Anhelina BelavezhaThe Impact of Cyber Security on Business: Jagiellonian University,

How to Protect Your Business Computer Science

The Impact of Cyber Security on Business: How to Protect Your Business

# Introduction

Imagine waking up tomorrow to find that your company's entire database has been compromised. Confidential client information, financial records, and sensitive emails — all stolen or corrupted. How prepared do you think your business is to handle such a cyber attack? Are your current security measures enough to protect against this growing threat?

# What is Cyberspace?

In this section, we explore the concept of "cyberspace," a term coined by science fiction author William Gibson in his 1982 novel "Burning Chrome" and popularized in his 1984 novel "Neuromancer."

1. *Definition:*

* Refers to the global digital universe encompassing all computer networks.
* Commonly known as the Internet.

1. *Activities in Cyberspace:*

* Includes online banking, communication, and data transfer.
* Covers both simple tasks (e.g., email, browsing) and complex fields (e.g., AI, cyber forensics).

1. *Technological Scope:*

* Defined by the use of electronics and the electromagnetic spectrum to store, modify, and transmit information.
* Obraz zawierający tekst, trójkąt, Czcionka, design

  Opis wygenerowany automatycznieEncompasses data networks, software systems, and human-computer interactions.

1. *Vulnerability and Dependency:*

* Increasing reliance on digital systems makes businesses and critical infrastructure vulnerable to cyber threats.
* Sectors like finance, healthcare, and utilities are common targets of cyberattacks.

1. *Network Security and the CIA Triad:*

* Confidentiality: Limiting access to information to authorized users; use of encryption techniques.
* Integrity: Ensuring data is not altered by unauthorized users; maintaining data accuracy.
* Availability: Ensuring network and data accessibility; regular updates and failover strategies to handle failures and attacks.

1. *Impacts of Cyber Threats:*

* Financial Costs: High expenses for legal fees, damages, and compliance with security standards.
* Reputational Damage: Breaches can erode customer trust and negatively impact stock value.

# Information Security Governance and Cyber Security

* *Governance:*
* Maintaining an effective corporate structure with clear vision, mission, transparency, equity, accountability, and corporate responsibility.
* *Information Security:*
* Key aspects: Confidentiality, Integrity, Availability (CIA).
* *ISG (Information Security Governance):*
* Combines corporate governance with information security.
* Emphasizes the importance of accountability and auditing in managing cyber threats.
* *Cyber Threats and Their Consequences:*
* Types: Cyberattacks, data breaches, hacking, identity theft, ransomware, phishing.
* Impacts: Financial loss, reputational damage, intellectual property loss, operational disruption, legal consequences, national security risks, psychological impacts.
* *Common Cyber Threats:*
* Malware: Injects malicious software to damage or steal information.
* Phishing: Deceptive practices to obtain confidential information.
* Ransomware: Encrypts data, demanding ransom for decryption.
* *Impact of Cyber Attacks:*
* Financial losses, operational stoppage, changes in practices, legal liabilities, reputational damage, compromised intellectual property.
* *Recommendations:*
* Governments and IT staff should raise awareness about cyber risks and support e-businesses with proactive security measures and advice.

# Conclusion

Cybercrime remains a widespread issue globally. Despite efforts to combat it, why does it continue to pose significant challenges for countries worldwide?

Researchers are implementing various defenses. What are the key obstacles that allow cybercrime to thrive in societies with inadequate laws or enforcement?

Enforcing laws and holding cybercriminals accountable could build trust in e-commerce and the internet. How can these measures be effectively implemented to mitigate cyber threats?

Are we nearing effective solutions to combat cybercrime, or are there still significant hurdles to overcome in securing our digital future?

# References

#### **Open Journal of Safety Science and Technology (June 30, 2023),** Emiles Mbungu Kala, The Impact of Cyber Security on Business:How to Protect Your Business (pages 51 – 65)