International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-7| 2023 Published: |22-07-2023|

"THE ROLE OF INSURANCE COMPANIES IN COMPENSATING CYBERCRIME VICTIMS"

https://doi.org/10.5281/zenodo.8223569

Boboqulov Azizbek Zoxid o'g'li
Huquqni muhofaza qilish akademiyasi magistri

Abstract

This article discusses the increasing importance of insurance companies in compensating victims of cybercrime. With the rise of digital age, cybercrime has become a significant issue and its cost is projected to exceed $8 trillion annually by 2023. The article also outlines some common types of cybercrime, including hacking, phishing, ransomware, and data breaches. Finally, the article explains various types of insurance policies available for individuals and organizations to protect themselves against the financial consequences of cybercrime, such as Cyber Liability Insurance, which provides coverage for data breaches, hacking and phishing attacks, and can cover the costs associated with responding to a cyber-attack.

Аннотация

В данной статье рассматривается возрастающая роль страховых компаний в возмещении ущерба жертвам киберпреступлений. С наступлением эпохи цифровых технологий киберпреступность стала серьезной проблемой, и, по прогнозам, к 2023 году ее стоимость превысит 8 триллионов долларов в год. В статье также описаны некоторые распространенные виды киберпреступлений, включая взлом, фишинг, программы-вымогатели и утечку данных. Наконец, в статье объясняются различные типы страховых полисов, доступных для частных лиц и организаций, чтобы защитить себя от финансовых последствий киберпреступлений, таких как страхование кибер-ответственности, которое обеспечивает покрытие утечек данных, хакерских и фишинговых атак и может покрывать расходы, связанные с кибератаками.

Annotatsiya

Ushbu maqolada kiberjinoyatlar qurbonlariga tovon to'lashda sug'urta kompaniyalarining ortib borayotgan roli muhokama qilinadi. Raqamli asrning kirib kelishi bilan kiberjinoyatlar o'ta muhim muammoga aylandi va ushbu jinoyatlar oqibatida yetkazilishi mumkin bo'lgan zarar 2023-yilga borib yiliga 8 trillion dollardan oshishi aytilgan. Maqolada, shuningdek, kiberjinoyatlarning ba'zi keng tarqalgan turlari, jumladan, hakerlik, fishing, tovlamachi dasturlar va ma'lumotlar tarqatish kabilar ko'rsatilgan. Nihoyat, maqolada jismoniy shaxslar va tashkilotlar uchun

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-7| 2023 Published: |22-07-2023|

kiberjinoyatlarning moliyaviy oqibatlaridan o'zlarini himoya qilish uchun mavjud bo'lgan sug'urta turlari tushuntiriladi. Masalan, ma'lumotlarning tarqatish, hakerlik va fishing hujumlari oqibatida yetkazilgan zararlar hamda bu bilan bog'liq boshqa harajatlarni Kiber-javobgarlik sug'urtasi vositasida qoplash masalalariga to'xtalib o'tiladi.

Keywords

Cybercrime, Insurance companies, compensation, financial losses, hacking, phishing, cyber fraud, identity theft, cyber-attack, general liability insurance, third-party coverage, lawsuits, cyber insurance.

Ключевые слова

Киберпреступление, страховые компании, компенсация, финансовые потери, хакерство, фишинг, кибермошенничество, кража личных данных, кибератака, страхование гражданской ответственности, покрытие ответственности перед третьими лицами, судебные иски, киберстрахование.

Калит сўзлар

Кибержиноят, суғурта компаниялари, компенсация, молиявий йўқотишлар, хакерлик, фишинг, киберфирибгарлик, шахсга доир маълумотларни ўғирлаш, киберҳужум, фуқаролик жавобгарлигини суғурта қилиш, учинчи шахслар олдидаги жавобгарликни қоплаш, даъволар, киберсуғурта.

Introduction

Cybercrime, also known as computer crime, refers to any illegal activity that involves the use of the internet or any other form of computer technology[161]. This can range from hacking and phishing to cyber fraud and identity theft. The rise of the digital age has resulted in a significant increase in cybercrime, with more individuals and organizations becoming victims every day.

Importance of Insurance Companies in compensating Cybercrime Victims

Insurance companies play a critical role in compensating victims of cybercrime. With the increasing frequency and sophistication of cyber attacks, insurance coverage has become a crucial way to protect against the financial losses and other damages that can result from these crimes. Insurance companies provide financial support to victims, as well as expertise in handling cybercrime cases and speed of response, which can be crucial in mitigating the harm caused by these crimes.

According to a report by Cybersecurity Ventures, cybercrime costs are projected to exceed $8 trillion annually by 2023, up from $5 trillion in 2015[162]. This

[161]Cybercrime. In Wikipedia. Retrieved February 1, 2023, from https://en.wikipedia.org/wiki/Cybercrime
[162]Cybersecurity Ventures. Cybercrime Report 2023. Retrieved February 1, 2023, from https://cybersecurityventures.com/stats/

highlights the growing importance of insurance companies in compensating cybercrime victims, as the cost of these crimes continues to escalate.

Types of Cybercrime

Cybercrime refers to illegal activities that are committed using the internet or other forms of computer networks. The following are some of the most common types of cybercrime:

Hacking

Hacking refers to unauthorized access to a computer system or network with the intent to cause harm or steal sensitive information. Hackers can use various techniques, including exploiting vulnerabilities in software or using malicious code, to gain access to a system.

Phishing

Phishing is a form of social engineering that involves tricking individuals into revealing sensitive information, such as passwords or credit card numbers[163]. This is typically done through the use of fake emails or websites that appear to be from a legitimate source, such as a bank or online retailer.

Ransomware

Ransomware is a type of malicious software that encrypts a victim's files and demands payment in exchange for the decryption key[164]. This type of attack can result in significant financial losses and downtime for the victim, as they may be unable to access important data or systems until the ransom is paid.

Data breaches

A data breach refers to the unauthorized access, use, or disclosure of sensitive information, such as financial data or personal information[165]. This can be the result of a number of factors, including hacking, phishing, or poor security practices within an organization.

Insurance Coverage for Cybercrime Victims

One way for individuals and organizations to protect themselves against the financial consequences of cybercrime is through insurance coverage. There are various types of insurance policies available that offer protection against cyber threats, including:

Cyber Liability Insurance

[163] What is Phishing?. Federal Trade Commission. Retrieved February 2, 2023, from https://www.consumer.ftc.gov/articles/0003-phishing

[164] Understanding Ransomware. US-CERT. Retrieved February 2, 2023, from https://www.us-cert.gov/ncas/tips/ST04-014

[165] Data Breaches: What You Need to Know. Federal Trade Commission. Retrieved February 2, 2023, from https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-7| 2023 Published: |22-07-2023|

Cyber liability insurance provides coverage for a range of cyber threats, such as data breaches, hacking, and phishing attacks[166]. This type of insurance can help cover the costs associated with responding to a cyber attack, such as hiring a forensic investigator, providing credit monitoring services to affected customers, and covering legal fees[167]. In addition, cyber liability insurance can also provide protection against the costs associated with repairing or replacing damaged hardware or software and lost or stolen data[168].

Organizations that handle sensitive information, such as personal data or financial information, are particularly vulnerable to cyber attacks and may benefit from cyber liability insurance. For example, a data breach could result in significant financial losses, including the cost of notifying affected customers, offering credit monitoring services, and paying legal fees to defend against any potential lawsuits. Cyber liability insurance can help cover these costs, providing organizations with a financial safety net in the event of a cyber attack.

First-party Coverage

First-party coverage refers to insurance that provides protection for the policyholder[169]. This type of coverage can include reimbursement for losses, such as the cost of restoring damaged data or equipment, or for income lost as a result of a cyber attack[170]. First-party coverage can also provide access to crisis management and communication services, which can be crucial in the aftermath of a cyber attack[171].

For example, a small business that relies on its website for sales could suffer significant losses if its website were to be taken down by a cyber attack. First-party coverage could help cover the costs of repairing the website and lost income during the downtime. In addition, first-party coverage can also provide access to crisis management services, which can help the business quickly and effectively respond to the attack and minimize the potential damage.

Third-party Coverage Third-party coverage refers to insurance that provides protection for those who are not the policyholder, such as customers or business

[166] Marsh. What is Cyber Liability Insurance? Retrieved February 5, 2023, from https://www.marshcommercial.co.uk/for-business/cyber-risks.
[167] Travelers. Cyber Liability Insurance. Retrieved February 5, 2023, from https://www.travelers.com/cyber-insurance
[168] Beazley. What is Cyber Liability Insurance? Retrieved February 5, 2023, from https://www.beazley.com/en-ca/products/cyber-tech-canada-english/bbr-cyber-breach-solution
[169] Chubb. What is Cyber Insurance? Retrieved February 4, 2023, from https://www.chubb.com/us-en/business-insurance/privacy-network-security
[170] AIG. What is Cyber Insurance? Retrieved February 5, 2023, from https://www.aig.com/business/insurance/cyber
[171] Beazley. What is Cyber Liability Insurance? Retrieved February 5, 2023, from https://www.beazley.com/en-ca/products/cyber-tech-canada-english/bbr-cyber-breach-solution

partners[172]. This type of coverage can provide protection against claims related to data breaches, such as claims for unauthorized access to sensitive information or for violations of privacy laws[173]. Third-party coverage can also provide protection against liability for damages related to intellectual property infringement or cyber extortion[174].

For example, a retailer that experiences a data breach could be liable for damages suffered by its customers as a result of the breach. Third-party coverage could help cover the costs of defending against any claims from affected customers and paying any settlements or awards. This type of coverage can be especially important for organizations that handle sensitive information, as it can help protect against the financial consequences of a data breach.

In conclusion, insurance companies play a crucial role in compensating cybercrime victims by providing various types of coverage, such as cyber liability insurance, first-party coverage, and third-party coverage. By providing financial protection against the costs associated with responding to a cyber attack, insurance companies help organizations and individuals minimize the potential damage and protect themselves against the financial consequences of cybercrime.

Challenges faced by Insurance Companies in compensating Cybercrime Victims

Lack of Awareness: Insurance companies may face challenges compensating cybercrime victims due to a lack of awareness about the issue. According to a study by Accenture[175], "54% of organizations do not have a cyber insurance policy, with many stating that they are simply not aware of the coverage available or the potential risks they face." The lack of awareness about the availability of cyber insurance and the risks posed by cybercrime can make it difficult for insurance companies to effectively compensate victims and protect against losses.

Complexity of Cybercrime: Cybercrime can be highly complex and difficult to understand, even for those in the cybersecurity industry. According to Beazley[176], "cyberattacks are becoming increasingly sophisticated and often involve multiple stages, making it difficult for organizations to detect and respond to them

[172] Chubb. What is Cyber Insurance? Retrieved February 6, 2023, from https://www.chubb.com/us-en/business-insurance/privacy-network-security
[173] Beazley. What is Cyber Liability Insurance? Retrieved February 6, 2023, from https://www.beazley.com/en-ca/products/cyber-tech-canada-english/bbr-cyber-breach-solution
[174] AIG. What is Cyber Insurance? Retrieved February 6, 2023, from https://www.aig.com/business/insurance/cyber
[175] Accenture. Many Organizations Remain Uninsured for Cyber Risks. Retrieved February 7, 2023, from https://newsroom.accenture.com/news/more-than-half-of-organizations-not-effectively-defending-against-cyber-attacks-according-to-accenture-study.htm
[176] Beazley. Beazley Breach Response (BBR) Services. Retrieved February 7, 2023, from https://www.beazley.com/en-gb/products/cyber-tech-united-kingdom/bbr-cyber-breach-solution

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-7| 2023 Published: |22-07-2023|

effectively." This complexity can pose significant challenges for insurance companies in compensating cybercrime victims, as they must have a deep understanding of the technical aspects of cybercrime in order to accurately assess and respond to claims.

Limited Coverage: Insurance companies may also face challenges compensating cybercrime victims due to limited coverage offered by some insurance policies. According to AIG[177], "some insurance policies may not cover all types of cyber risks or may have exclusions for specific types of losses." This can make it difficult for insurance companies to provide adequate protection against the financial consequences of cybercrime, as they may not be able to fully compensate victims for their losses.

No legal regulations in Uzbekistan: In countries like Uzbekistan where there may not be a legal framework in place to regulate the cyber insurance industry, insurance companies may face difficulties compensating cybercrime victims. Without clear regulations, insurance companies may struggle to accurately assess and respond to claims, leading to disputes and difficulties in compensating victims.

In conclusion, insurance coverage for cybercrime victims plays an important role in providing financial protection against the costs associated with responding to a cyber attack. Insurance companies can offer various types of coverage, including cyber liability insurance, first-party coverage, and third-party coverage, to help organizations and individuals minimize the potential damage and protect themselves against the financial consequences of cybercrime. Despite the challenges faced by insurance companies, such as lack of awareness, complexity of cybercrime, limited coverage, and absence of legal regulations in some countries, the future outlook for insurance companies in compensating cybercrime victims is positive. As the frequency and sophistication of cyber attacks continue to increase, the demand for insurance coverage for cybercrime victims is likely to grow, providing insurance companies with a significant opportunity to expand their business and help protect against the financial consequences of cybercrime.

REFERENCES:

1. Cybercrime. In Wikipedia. https://en.wikipedia.org/wiki/Cybercrime
2. Cybersecurity Ventures. Cybercrime Report 2023. Retrieved February 1, 2023, from https://cybersecurityventures.com/stats/

[177] AIG. Cyber Insurance. Retrieved February 7, 2023, from https://www.aig.com/business/insurance/cyber)

3. What is Phishing? Federal Trade Commission. from https://www.consumer.ftc.gov/articles/0003-phishing

4. Understanding Ransomware. US-CERT. https://www.us-cert.gov/ncas/tips/ST04-014

5. Data Breaches: What You Need to Know. Federal Trade Commission. Retrieved February 2, 2023, from https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

6. Marsh. What is Cyber Liability Insurance? Retrieved February 5, 2023, from https://www.marshcommercial.co.uk/for-business/cyber-risks.

7. Travelers. Cyber Liability Insurance. Retrieved February 5, 2023, from https://www.travelers.com/cyber-insurance

8. Beazley. What is Cyber Liability Insurance? Retrieved February 5, 2023, from https://www.beazley.com/en-ca/products/cyber-tech-canada-english/bbr-cyber-breach-solution

9. Chubb. What is Cyber Insurance? Retrieved February 4, 2023, from https://www.chubb.com/us-en/business-insurance/privacy-network-security

10. AIG. What is Cyber Insurance? Retrieved February 6, 2023, from https://www.aig.com/business/insurance/cyber

11. Accenture. Many Organizations Remain Uninsured for Cyber Risks. Retrieved February 7, 2023, from https://newsroom.accenture.com/news/more-than-half-of-organizations-not-effectively-defending-against-cyber-attacks-according-to-accenture-study.htm