to do next.

5.7.2 Use of Block chain and Smart Contracts in Compensation

Using blockchain technology and smart contracts to automate the compensation system has benefits like integration, openness, and speed. Smart contracts are pieces of code that are stored on the blockchain and run automatically when certain conditions are met [55].

Table: Applications in Compensation Mechanisms:

Application Area	Description	Example
Incentive Compensation	Automates the distribution of incentives based on predefined criteria, ensuring timely and accurate payments.	A company could implement a smart contract to automatically release bonus payments to employees upon achieving certain performance metrics. Medium
Service Level Agreements (SLAs)	Facilitates dynamic compensation by automating penalty payments when service providers fail to meet agreed-upon performance levels.	If a cloud service provider's uptime falls below the SLA threshold, a smart contract could automatically compensate the customer. IEEE Xplore
Insurance Claims	Streamlines claim processing by triggering payouts when specific conditions are verified, reducing the need for manual intervention.	In parametric insurance, a smart contract could automatically disburse funds to farmers when a drought is detected via weather data. Reuters

5.8 Benefits

Efficiency Automates processes, reduces administrative overhead, and minimizes errors.

Transparency creates an immutable record of transactions, which increases the amount of trust between parties.

Cost Savings: Eliminates intermediaries, thereby reducing associated costs.

By applying blockchain and smart contracts, organisations can enhance the effectiveness and reliability of their compensation mechanisms, thus contributing towards efficiency in operations and higher satisfaction from the stakeholders.

5.9 Cybersecurity Measures to Minimize Damage

The potential damage from actualised cyberattacks is minimal, largely due to the execution of strong security measures. Many key strategies have come out in very recent literature including:

5.9.1 Regular Data Backups

Regularly back up critical data so that, in the event of an incident, most information can be regained with minimal disturbances. The United States Small Business Administration advises conducting weekly backups to the cloud storage facility to reduce cases of data loss [56].

5.9.2 Access Control Management

Strict access controls limit the exposure of data. Data repositories must be audited regularly, and administrators must be assigned to monitor user permissions. Employees should only have access to information relevant to their jobs [57].

5.9.3 Strong Password Policies

Generalizing, enforcing the use of strong and unique passwords across all devices and accounts is basic. The Information Commissioner's Office advises using robust passwords to protect personal and organizational data [58].

5.9.4 Employee Training and Awareness

Employees are less likely to cause a breach due to human error if they are educated and aware of optimal cybersecurity usage. Training should include how to identify phishing attacks and internet safety [59].

5.9.5 Regular Software Updates

Keeping applications and systems up to date eliminates known vulnerabilities. CISA is keen on warning the public that keeping applications updated in real time is a way of ensuring security [60].

5.9.6 Incident Response Planning

Having an incident response plan in place and regularly updating makes the business prepared for possible cyber incidents. A company such as JPMorgan Chase requires a disaster recovery plan that protects data and restores systems, Morgan stated in 2022.

By implementing these measures, organisations can significantly reduce the risk and impact of cyber threats.

6. Challenges and Limitations

6.1 Legal and Regulatory Challenges

The legal and regulatory environment surrounding cybersecurity poses several challenges for organisations. Some of the major concerns are:

6.1.1 Dynamic Regulatory Requirements

The cyber threats are dynamic, and thus the regulations need to be updated continuously. Organisational awareness regarding changes in regulatory laws is required to comply with their presence [61].

6.1.2 Jurisdictional Differences

The cybersecurity laws of different regions are different, which makes it challenging for the multinational organizations to have uniform compliance [62].

6.1.3 Liability and Accountability

Assigning liability in case of a cyber breach is very complex, especially if third-party vendors are involved. Recent cases indicate that service providers may face serious legal consequences [63].

6.1.4 Compliance Costs

This adherence to different types of regulatory requirements is very costlier, especially to small and medium-sized enterprises (CompTIA, 2024).

6.1.5 Fast Pace of Technology

Advances in technology move much faster than the laws designed for

them and often leave voids in legal compliance [64].

It calls for an active strategy, including regular meetings with lawyers, a budget for the compliance program, and community engagement to remain vigilant for regulatory amendments.

6.2 Economic and Financial Barriers

The implementation of good cybersecurity measures will often face tough economic and financial hurdles, mostly for SMEs. A summary review shows that SMEs can lack the wherewithal to finance a cybersecurity infrastructure, keeping them exposed to cyber threats [65].

In addition, achieving investment in advanced security technologies and skilled personnel would be impossible due to the ever-changing nature of cyber threats over time. This often requires a higher investment cost, especially for companies with restricted budgets. The constraint in this regard further bites harder as the business has to abide by changing regulatory regimes, which at times, may present additional economic costs that they need to assume in order to sustain cybersecurity resilience.

These economic and financial barriers need to be addressed from multiple angles. This includes developing cost-effective security solutions, creating government incentives, and merging industry capabilities to pool resources and knowledge. Such strategies can help to alleviate the financial burdens involved with designing and maintaining these highly effective forms of cybersecurity.

6.3 Technological and Operational Limitations

Robust cybersecurity measures in OT environments have many technological and operational challenges associated with them. The most prominent limitations are identified as below.

6.3.1 Legacy Systems

Most of the OT systems are based on outdated hardware and software that do not offer the latest security features to curb cyber threats [66].

6.3.2 Insufficient Network Segmentation

Lack of proper segmentation enables attackers to laterally move within the network after having crossed the boundary. Such a condition will increase the potential impact of cyber incidents [67].

6.3.3 Inadequate Authentication Mechanisms

Lack of satisfactory authentication and access controls enables unauthorised users to access sensitive systems and data [68].

6.3.4 Insecure Communication Protocols

Many OT networks are based on proprietary or legacy communication protocols that lack encryption, thereby making them vulnerable to eavesdropping and data tampering.

6.3.5 Limited Monitoring and Visibility

OT networks have limited monitoring tools, which affect the detection and response to security incidents [69].

6.3.6 Interoperability with IT Networks

The integration of IT and OT networks creates new risks because weaknesses in one can allow intruders to gain access and exploit others [69].

Therefore, it demands all-round handling, including legacy systems upgrades, the introduction of a strong authentication protocol, network segregation, and enhanced surveillance capabilities to introduce more security features into the OT environment.

7. Future Directions and Recommendations

7.1 Policy Recommendations

Developing effective cybersecurity policies is crucial for organisations to protect themselves against evolving threats. Recent literature emphasizes several key recommendations.

7.1.1 Comprehensive Risk Assessment

Organisations should conduct adequate risk assessments of their vulnerabilities so that they can prioritise security measures. This will allow for a proactive approach to targeted strategies that might mitigate potential threats [70].

7.1.2 Regular Policy Updates

Cybersecurity policies need to be dynamic in order to cope with the faster-changing threats continually. Regularly reviewing and updating them ensures policies are effective, representing the existing best practices [71].

7.1.3 Employee Training and Awareness

The greatest security threat arises from human errors. Well-planned employee training and security awareness can promote a security-aware culture and arm employees with knowledge on how to detect and act upon possible threats [72].

7.1.4 Incident Response Planning

A well-articulated incident response plan helps the organization respond to any security incidents promptly and efficiently that limits the impact of possible damage and aids in recovery [73].

7.1.5 Access Control Measures

Stringent access controls ensure that sensitive information is available only to authorized personnel, decreasing internal threats and data breaches [74].

Adoption of these policy recommendations would help strengthen an organization's cybersecurity posture to ward off the plethora of threats in the current digital environment.

7.2 Advancements in Cyber Insurance

Advances in cyber insurance are marking its future: sustainability, risk management, and market growth. Annual cyber insurance premiums are projected to increase by 15% to 20% per year, reaching about $23 billion by the end of 2026, up from around $14 billion at the end of 2023, as per S&P Global Ratings [75].

The European Union Agency for Cybersecurity, more commonly known as ENISA, has noted several breakthroughs in cyber insurance markets, where the advanced application of risk assessment technologies and speciality incident response teams has been accepted [76].

Even though the frequency and complexity of cyber incidents are rising, industrywide underwriting profitability is strong, given large rate gains and changes to policy terms that have been implemented during the last several years [77].

All of these developments speak to the increasing maturity of the cyber insurance marketplace, with a focus on proactive risk management and embracing new solutions in adapting to an evolving cyber threat landscape.

7.3 Emerging Technologies and their Role in Compensation

Emerging technologies are drastically changing compensation structures in many industries. The integration of sophisticated tools and systems is changing how organizations approach the remuneration and benefits of employees.

7.3.1 Wearable Technology

The global wearable technology market was $61.3 billion in 2022. The market is expected to grow at a compound annual growth rate of 14.6% from 2022 to 2030. For example, smartwatches and fitness trackers are enhancing workplace safety through the monitoring of employee movements and vital signs, which may eventually lead to reduced workers' compensation claims [78].

7.3.2 Telemedicine

In 2021, telemedicine became the most popular technology initiative in the workers' compensation industry. It allows for remote medical consultations, which results in faster treatment and possibly reduced compensation costs [79].

The adoption of autonomous vehicles and drones also provides advantages in workplace safety assessment and incident response. Drones can be equipped with high-resolution cameras to capture detailed images of accident scenes. It provides more detailed data for responders and adjusters, hence easing the compensation process [78].

These technological advancements indicate a growing trend towards integrating more technology into compensation systems, thereby making them more effective and efficient.

8. Conclusion

The review has researched the more complex landscape of cyberattacks and their attendant compensation mechanisms. Key findings show the rising sophistication of cyber threats and thus the importance of having adequately robust legal frameworks and advanced risk management strategies. The utilisation of cyber insurance, along with emerging technologies such as blockchain, points to an emerging trajectory for mitigating financial losses from cyber incidents. Policy implications call for dynamic regulatory adaptations and comprehensive coverage policies to strengthen resiliency. The policy implications recommend dynamic regulatory adaptations and various coverage policies to manage the increasing resilience. Future research work may thus emphasize refining the compensation models, integrating technological innovations for enhanced compensation of cyberattacks, and assessing the long-term economic impact of such compensation, making the digital ecosystem more secure.

References

[1] Alharbi F, Alsulami M, Al-Solami A, Al-Otaibi Y, Al-Osimi M, Al-Qanor F, & Al-Otaibi K. The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. Sensors. 2021;21(20):6901 https://doi.org/10.3390/s21206901

[2] Morgan JP. 12 Tips for Mitigating Cyber Risk | JPMorgan Chase. 2022.Retrieved from: . https://www.jpmorgan.com/insights/cybersecurity/ransomware/12-tips-for-mitigating-cyber-risk?utm_source=chatgpt.com

[3] Huang L, & Cornell K, editors. Cyber Protection Strategies: Balancing Insurance and Security. Proceedings of the 19th International Conference on Cyber Warfare and Security; 2025: Academic Conferences and publishing limited.http://doi.org/10.34190/iccws.20.1.3218

[4] Alsharif M, Mishra S, & AlShehri M. Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science & Engineering. 2022;40(3) https://doi.org/10.32604/csse.2022.019938

[5] Sharma A. THE IMPACT OF CYBERSECURITY BREACHES ON BIG BUSINESSES. 2024.Retrieved from: https://www.researchgate.net/publication/385421361_

[6] Alenezi MN, Alabdulrazzaq H, Alshaher AA, & Alkharang MM. Evolution of malware threats and techniques: A review. International journal of communication networks and information security. 2020;12(3):326-337 https://doi.org/10.17762/ijcnis.v12i3.4723

[7] Mallik A. Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi. 2018;2(2):109-134 https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453

[8] Ali M. Information security threats in cloud services: a comprehensive overview. 2025 https://urn.fi/URN:NBN:fi:amk-2025060420050

[9] Die YW. A Comprehensive Analysis of High-Impact Cybersecurity Incidents. Case Studies and Implications. 2023.Retrieved from: http://dx.doi.org/10.13140/RG.2.2.17461.65763

[10] Birchwood U. Real World Case-Studies on Cyber Security Incidents. Birchwood, University. 2024 https://www.birchwoodu.org/top-10-real-world-case-studies-on-cyber-security-incidents/?utm_source=chatgpt.com

[11] Park KJ, Park SM, & James JI, editors. A case study of the 2016 Korean cyber command compromise. European Conference on Information Warfare and Security; 2017.Park, K. J., Park, S. M., & James, J. (2017). A Case Study of the 2016 Korean Cyber Command Compromise. European Conference on Information Warfare and Security, ECCWS, 0, 315–321. https://arxiv.org/abs/1711.04500v1

[12] Kaushik D. The impacts of cybersecurity and AI on businesses and individuals. Journal of Student Research. 2023;12(4):1-10 https://doi.org/10.47611/JSR.V12I4.2282

[13] Katagiri N. Why international law and norms do little in preventing non-state cyber attacks. Journal of Cybersecurity. 2021;7(1):tyab009 https://doi.org/10.1093/CYBSEC/TYAB009

[14] Walton BA. Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law. Yale LJ. 2016;126:1460 https://heinonline.org/HOL/LandingPage?handle=hein.journals/ylr126&div=34&id=&page=

[15] PWC. Cyber breach reporting to be required by law for better cyber defense: PwC. Price Water Coopers. 2023.Retrieved from: . https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html?utm_source=chatgpt.com

[16] DoSIT. Cyber Security and Resilience Bill - GOV.UK. Government of United Kingdom. . 2024 https://www.gov.uk/government/collections/cyber-security-and-resilience-bill?utm_source=chatgpt.com

[17] ICO. Taking your case to court and claiming compensation. Information Commissioner's Office 2024 https://ico.org.uk/for-the-public/data-protection-and-journalism/taking-your-case-to-court-and-claiming-compensation/

[18] Eecke PV, Enrique C, & Bartholomäus R. European Court of Justice Clarifies Rules on Damages Compensation for GDPR Breaches -. cyber/data/privacy insights. FTC - Cyber/Data/Privacy Insights. 2023 https://cdp.cooley.com/european-court-of-justice-clarifies-rules-on-damages-compensation-for-gdpr-breaches/?utm_source=chatgpt.com

[19] Nansi M. (PDF) Law and Society in the Digital Age: A Comparative Study of Cyber Law and Its Impact on Medical Legal Practices. ResearchGate. 2024.Retrieved from: https://www.nao.org.uk/insights/government-compensation-schemes/

[20] kale MP. Comparative Law and Cybersecurity: Analyzing Legal Frameworks for Data Protection in the Digital Age. African Journal of Biomedical Research. 2024 http://dx.doi.org/10.13140/RG.2.2.25114.04801

[21] Micro. T. What Is Cyber Insurance? | Trend Micro (US). TrendMicro. 2025.Retrieved from: https://www.trendmicro.com/en_us/what-is/cyber-insurance.html?utm_source=chatgpt.com

[22] Nationwide. What Is Cyber Insurance? – Nationwide. Nationwide - Business solutions center . 2025.Retrieved from: https://www.nationwide.com/business/solutions-center/cybersecurity/what-is-cyber-insurance?utm_source=chatgpt.com

[23] Smith. Insurance groups urge state support for 'uninsurable' cyber risks. Financial Times. 2024.Retrieved from: . https://www.ft.com/content/c2769c6d-8bec-4167-af5c-53c6cf139851?utm_source=chatgpt.com

[24] Vaideeswaran N. Cyber Insurance Explained | CrowdStrike. 2024.Retrieved from: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/cyber-insurance/?utm_source=chatgpt.com

[25] Re M. Cyber Insurance: Risks and Trends 2024 | Munich Re. Global Cyber Risk and Insurance Survey. 2024.Retrieved from: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

[26] Zukerman A. 8 Cyber Insurance Challenges | Sapiens. Sapiens. . 2020.Retrieved from: https://sapiens.com/blog/8-cyber-insurance-challenges/?utm_source=chatgpt.com

[27] Rani N, Kaur , J. Cyber Insurance: An Emerging Challenge Cum Opportunity In The Indian Service Industry 2024.Retrieved from: https://www.researchgate.net/publication/384448922_

[28] Pirra M. Challenges in Cyber Risk Insurance. Mathematical and Statistical Methods for Actuarial Sciences and Finance: Springer; 2024. p. 261-266. https://doi.org/10.1007/978-3-031-64273-9_43

[29] Kaushik N. Risks, Trends, Challenges for Cyber Insurance | Insurance Thought Leadership. Insurance Thought Leadership. 2024 https://www.insurancethoughtleadership.com/cyber/risks-trends-challenges-cyber-insurance?utm_source=chatgpt.com

[30] Granato A, & Polacek A. The growth and challenges of cyber insurance. Chicago Fed Letter. 2019;426:1-6 https://doi.org/10.21033/CFL-2019-426

[31] Rundle J, & Stupp, C. Insurers Warn Standardizing Cyber Policies Could Limit Future Coverage - WSJ. Wall Street Journal

2024.Retrieved from: https://www.wsj.com/articles/insurers-warn-standardizing-cyber-policies-could-limit-future-coverage-fb0b7876?utm_source=chatgpt.com
[32] General A. Scheme for Compensation for Detriment caused by Defective Administration | Attorney-General's Department. Attorney-General's Department. 2024.Retrieved from: https://www.ag.gov.au/about-us/connect-us/scheme-compensation-detriment-caused-defective-administration?utm_source=chatgpt.com
[33] . NAO. National Audit Office. Lessons learned : Government compensation schemes. Report by the Comptroller and Auditor General. In National Audit Office. 2024 Retrieved from: https://www.nao.org.uk/insights/government-compensation-schemes/
[34] GAO. Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks | U.S. GAO. US Government Accountability Office 2022 https://www.gao.gov/products/gao-22-104256?utm_source=chatgpt.com
[35] Banerjee S, & Das S, editors. Analyzing the Critical Challenges of Cyber Insurance Market: A Fuzzy DEMATEL Approach. Proceedings of the International Conference on Industrial Engineering and Operations Management; 2024.https://doi.org/10.46254/EU07.20240258
[36] Jebur JK, & Abdul Rahman AT. Challenges of Insuring Cyber Risks. Pakistan Journal of Life & Social Sciences. 2024;22(1) https://doi.org/10.57239/PJLSS-2024-22.1.00161
[37] Lostri E, Lewis JA, & Wood G. A Shared Responsibility: Public-Private Cooperation for Cybersecurity. 2022 https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity
[38] UTILE L-U, & UTILE I. Analiza unor studii de caz privind atacurile cibernetice și metode propuse pentru prevenirea acestora. Revista Română de Informatică și Automatică/Vol. 2023;33(2) https://rria.ici.ro/ro/vol-33-no-2-2023/analiza-unor-studii-de-caz-privind-atacurile-cibernetice-si-metode-propuse-pentru-prevenirea-acestora/
[39] Editor. Taking a cost-benefit analysis approach to cyber security. Information Age. 2021 https://www.information-age.com/cost-benefit-analysis-approach-cyber-security-18370/?utm_source=chatgpt.com
[40] Troisi O, Fenza G, Grimaldi M, & Loia F. Covid-19 sentiments in smart cities: The role of technology anxiety before and during the pandemic. Computers in Human Behavior. 2022;126:106986
[41] Phil A. Getting the board on board: a cost-benefit analysis approach to cyber security. Information Age. 2021.Retrieved from: . https://www.information-age.com/cost-benefit-analysis-approach-cyber-security-18370/?utm_source=chatgpt.com
[42] Natalucci F, Qureshi MS, & Suntheim F. Rising cyber threats pose serious concerns for financial stability. International Monetary Fund. 2024 https://www.imf.org/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability
[43] Kokaji A, & Goto A. An analysis of economic losses from cyberattacks: based on input–output model and production function. Journal of Economic Structures. 2022;11(1):34 https://doi.org/10.1186/s40008-022-00286-4
[44] Kamiya S, Kang J-K, Kim J, Milidonis A, & Stulz RM. Economic and Financial Consequences of Corporate Cyberattacks | NBER. The Digest. . 2018 https://www.nber.org/digest/jun18/economic-and-financial-consequences-corporate-cyberattacks
[45] Lewis JA, & Baker S. The economic impact of cybercrime and cyber espionage. 2013 http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf
[46] . W. Cyberattacks threaten global financial stability, IMF warns | World Economic Forum. World Economic Forum. 2024 Retrieved from: https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/?utm_source=chatgpt.com
[47] Zhu C, Liu X, Chen D, & Yue Y. Executive compensation and corporate sustainability: Evidence from ESG ratings. Heliyon. 2024;10(12) https://www.cell.com/heliyon/fulltext/S2405-8440(24)08974-6
[48] Junaedi J. Understanding the role of finance in sustainable development: A qualitative study on environmental, social, and governance (ESG) practices. Golden Ratio of Finance Management. 2024;4(2):113-130 https://doi.org/10.52970/grfm.v4i2.422
[49] Nogueira E, Gomes S, & Lopes JM. Financial Sustainability: Exploring the Influence of the Triple Bottom Line Economic Dimension on Firm Performance. Sustainability (2071-1050). 2024;16(15). Doi: https://doi.org/10.3390/su16156458
[50] Khalid F, Su C-Y, Weiwei K, Voinea CL, & Srivastava M. Financial mechanism for sustainability: the case of China's green financial system and corporate green investment. China Finance Review International. 2025;15(1):93-116 https://doi.org/10.1108/CFRI-11-2023-0291
[51] Ezeji CL. Emerging technologies and cyber-crime: strategies for mitigating cyber-crime and misinformation on social media and cyber systems. International Journal of Business Ecosystem & Strategy (2687-2293). 2024;6(4):271-284 https://doi.org/10.36096/ijbes.v6i4.635
[52] Ngunjiri N. Technological Developments And Innovations Influence Cybercrime Rise In Juja Sub-County. National Security . 2024 Retrieved from: https://www.researchgate.net/publication/38551698
[53] Admass WS, Munaye YY, & Diro AA. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications. 2024;2:100031 https://doi.org/10.1016/j.csa.2023.100031
[54] UNDP. Technology to assess disaster damage | United Nations Development Programme. United Nations Disaster Prevention. 2018.Retrieved from: https://www.undp.org/stories/technology-assess-disaster-damage?utm_source=chatgpt.com
[55] IBM. What Are Smart Contracts on Blockchain? | IBM. 2024 [Retrieved from: https://www.ibm.com/think/topics/smart-contracts?utm_source=chatgpt.com
[56] Kuzior A, Tiutiunyk I, Zielińska A, & Kelemen R. Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies (2071-8330). 2024;17(2) https://www.ceeol.com/search/article-detail?id=1273929
[57] Government. U. Strengthen your cybersecurity | U.S. Small Business Administration. . 2024.Retrieved from: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity?utm_source=chatgpt.com
[58] Fitri RD, Hilman M, & Yazid S. Improving password policy strategies: a government employee perspective. Information & Computer Security. 2025 https://doi.org/10.1108/ICS-12-2024-0335
[59] Seethaler RK, & Rose G. Six principles of persuasion to promote community-based travel behavior change. Transportation research record. 2006;1956(1):42-51 https://doi.org/10.1177/0361198106195600106
[60] CISA. Cybersecurity Best Practices | Cybersecurity And Infrastructure Security Agency Cisa (National Coordinator For Critical Infrastructure Security And Resilience, Trans.). 2024.Retrieved from: https://www.cisa.gov/topics/cybersecurity-best-practices?utm_source=chatgpt.com
[61] Viard P, & Gaultier, V . . Cyber regulatory landscape: challenges and prospects - RiskInsight. The Cybersecurity & Digital Trust Blog by Wavestone's Consultants. 2024 Retrieved from: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/cyber-insurance/?utm_source=chatgpt.com
[62] Mendoza MÁ. Challenges and implications of cybersecurity legislation. Welivesecurity. 2017.Retrieved from: https://www.welivesecurity.com/2017/03/13/challenges-implications-cybersecurity-legislation/?utm_source=chatgpt.com
[63] khalili J. CrowdStrike Faces a Potential Tsunami of Lawsuits. Only the Fine Print Can Save It, Experts Say 2024.Retrieved from: https://www.wired.com/story/crowdstrike-outage-microsoft-delta-lawsuits-analysis/?utm_source=chatgpt.com
[64] Goswami NG, Sampathila N, Bairy GM, Chadaga K, Goswami A, & Belurkar S. Digital Pathology in Healthcare: Current Trends and Future Perspective. International Journal of Online & Biomedical Engineering. 2024;20(9)
[65] Franco MF, Mullick AR, & Jha S. QBER: Quantifying Cyber Risks for Strategic Decisions. arXiv preprint arXiv:2405.03513. 2024 https://doi.org/10.48550/arXiv.2405.03513
[66] Naidu TS. "EMERGING TRENDS IN CYBERCRIME: CHALLENGES AND COUNTERMEASURES IN INDIA." ResearchGate.; 2024 Retrieved from: https://www.researchgate.net/publication
[67] Rajasekharaiah K, Dule CS, & Sudarshan E, editors. Cyber security challenges and its emerging trends on latest technologies. IOP conference series: materials science and engineering; 2020: IOP Publishing.http://doi.org/10.1088/1757-899X/981/2/022062
[68] Cotrina L, León P, Reyes C, Arbulú Ballesteros M, Guzmán M, Castillo J, Acosta R, & Morales A. Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches. Journal of

Educational and Social Research. 2024;14(5):96 https://doi.org/10.36941/JESR-2024-0124
[69] Bruce M, Lusthaus J, Kashyap R, Phair N, & Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index. Plos one. 2024;19(4):e0297312 https://doi.org/10.1371/journal.pone.0297312
[70] Landoll D. The security risk assessment handbook: A complete guide for performing security risk assessments: CRC press; 2021. https://doi.org/10.1201/9781003090441
[71] Swanagan M. How To Plan & Develop An Effective Cybersecurity Strategy 2024.Retrieved from: . https://purplesec.us/learn/cybersecurity-strategy/?utm_source=chatgpt.com
[72] Mugwagwa A, Bhero E, & Chibaya C. Cybersecurity strategy: Future proof cybersecurity for small to medium enterprises in South Africa. International Journal of Research in Business and Social Science. 2024;13(4):15-24. Doi: https://doi.org/10.20525/ijrbs.vl3i4.3308
[73] Chidukwani A, Zander S, & Koutsakis P. A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEe Access. 2022;10:85701-85719 https://doi.org/10.1109/ACCESS.2022.3197899
[74] Kaur P, Alam A, Kaur S, & Sahota RS. Access Control Application Prevention and Mitigation of Cyber Attacks. International Journal of Research and Innovation in Applied Science. 2023;8(10):91-105 http://dx.doi.org/10.51584/IJRIAS.2023.81011
[75] Boyer M, & Eling M. New advances on cyber risk and cyber insurance. The Geneva Papers on Risk and Insurance-Issues and Practice. 2023;48(2):267-274 https://doi.org/10.1057/s41288-023-00294-w
[76] Taskin N, Özkeleş Yıldırım A, Ercan HD, Wynn M, & Metin B. Cyber insurance adoption and digitalisation in small and medium-sized enterprises. Information. 2025;16(1):66 https://doi.org/10.3390/info16010066
[77] Dr D. Divya, & Devarajan S. Enhancing Cyber Security in the Insurance Sector: An Empirical Analysis of 30 Companies. Conference: Cyber Threats - New Challenges for InsuranceAt. . 2024 https://www.researchgate.net/publication/382446499
[78] Goldsby EH. Emerging Technology Trends in Workers' Compensation | Enlyte. Enlyte. 2024 https://www.enlyte.com/insights/workers-comp/article/workers-comp-technology-trends?utm_source=chatgpt.com
[79] Tsohou A, Diamantopoulou V, Gritzalis S, & Lambrinoudakis C. Cyber insurance: state of the art, trends and future directions. International Journal of Information Security. 2023;22(3):737-748 https://doi.org/10.1007/s10207-023-00660-8