Emro Science and Education
International open-access scientific journal
Journal homepage: https://journal.emro.uz
OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 2 (2024) · “Raqamli iqtisodiyot sharoitida moliyaning dolzarb muammolari, yechimlari va istiq... DOI: 10.5281/zenodo.24317010

Bulutli xarajatlar haqida gap ketganda, ular, albatta, tushib ketmoqda, bu bozordagi jiddiy raqobat va bir qator provayderlar vaziyatni tartibga solmasdan va hukmronlik zanjiri paydo bo'lishidan oldin eng katta ulushni ta'minlash uchun bir-biri bilan kurashayotganligi sababli. tashkil etilgan.

Yakuniy foydalanuvchilar uchun bu bulutli xosting xarajatlari, ayniqsa o'tmishda talab qilinishi mumkin bo'lgan ichki muqobil echimlar bilan solishtirganda, pasayishda davom etishini anglatadi.

Bulutda ko'plab boshqa xosting formatlari uchun jismoniy cheklovlar yo'qligi sababli, u keyingi bir necha yil ichida korporativ hosting uchun de-fakto standartga aylanishi kerak.

Bulutli serverlar tejamkor, bardoshli, boshqarish oson va oldindan mavjud bo'lgan har qanday yechimga qaraganda ancha kengaytirilishi mumkin. Naysaylar har doim ovozli ozchilik sifatida mavjud bo'ladi, ammo dalillar shuni ko'rsatadiki, bulut bilan haqiqatan ham shug'ullanganlar uni rad etishga tayyor.

**Foydalanilgan adabiyotlar ro’yhati:**

1. https://www.ibm.com/topics/mainframe
2. https://intellipaat.com
3. https://www.lawinsider.com

## CYBER SECURITY IN BUSINESS ORGANIZATIONS

**Parpiyev G‘afurjon G‘ayratovich**
Andijan machine-building institute, doctorant,
**Tojiboyev Abdumo‘min Muxtorjon o‘g‘li**
Andijan machine-building institute, student,
kuyganyor@gmail.com

**Annotatsiya:** Ushbu maqolamizda texnologik o'sishda zamonaviy dunyoda tashkilotlarni boshqarishda qiyinchiliklar tug'diradigan ba'zi jinoyatlarga va ularni oldini olish haqida fikr bildiriladi.

**Аннотация:** В этой статье мы обсудим некоторые преступления, которые затрудняют управление организациями в современном мире с технологическим ростом, и способы их предотвращения.

**Annotation:** In this article, we will discuss some of the crimes that make it difficult to manage organizations in the modern world with technological growth and how to prevent them.

### Introduction

Technological growth has led to some crimes, which pose challenges to managing organizations in the modern world. The most dangerous crime associated with



Published: 28.03.2024

**Cite this article:** Parpiyev G‘afurjon G‘ayratovich, Tojiboyev Abdumo‘min Muxtorjon o‘g‘li (2024). Cyber security in business organizations. Emro Science and Education, 1(2). https://doi.org/10.5281/zenodo.24317010

*© 2024 The Author(s). Published by Emro Science and Education. This is an open access article.*

technology is the emergence of hackers, who steal organizations’ information for financial benefits. Hacking has been a threat to organizational growth, thus resulting in huge financial losses (Erickson, 2008).

This paper will highlight the challenges that organizations face in protecting the customers and assets, the red flags that the Target Company ignored, and the actions employed after the hacking thievery coupled with discussing the main reasons that made the breach successful with reference to the article, “Missed Alarms and 40 million Stolen Credit Card Numbers: How Target Blew it”.

**Challenges organizations face in protecting organizational assets and information**

The most historic hacking happened in Target and it culminated in huge financial losses. For instance, customers for Target demanded compensation for the losses incurred by the organization, which cost about $ 61 million (Riley, Lawrence, Elgin & Matlack, 2014). Therefore, today’s business organizations face serious challenges that limit their financial growth. The following are the challenges that modern business organizations face in protecting their assets and information.

**Information Resilience**

Modern organizations encounter several challenges in protecting and sustaining critical information concerning their assets. The pathway through which the organizational information is processed, organized, stored, and deleted should be contained secretly (Myatt, 2013). The organizational risk management team ensures that the critical information assets that are used to drive the companies’ success are highly protected and contained within the risk management framework.

The data may be contract information or data related to an organization’s financial performance. However, organizations face the challenge of maintaining and controlling this vital information due to irresponsible and unethical employees (Middo, 2013). For instance, employees who may retire or undergo retrenchment may decide to spill out an organization’s important information. This aspect may lead to the damaging of the organizational public image. Moreover, the information can be used by hackers to trace information of their interest.

For example, the investigations on Target hacking incidence revealed that the arrested irresponsible IT employee may have given out the company’s information (Riley et al., 2014). Similarly, this scenario happens if the former employer has the full grasp of the company’s operational systems. Ultimately, the revealed information leads to financial losses through hacking.

In addition, the destroyed company’s public image may lead to reduced customer trust, if the spilled information has negative effects on the products or services offered by the company (Middo, 2013). The resulting effects will have an impact on the consumer behavior whereby the company sales will reduce significantly, hence low demand, thus leading to poor performance.

**Increased operation costs**

Due to the high technological development, the growing number of hackers increases organizational responsibility and efforts towards safe data and information keeping. Therefore, organizations hire or establish their own security data-management team or systems to protect information assets (Myatt, 2013). This move comes with increased financial costs on top of the normal operational costs.

The costs incurred may be through setting highly detective systems or hiring a specialized data security agency to monitor and respond to hackers at an early stage. For instance, Target established a data security system, which cost them a lump sum of cash (Riley et al., 2014). This extra cost could have been used to increase productivity. Target had installed a malware detection system at a cost of $1.6 billion.

**Highly informational economy**

Currently, the business sector relies on processed and stored information data that appears on organizational profiles, social media platforms, and company websites where it is mainly used for marketing purposes. This aspect exposes some of the information that organizations use in their daily routine for increased productivity. For instance, the modern economy depends on virtual information records, whish are based on their websites.

In fact, almost all business entities use virtual customer records, virtual product specification, virtual stock markets, virtual offices, and social media chatting systems. Apparently, these platforms are the main exposure avenues to the hackers. In addition, in case of a successful hacking thievery, organizations incur huge financial losses to compensate their customers and reform their organizational structure and design. Target is a good example of the costs incurred to compensate its customers on losses and restructuring its IT data systems (Riley et al., 2014).

**The red flags that Target overlooked**

On November 30, Fire Eye Security, which is firm in the computer systems security, detected the hackers’ malware on behalf of the Target data security. Immediately, the Bangalore-based Minneapolis computer specialist team, viz. the Target security management team, was alerted (Riley et al., 2014).

In addition, in December the same year, another software malware was sent by the hackers, but the Bangalore team had switched off its detection and monitoring software. The hackers had professionally structured their operation such that they used the same Target computer system by cloaking codes to ensure safety. The Target’s computer specialist team ignored the alarms sent by the Fire Eye security systems after the first detection.

Moreover, the Target management team ignored the attention of the irresponsible IT specialized employee, who was arrested from their office (Riley et al., 2014). Something was amiss, and thus that risk reduction, mitigation, and avoidance measures needed to be put in place. Nevertheless, no response was witnessed from the Target

Security system to thwart the hacking efforts. Ultimately, the ignored security alarms culminated in great financial loss to Target,

**Response Actions after the Hacking thievery in Target**

After suffering great data and information loss, Target decided to restructure the entire organizational structure. On his response following the breach incidence, Gregg Steinhafel, the Targets’ Executive officer, said that the organization was restructuring the employees, the processes, and the entire technological systems in order to tighten the security level. Moreover, the executive officer reported that the organization was scrutinizing the information systems to rectify and establish new systems.

Moreover, Gregg indicated that the company had already set up a customer response strategy (Riley et al., 2014). This move aimed at restoring the lost customer trust and above all maintaining the productivity level. In addition, customers were not to pay for any fraud charges arising from the information breach incidence. Ultimately, the breach of information incidence led to serious investigations by the Fire Eye Security systems to establish the entry and pathway of the hackers. The results revealed that the highly specialized hackers had mimic software to that of Target to conceal the thievery.

**Reasons that led to Target thievery**

After thorough investigations by the Fire Eye in 2008, the results revealed several pit holes in the Target, which include

**Targets’ Management ignorance**

The security specialist in Minneapolis ignored the alarms sent by the Fire Eye computer specialists. According to the Fire Eyes report, if the company had taken a quick response, such damages would have not occurred. Moreover, the company did not consider keeping secretive information about customer payments, contracts, and billings. Furthermore, the vendor that the company worked with revealed some crucial information that may have led to the hacking incidence.

**Lost trust on Fire Eyes’ report**

Target computer security specialists had switched off the system that would have automatically deleted any detected hacking malware (Riley et al., 2014). This system prevents any access to the customers’ and organizational vital information. This aspect culminated in easy access to the company’s credit cards. In addition, the Target’s computer security team had lost trust on Fire Eye organization. This aspect led to ignorance on any findings that the Fire Eye presented to them.

**Poorly designed organizational structure system**

According to report after the hacking thievery by Fire Eye, the IT infrastructure was poorly designed. For instance, the entire Targets’ anti-hacking system had only locked doors without CCTV screen surveillance of the operations. This aspect led to the loss of organizational data through manual and visual scanning. Moreover, the entire security systems had been designed in a poorly planned structure that enabled access to everyone’s information. Furthermore, the Target’s security software systems were

outdated to detect any highly technologized software. All these factors paved way and ease of access to the Target’s customer data and information

**Conclusion**

Hacking has been a threat to the modern businesses and organizations. In addition, hackers go to the extent of tracking personal bank information for financial benefits. Therefore, every organization should establish strict and reliable anti-hacking system. Moreover, every organization should focus on having a reliable and quick communication channel to foster timely response. If only Target had considered all these factors, the breach would have been managed without dire financial consequences.

**References**

1. Middo, M. (2013). *5 Minute Businesses- Growth Hacking Secrets Revealed*. Woollahra, NSW: Longueville Media.
2. Myatt, M. (2013). *Hacking Leadership: The 11 Gaps Every Business Needs to Close and the Secrets to closing them quickly*. Hoboken, NJ: Wiley.
3. Riley, M., Lawrence, D., Elgin, B., & Matlack, C. (2014). *Hack*: *Missed Alarms and 40 million Stolen Credit Cards Numbers: How Target blew it*.
4. Xoldarboyev, R. A., & Abduvaxobova, R. A. Q. (2022). Kiberxavfsizlik. *Science and Education*, *3(7), 29-34*
5. StudyCorgi. (2020, May 10). *Cyber Security in Business Organizations. Retrieved from https://studycorgi.com/cyber-security-in-business-organizations/*

## KICHIK BIZNES IQTISODIY XAVFSIZLIGINI TA’MINLASHDA AXBOROT XAVFSIZLIGINING AHAMIYATI

**Akbarov Abdulhamid Akmal o‘g‘li**

Andijon mashinasozlik instituti tayanch doktoranti,

TDIU Andijon fakulteti katta o‘qituvchisi

**Annotatsiya:** Raqamli dunyoda iqtisodiyotning turli soha va tarmoqlari o‘z faoliyatida zamonaviy axborot-kommunikatsion texnologiyalarni joriy etmoqda. Tadbirkorlik va biznes faoliyatini esa hozirgi kunda axborot texnologiyalarsiz tasavvur etish qiyin. Shu nuqtai nazardan ushbu tezisda kichik biznes faoliyatini raqamlashtirish ahamiyati hamda bunda axborot xavfsizligi masalasi tahlil etilgan.