**Ministry of Education and Science of UkraineUkrainian-American Concordia University**

Faculty of Management and Business
*Department of International Economic Relations, Business & Management*

# Bachelor's Qualification Work

**Management of information security of the company** (based on Business Media Network case)

Bachelor student of the 4th year of study
Field of Study 07 – Management
and Administration
Specialty 073 – Management
Educ. program – IT Management

**Volodymyr Brustinov**

Research supervisor

**Ruslana Seleznova**
Ph.D. in Engineering Science

Kyiv – 2024

## Abstract

Topic – Management of Information Security of The Company(based on the “Business Media Network” case)

The work investigates the implementation of information security management practices within a corporate environment. By focusing on Business Media Network (BMN) as a case study, the research delves into the theoretical foundations of information security and analyzes how BMN approaches data security within its operations. The study utilizes a comprehensive research approach to examine BMN's current practices in areas such as human resource management, marketing, and logistics, all from the perspective of information security. By identifying both challenges and opportunities, the research proposes concrete recommendations for enhancing BMN's information security posture. This work contributes to the field of information security management by providing practical insights into implementing robust data security measures within a specific business context.

**Keywords:** Information Security Management, Data Security, Business Media Network (BMN), Case Study, Human Resource Management, Marketing, Logistics

## Анотація

Робота досліджує впровадження практик управління інформаційною безпекою в корпоративному середовищі. Зосереджуючись на медійному бізнесі Business Media Network (BMN), дослідження глибоко занурюється в теоретичні засади інформаційної безпеки та аналізує, як BMN підходить до захисту даних у своїй діяльності. Дослідження використовує комплексний підхід до дослідження поточних практик BMN у таких галузях, як управління людськими ресурсами, маркетинг та логістика, усе з точки зору інформаційної безпеки. Ідентифікуючи як виклики, так і можливості, дослідження пропонує конкретні рекомендації для посилення позиції інформаційної безпеки у BMN. Ця робота вносить свій вклад у галузь управління інформаційною безпекою, надаючи практичні уявлення про впровадження надійних заходів інформаційної безпеки в конкретному бізнес-контексті.

**Ключові слова:** Управління Інформаційною Безпекою, Захист Даних, Бізнес Медіа Мережа (BMN), Управління Людськими Ресурсами, Маркетинг, Логістика.

**PHEE-institute «Ukrainian-American Concordia University»**

**Faculty of Management and Business**
**Department of International Economic Relations, Business and Management**

Educational level: **Bachelor degree**
Specialty **073 – Management**
Educational program **“Information Technology Management”**

**APPROVED**
**Head of Department** ________________
**__Prof. Zharova L.V.__**_____________ “10” May 2024

# TASK

## FOR BACHELOR’S QUALIFICATION WORK OF STUDENT

______________________________**Volodymyr Brustinov**______________________

(Name, Surname)

1. Topic of the bachelor’s qualification work

Management of Information Security of The Company (based on the Business Media Network case). Supervisor of the bachelor’s qualification work Ruslana Seleznova, Ph.D. in Technical Sciences, Associate Professor at the Department of Information Technologies & Innovations.

(surname, name, degree, academic rank)

Which approved by Order of University from ***“04” September 2023*** № 04-09/2023-5к
2. Deadline for bachelor’s qualification work submission “***25” April 2024.*** 3. Data-out to the bachelor’s qualification work

This study employs a mixed-methods approach, combining qualitative and quantitative research methods, to evaluate information security maturity. It utilizes a tailored information security maturity framework as a foundational structure for assessment. Data collection methods include surveys, interviews, and analysis of secondary data from industry reports and academic literature.
4. Contents of the explanatory note (list of issues to be developed)

To review the concept of information security management and its relevance to modern business practices; to identify key factors determining a company's readiness to implement data democratization, considering its impact on information security; analyze the challenges faced by the company in implementing data democratization, focusing on cultural, technological, and regulatory barriers; and analyze the implementation of data democratization within the Business Media Network (BMN) with a focus on its implications for information security.

5. List of graphic material (with exact indication of any mandatory drawings)

The work includes 3 charts, 2 graphs, and 1 table with the relevant economical and statistical information.

6. Date of issue of the assignment

Time Schedule

| № | The title of the parts of the qualification paper (work) | Deadlines | Notes |
|---|---|---|---|
| 1. | I part of bachelor thesis | *10.12.2023* | On time |
| 2. | II part of bachelor thesis | *27.02.2024* | On time |
| 3. | Introduction, conclusions, summary | *25.04.2024* | On time |
| 4. | Pre-defense of the thesis | *30.04.2024* | On time |

Student

(signature)

Supervisor ______________________ (signature)

Conclusions (*general description of the work; participation in scientific conferences/ prepared scientific article; what grade does the student deserve*):

The student's research paper demonstrates a strong grasp of information security management principles and their practical applications. Chapter one provides a wellorganized analysis of the topic, emphasizing its relevance to modern business environments. The second chapter's empirical study is particularly insightful. By examining data security practices and assessing implementation readiness, the student effectively highlights the challenges and opportunities organizations face in adopting robust information security measures. The Business Media Network case study showcases the student's ability to analyze real-world scenarios and draw practical conclusions. Focusing on access control initiatives and leveraging data analytics to improve security posture exemplifies the practical application of the theoretical concepts explored.

It's also worth mentioning Volodymyr’s notable effort in preparing a scientific article that delves deeper into the implications of information security management within an organizational context. This article not only strengthens the academic merit of the research paper but also contributes significantly to the ongoing discussion on information governance in modern businesses.

Overall, the student is allowed to defend and demonstrates an understanding of information security management. The student deserves a good grade for their efforts

Supervisor_______________________ (signature)

# TABLE OF CONTENTS

# INTRODUCTION

In today's dynamic business environment, the management of information security stands as a critical cornerstone for ensuring operational integrity and safeguarding sensitive data. This dissertation embarks on an intricate exploration of information security practices, focusing specifically on the case study of Business Media Network (BMN). In an era where digital assets and data have become paramount to organizational success, the robustness of information security frameworks is indispensable.

In the ever-evolving landscape of global commerce, the significance of robust information security management cannot be overstated. Particularly within large-scale enterprises operating extensively in digital domains, such as the Business Media Network, ensuring the confidentiality, integrity, and availability of data is paramount. The surge in cyber threats, coupled with stringent regulatory requirements and the profound repercussions of data breaches, underscores the critical need for effective information security management systems (ISMS). This thesis explores the multifaceted approach to managing information security in the context of the Business Media Network, a leading entity in the digital media space, which makes it a pertinent case study for this research.

The purpose of this work is twofold. First, it aims to provide a comprehensive analysis of the current information security strategies employed by Business Media Network, evaluating their effectiveness in safeguarding sensitive data and maintaining uninterrupted business operations. Second, it endeavors to propose enhancements or alternative strategies that could bolster the company’s defenses against the increasingly sophisticated cyber threats. This study not only seeks to contribute academically by detailing an in-depth analysis of applied security measures but also aims to offer practical recommendations that can be implemented by similar organizations to improve their information security postures.

The object of research for this thesis is the information security management framework of Business Media Network. This framework comprises the policies, procedures, and technological controls implemented by the company to protect its information assets. The subject of research delves deeper into the specific strategies and tools employed within this framework, analyzing how they are integrated into the broader corporate structure and day-to-day operations of the company.

To thoroughly investigate the management of information security within Business Media Network, this thesis will undertake several tasks.

The first task will involve a detailed examination of the existing literature on information security management, focusing on established frameworks such as ISO/IEC 27001, which provides a systematic approach to managing sensitive company information, ensuring it remains secure. It will also review recent scholarly articles and industry reports to understand current trends and challenges in information security management.

The second task will assess the specific information security strategies currently in place at Business Media Network. This will include an analysis of the company's use of cybersecurity technologies such as firewalls, encryption protocols, and intrusion detection systems. The effectiveness of these technologies will be evaluated based on recent security incidents reported within the company and how these incidents were managed.

The third task will involve interviews with key stakeholders within Business Media Network, including IT managers, cybersecurity staff, and policy makers. These interviews aim to gain insights into the practical challenges and considerations that influence the company’s information security decisions. This primary data will be critical in understanding the alignment between the company's information security policies and its operational objectives.

The fourth task will examine the training and awareness programs in place at Business Media Network to educate employees about their roles in maintaining information security. The effectiveness of these programs will be critically assessed to determine if they adequately equip employees to handle potential security threats.

The fifth task will explore how regulatory requirements influence information security management at Business Media Network. This will involve an analysis of compliance with relevant laws and regulations, such as the General Data Protection Regulation (GDPR) in the EU, and how these regulations affect the company's security strategies.

The sixth task will focus on identifying any gaps or weaknesses in the current information security management practices at Business Media Network. This will be achieved through a SWOT analysis—identifying strengths, weaknesses, opportunities, and threats related to the company’s information security management.

The seventh task will propose actionable recommendations based on the findings of the previous tasks. These recommendations will aim to enhance the company’s information security framework, addressing any identified gaps and leveraging opportunities to improve security measures.

By undertaking these tasks, this thesis will provide a detailed exploration of the strategies, challenges, and opportunities associated with managing information security in a high-profile digital media company. This research is expected to contribute valuable insights and practical recommendations that can aid similar organizations in strengthening their information security management systems.

Aim of the Bachelor's Qualification Work: The aim of this Bachelor's qualification work is to conduct a comprehensive analysis of BMN's information security management practices within the framework of contemporary business landscapes. The study seeks to understand how BMN navigates the complexities of information security in the digital age and to provide actionable insights and recommendations for enhancing the company's resilience against evolving cyber threats.

The overarching aim of this study is to conduct an in-depth analysis of how BMN, a conglomerate comprising Business Media Network, USU, Mayors club, and EOT, navigates the complexities of information security. As technology advances at an unprecedented pace, so do the challenges and threats associated with safeguarding digital assets. BMN's approach to information security serves as a real-world lens through which we can dissect the multifaceted dimensions of contemporary corporate data protection.

# CHAPTER 1. THEORETICAL FOUNDATIONS

## 1.1. Overview of Business Media Network

Information security serves as a cornerstone of modern business operations, particularly within conglomerates like Business Media Network (BMN), where the protection of sensitive data and digital assets is critical to maintaining operational integrity, safeguarding intellectual property, and preserving trustworthiness among stakeholders. In today's digital age, where information is increasingly digitized, interconnected, and susceptible to cyber threats, the need for robust information security measures has never been more pressing.

Within conglomerates like BMN, which operate across diverse sectors and handle vast amounts of sensitive information, the stakes of inadequate information security practices are exceptionally high. The repercussions of a security breach can extend far beyond financial losses, encompassing reputational damage, legal liabilities, and regulatory non-compliance. Therefore, ensuring the confidentiality, integrity, and availability of information assets is paramount to the long-term viability and success of conglomerates like BMN.

To address these challenges, conglomerates like BMN must adopt a proactive and comprehensive approach to information security, encompassing a range of strategies, frameworks, and best practices. This includes implementing robust access controls to restrict unauthorized access to sensitive information, encrypting data to protect against interception or tampering, and implementing intrusion detection and prevention systems to detect and respond to cyber threats in real-time (Packetlabs Pty Ltd, 2023).

Central to this endeavor is the CIA triad, a foundational framework that delineates three core principles: confidentiality, integrity, and availability. Within conglomerates like Business Media Network (BMN), understanding and implementing the principles of the CIA triad are paramount to ensuring the security and resilience of sensitive data and digital assets.

Just want to address this triad, the CIA stands for: Confidentiality, Integrity and Availability.

To begin with, we can take into consideration the first thing, that is confidentiality. Confidentiality serves as the cornerstone of information security, ensuring that sensitive information is accessible only to authorized individuals or entities. Within BMN, safeguarding the confidentiality of proprietary business data, customer information, and intellectual property is essential to maintaining trust and competitive advantage. To uphold confidentiality, BMN employs a range of measures such as encryption, access controls, and user authentication mechanisms to restrict access to sensitive information and prevent unauthorized disclosure or interception (Cybersecurity FAQs, 2024).

Next, we've got Integrity. Integrity embodies the assurance that information remains accurate, reliable, and trustworthy throughout its lifecycle, free from unauthorized modification or tampering. For BMN, preserving the integrity of critical business data and digital assets is vital to sustaining operational reliability, decision-making accuracy, and regulatory compliance. To maintain integrity, BMN implements robust data validation mechanisms, digital signatures, and version control systems to detect and prevent unauthorized changes or alterations to information (InterviewPrep Career Coach, 2023).

The last one is the Availability, as it ensures that information is accessible and usable when needed by authorized users, without disruption or degradation of service. Within BMN, ensuring the availability of essential business data, applications, and systems is crucial to sustaining productivity, customer satisfaction, and operational resilience. To enhance availability, BMN employs redundancy measures, disaster recovery plans, and robust network infrastructure to mitigate the risk of downtime, data loss, or service interruptions.

The CIA triad provides a comprehensive framework for understanding and implementing effective information security measures within modern business operations, including conglomerates like BMN. By prioritizing the principles of confidentiality, integrity, and availability, BMN can safeguard sensitive information, preserve operational continuity, and uphold the trust and confidence of stakeholders. Through a holistic approach to information security, BMN can mitigate risks, respond to threats, and navigate the complex landscape of cybersecurity with resilience and confidence.

Effective information security practices are underpinned by a set of key principles that guide the design, implementation, and management of security controls within organizations like Business Media Network (BMN). Among these principles are the principle of least privilege and the principle of defense-in-depth, both of which play a pivotal role in mitigating the risk of unauthorized access and exploitation of sensitive information and digital assets (Acronis, 2018).

What is the principle of least privilege? The principle of least privilege dictates that individuals should only be granted access to the resources and information necessary to perform their job functions. Within the context of BMN, adhering to the principle of least privilege ensures that employees, contractors, and other stakeholders are granted access to the minimum level of privileges required to fulfill their responsibilities effectively. By limiting access rights to only those resources and systems essential to job functions, BMN can minimize the risk of unauthorized access, data breaches, and insider threats (InterviewPrep Career Coach, 2023).

Implementing the principle of least privilege involves conducting a thorough assessment of user roles, responsibilities, and access requirements, followed by the implementation of granular access controls based on the principle of least privilege. This may include role-based access control (RBAC) mechanisms, attribute-based access control (ABAC) policies, and least privilege policies that restrict access to sensitive information and critical systems based on predefined criteria such as job roles, organizational hierarchy, and data sensitivity levels (Frontegg, 2024).

As we began with the principle of least privilege, there is another one, that is the principle of defense-in-depth, that advocates for the implementation of multiple layers of security controls to create overlapping defenses that collectively mitigate the risk of unauthorized access or exploitation. Within BMN, adopting a defense-in-depth strategy involves deploying a diverse array of security measures across people, processes, and technology to safeguard information assets from a wide range of threats and vulnerabilities (Kidd, D, 2023).

Defense-in-depth encompasses a multifaceted approach to security that includes physical security measures, network security controls, endpoint security solutions, and security awareness training programs. By implementing multiple layers of security controls, such as firewalls, intrusion detection systems, antivirus software, encryption technologies, and security monitoring tools, BMN can create a robust security posture that protects against both external and internal threats (InterviewPrep Career Coach, 2023).

Furthermore, defense-in-depth extends beyond technical controls to include administrative and procedural safeguards, such as security policies, incident response plans, and employee training programs. By integrating security into every aspect of operations, BMN can create a culture of security awareness and accountability that reinforces the effectiveness of technical controls and enhances overall security resilience.

As technology continues to advance and organizations become increasingly interconnected, the scope and sophistication of cyber threats have grown exponentially, posing significant challenges to the integrity, confidentiality, and availability of sensitive information and digital assets.

Organizations like BMN encounter a wide spectrum of cyber threats, each presenting unique risks and potential consequences. Among the most prevalent threats are:

Malware: Malicious software, including viruses, worms, ransomware, and Trojans, poses a significant threat to organizational systems and data by infiltrating networks, compromising devices, and disrupting operations.

Phishing Attacks: Phishing attacks involve the use of deceptive emails, websites, or messages to trick individuals into divulging sensitive information, such as login credentials, financial data, or personal details, posing a serious threat to data confidentiality and user privacy (Cybersecurity FAQs, 2024).

Insider Threats: Insider threats arise from individuals within an organization who misuse their authorized access privileges to intentionally or unintentionally compromise information security, whether through malicious actions, negligence, or human error (Cybersecurity FAQs, 2024).

Advanced Persistent Threats (APTs): APTs are sophisticated and targeted cyber attacks launched by skilled adversaries with the intent of gaining unauthorized access to sensitive information, perpetrating espionage, or disrupting organizational operations over an extended period, posing a significant challenge to organizational resilience and security defenses (Cybersecurity FAQs, 2024).

The implications of these cyber threats for organizational security are profound, encompassing operational disruptions, financial losses, reputational damage, and regulatory non-compliance. A successful cyber attack can result in downtime, data breaches, intellectual property theft, fraud, legal liabilities, and erosion of stakeholder trust, highlighting the critical importance of proactive risk management and threat mitigation measures.

In response to the evolving threat landscape, organizations like BMN must adopt a proactive and multifaceted approach to risk management and threat mitigation. This involves implementing a combination of technical controls, such as firewalls, antivirus software, intrusion detection systems, and encryption technologies, along with robust security policies, employee training programs, and incident response plans.

Moreover, organizations must stay abreast of emerging threats and evolving attack vectors through continuous monitoring, threat intelligence sharing, and collaboration with industry peers and cybersecurity experts. By remaining vigilant and adaptive, organizations can effectively identify, assess, and mitigate cyber risks, enhancing their resilience and ability to withstand cyber attacks and security incidents.

We can also take into account the risk management, that is a foundational pillar of effective information security governance, providing organizations like Business Media Network (BMN) with a structured approach to identifying, assessing, and mitigating risks to information assets. By systematically managing risks, organizations can minimize the likelihood and impact of security incidents, enhance resilience, and protect sensitive information from unauthorized access, disclosure, or exploitation.

The risk management process encompasses several critical components, each playing a pivotal role in safeguarding information assets and ensuring the resilience of organizational operations. These key components include:

The initial phase of risk management involves the comprehensive identification of potential threats, vulnerabilities, and weaknesses that could pose risks to information assets within the organization. This crucial step often entails conducting thorough risk assessments, vulnerability scans, and security audits to identify and catalog potential risks. By analyzing the impact of these risks on organizational operations, reputation, and financial stability, organizations like Business Media Network (BMN) can gain insights into the specific challenges they face and prioritize risk mitigation efforts accordingly.

Following the identification of risks, the next step is to assess their likelihood and potential impact on information assets. This involves conducting a detailed evaluation of the probability of risk occurrence and the severity of potential consequences. Factors such as the value of assets at risk, the effectiveness of existing controls, and the organization's risk tolerance levels are taken into account during this assessment. By quantifying and qualifying risks, organizations can make informed decisions regarding risk mitigation strategies and resource allocation to address the most pressing security threats effectively.

Once risks have been assessed, organizations must develop and implement appropriate risk treatment strategies to mitigate identified risks to an acceptable level. This may involve the implementation of various security controls, safeguards, or countermeasures aimed at reducing the likelihood or impact of risks. Examples include enhancing access controls, implementing encryption technologies, or deploying intrusion detection systems. Additionally, organizations may choose to transfer risks through insurance policies or contractual agreements or accept risks when the cost of mitigation outweighs the potential impact. By carefully considering risk treatment options, organizations can effectively manage their exposure to security threats and minimize the potential impact on their operations and stakeholders.

Risk management is an iterative process that requires ongoing monitoring and review to ensure the effectiveness of implemented security controls. Continuous vigilance is essential to detect changes in the threat landscape, assess the performance of existing controls, and identify emerging risks and vulnerabilities. Regular reviews of risk assessments and treatment plans enable organizations to adapt their security posture dynamically and address evolving threats effectively. By remaining proactive and responsive to changes in the cybersecurity landscape, organizations like BMN can maintain the resilience of their information security programs and protect sensitive assets from evolving threats and vulnerabilities.

In addition to implementing robust internal risk management practices, organizations such as Business Media Network (BMN) must also navigate a complex landscape of external regulatory requirements and industry standards governing information security. Compliance with these regulations and standards is essential for safeguarding sensitive data, maintaining legal and regulatory compliance, and mitigating the risk of fines, penalties, or legal repercussions.

For multinational conglomerates like BMN, compliance with a myriad of regulations and standards is imperative to operate ethically, transparently, and securely in today's interconnected business environment. Among the most prominent regulatory frameworks impacting information security are:

General Data Protection Regulation (GDPR): The GDPR, enacted by the European Union (EU), sets strict guidelines for the protection of personal data and the rights of individuals. Compliance with GDPR requires organizations to implement robust data protection measures, obtain explicit consent for data processing, and notify authorities of data breaches promptly.

Non-compliance with GDPR can result in significant fines and reputational damage for organizations like BMN.

Payment Card Industry Data Security Standard (PCI DSS): PCI DSS is a set of security standards designed to ensure the secure handling of credit card information by merchants and service providers. Compliance with PCI DSS requires organizations to implement stringent security controls, conduct regular security assessments, and undergo annual audits to validate compliance. Failure to comply with PCI DSS can lead to severe financial penalties and the loss of customer trust (Khan, T, 2024).

International Organization for Standardization (ISO) Standards: ISO standards, such as ISO/IEC 27001 for information security management systems (ISMS), provide organizations with a framework for establishing, implementing, maintaining, and continually improving an effective ISMS. Compliance with ISO standards demonstrates an organization's commitment to information security best practices, enhances organizational resilience, and fosters trust among stakeholders.

*Table 1.1 - the most prominent regulatory frameworks impacting information security*

| Framework | Focus | Applies To | Key Requirements | Enforcement |
|---|---|---|---|---|
| GDPR | Data Privacy | EU resident data | Consent, breach notification, individual rights | Fines |
| PCI DSS | Payment Card Security | Cardholder data processors | Secure network, data protection, access control | Fines, loss of privileges |
| ISO 27001 | InfoSec Management | Any organization | InfoSec framework | Certification |

Source: created by author, based on the information from European Union (2016, April 14)& International Organization for Standardization (2013)& PCI Security Standards Council. PCI Security Standards Council.

For organizations like BMN, ensuring compliance with external regulatory requirements and industry standards requires a proactive and multifaceted approach. This involves:

Conducting Regulatory Assessments: Organizations must conduct regular assessments to identify relevant regulatory requirements and assess their current level of compliance. This may involve conducting gap analyses, risk assessments, and compliance audits to identify areas of non-compliance and prioritize remediation efforts (Valency Networks, 2013).

Implementing Compliance Controls: Once regulatory requirements have been identified, organizations must implement appropriate controls and measures to achieve and maintain compliance. This may involve developing policies and procedures, deploying technical safeguards, and providing employee training to ensure adherence to regulatory requirements.

Monitoring and Reporting: Continuous monitoring and reporting are essential to track compliance status, identify emerging risks, and demonstrate ongoing compliance to regulatory authorities and stakeholders. This may involve implementing monitoring tools, conducting regular assessments, and maintaining accurate records of compliance activities and outcomes. Given the strategic significance of information security in safeguarding sensitive corporate data, it is crucial to conceptualize and understand the specific methods employed by companies like Business Media Network (BMN) to tackle emerging cyber threats effectively. This is particularly vital in an era where digital assets are integral to operational integrity and competitive positioning. The comprehensive approach adopted by BMN, focusing on the principles of confidentiality, integrity, and availability, provides a solid framework for their cybersecurity strategy.

To visually represent this strategy, the following table summarizes the key components of BMN's information security measures based on the CIA (Confidentiality, Integrity, and Availability) triad.

*Table 1.2 - Key components of BMN's information security measures*

| Security Principle Measures Implemented by BMN | |
|---|---|
| Confidentiality | Encryption, Access Controls, User Authentication |
| Integrity | Data Validation Mechanisms, Digital Signatures, Version Control |
| Availability | Redundancy Measures, Disaster Recovery Plans, Robust Infrastructure |

Source: created by author, based on the information that I cannot share due to NDA.

The table provides a comprehensive breakdown of the various tactics BMN utilizes to address each facet of the CIA triad, showcasing a layered approach to cybersecurity. For instance, to ensure data confidentiality, the table might detail BMN's use of the industry-standard encryption algorithm and multi-factor authentication (MFA) to restrict unauthorized access.

Furthermore, the table highlights how BMN upholds data integrity. This could involve data validation techniques like checksums and hash functions, which verify data hasn't been tampered with during transmission or storage. Additionally, digital signatures allow BMN to confirm the authenticity of the data source and prevent unauthorized modifications.

Data availability is another crucial aspect addressed in the CIA triad. The table might showcase BMN's use of a robust (data backup and recovery strategy), dispersed data centers, and redundancy measures to minimize downtime in case of outages. This ensures data remains accessible even during unforeseen circumstances.

The beauty of the CIA triad lies in its layered approach. By employing a combination of these security measures, BMN strengthens its overall security posture. They don't rely on a single safeguard but implement multiple controls that work in that way that it creates a more robust defense. This layered approach helps prevent a single point of failure and mitigates the potential impact of a security breach.

By focusing on confidentiality, integrity, and availability, BMN safeguards sensitive information, ensures data accuracy and prevents unauthorized changes, and guarantees data accessibility when needed.

In addition to the written component, I want to provide a visual representation of how the CIA triad appears under the majority settings.

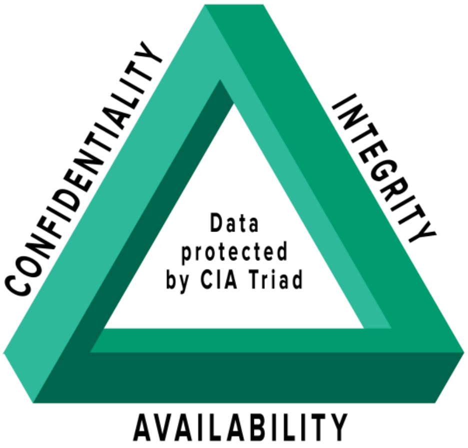


**Figure 1**. The CIA Triad. Source:created by Debbie Walkowski, 2019. Retrieved from:https://www.f5.com/labs/learning-center/what-is-the-cia-triad

This detailed examination and visual representation of BMN's information security framework underscore the critical role that well-rounded security measures play in the protection and sustainable management of digital assets in today's interconnected and risk-prone business environment. Through such strategic investments, BMN is able to fortify its defenses against potential cyber threats, thereby ensuring operational continuity and the preservation of stakeholder trust.

### 1.2 Understanding Information Security

As a result of the widespread incidence of data breaches, cyberattacks, and unauthorized data access in the present era of technology, it is of the utmost necessity to have a comprehensive understanding of information security. As we go deeper into the complexities of information security, it is essential to recognize that it encompasses the processes and methods that have been developed to protect data from being accessed, used, disclosed, interrupted, altered, or destroyed without authorization.

Information security is built on three fundamental principles: confidentiality, integrity, and availability, which are frequently referred to as CIA. These principles constitute the basis of information security. When it comes to maintaining confidentiality, the act of ensuring that classified information is only accessible to those individuals who have been given authorization to access it is referred to as confidentiality. There are numerous well-known breaches that have resulted in the disclosure of sensitive information, which demonstrates that this aspect of information security is commonly overlooked. More over thirty percent of all cyberattacks were undertaken with the intention of stealing personal information. The importance of safeguarding such information is brought into further focus by this.

Integrity refers to the protection of information from being tampered with in an unauthorized manner. When it comes to ensuring the dependability of information systems, it is of the utmost importance to ensure that the data is accurate and comprehensive throughout all stages of its existence. Malware, which is software that infiltrates computer systems and modifies data without the knowledge of users or administrators, is a common method that is used to compromise the integrity of a system.

As the third and final pillar, availability ensures that authorized users are able to quickly access the information and resources that they require whenever they are needed. Instances of attacks on availability can take many forms, one of which is the distributed denial of service (DDoS) attack, which is designed to flood systems with traffic in order to render them inoperable. There was a twenty percent increase in distributed denial of service attacks (DDoS) in comparison to the previous year. This suggests that there is a growing tendency to target service availability.

Phishing, social engineering, malware, and advanced persistent threats (APTs) are just some of the methods that might compromise information security. The hazards that are associated with information security are varied and sophisticated. Phishing attacks, in which the perpetrators pose as trustworthy companies in order to steal critical information from consumers who are unaware of the attack, continue to be one of the most common types of cyberattacks. Phishing was considered to be a contributing factor in nearly ninety percent of all data breaches, according to the Deloitte Malaysia report, that was conducted in 2020 (Deloitte Malaysia, 2020).

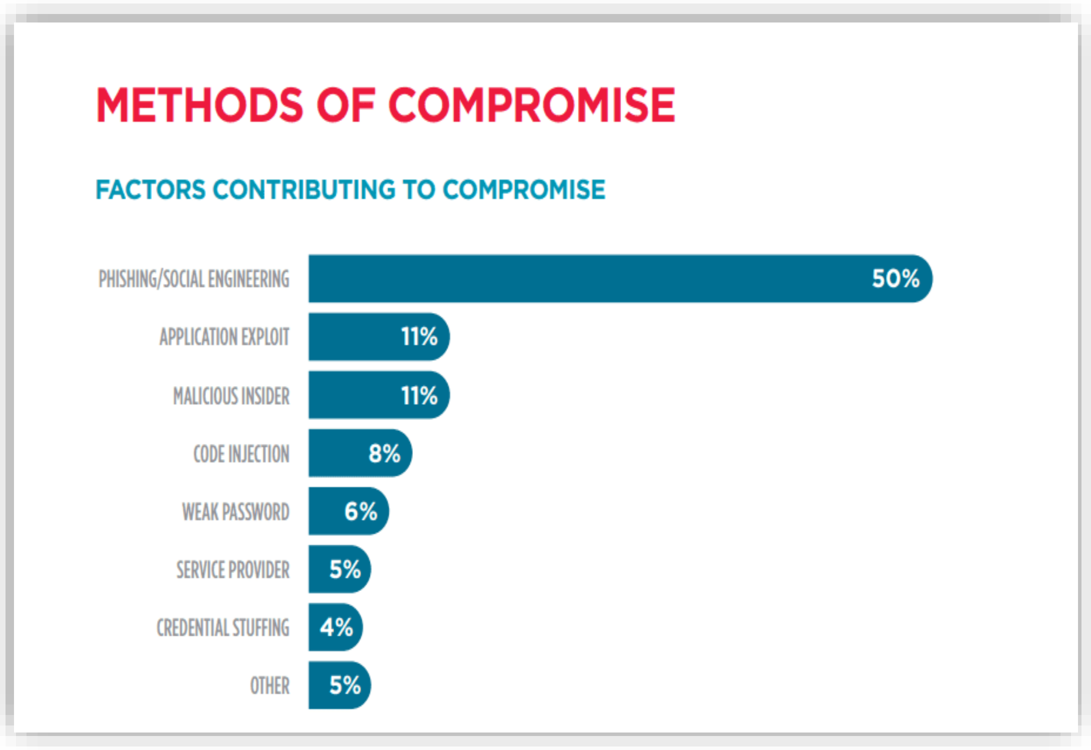


**Figure 2**. Methods of compromise.

Retrieved from https://www.resolutets.com/cyber-security-threat-remediation/

The use of social engineering techniques, which exploit human psychology rather than technological vulnerabilities, remains a significant threat. Attackers can gain unauthorized access to systems and data by deceiving employees into breaking established security protocols, leading to security breaches. One of the most notorious examples of this was carried out by Lithuanian national Evaldas Rimasauskas against two of the world's largest companies, Google and Facebook. Rimasauskas and his team created a fake company, mimicking a legitimate computer manufacturer that worked with Google and Facebook. They set up bank accounts in the company's name and sent phishing emails to specific employees at both companies, invoicing them for genuine goods and services but directing payments to their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates managed to defraud the two tech giants of over $100 million. As a further point of interest, the discipline of information security is always evolving in response to the progression of technology. (Tessian, 2023)

The explosion of the Internet of Things (IoT) creates a vast network of interconnected devices, but each one also introduces a potential security hole. These often inadequately secured devices can be exploited by cybercriminals as entry points for attacks. Studies suggest a significant rise in IoT-based attacks on businesses. According to CompTIA, experts predict over 25% of all cyberattacks against businesses will involve IoT devices by 2025**. (**CompTIA, 2016).

In terms of information security, the legislative framework is still another significant factor to take into mind. With the goal of protecting both personal and organizational information, numerous rules and regulations have been put into place all over the world. A few of examples of legislation that enforce strong limitations and penalties to guarantee the protection of data include the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. Both of these pieces of legislation are examples of legislation. The failure to comply with these standards may result in severe monetary sanctions, as the fines imposed by the General Data Protection Regulation (GDPR) can amount to 4% of the company's annual worldwide revenue or €20 million, whichever is greater.

A complete strategy for information security should be implemented by organizations. This approach should comprise many layers of protection, including administrative, technical, and physical safeguards. In contrast to administrative controls, which involve the application of rules and procedures, physical controls include measures such as the installation of secure hardware and facilities. On the other hand, technical controls are those that pertain to the software and technology that is utilized in order to protect their data. Furthermore, it is of the utmost importance to establish training and awareness programs in order to educate staff members about the potential dangers and suitable security practices. This is because human fallibility is typically the most vulnerable part of security systems.

There is no possible way to overstate the significance of encryption when it comes to the protection of information. When it comes to protecting digital data while it is being transmitted across global networks, encryption is an extremely important factor. The data that can be read is transformed into a language that is incomprehensible and can only be decoded with the use of a customized key. Encryption has the potential to reduce the likelihood of data breaches by as much as fifty percent. This highlights the significance of encryption. This illustrates that encryption is an instrument that is vital in the field of information security.

The utilization of encryption technology, on the other hand, is not devoid of challenges. The administration of keys continues to be a complex matter, as it requires the protection of key storage and the implementation of frequent upgrades in order to discourage unauthorized access. In addition, the development of quantum computing has led to an increase in the likelihood that traditional encryption algorithms may be broken. The development of encryption methods that are capable of withstanding quantum attacks is required as a result of this. The development of systems that are able to effectively resist the computing power of quantum computers is the objective of a number of cybersecurity organizations, which are aggressively emphasizing research on post-quantum cryptography.

In addition to encryption, other security precautions are significantly strengthened by the implementation of robust authentication mechanisms. It is becoming increasingly usual to implement multi-factor authentication (MFA), which is a security feature that requires the utilization of several various verification techniques. A recent survey discovered that eighty percent of enterprises had utilized Multi-Factor Authentication (MFA) to varied degrees throughout their organizations. The effectiveness of multi-factor authentication (MFA) in reducing the risk of unwanted access is demonstrated by this.

Despite the existence of these instruments, the human element continues to persist as a significant vulnerability in the realm of information security. Social engineering attacks, more specifically phishing, continue to take advantage of the fallibility of humans. Since this is the case, it is of the utmost importance to give ongoing security awareness training. Businesses that hold regular security training sessions see a considerable drop of forty percent in the percentage of successful phishing attacks.

In addition, the rise in the number of teleworkers and remote workers has resulted in the emergence of new security challenges. This makes mobile devices more susceptible to attacks since, in comparison to traditional networked systems, they typically have less security safeguards in place.

At the same time that the characteristics of cyber attacks are evolving, the security measures are also becoming more complex. Artificial intelligence (AI) and machine learning (ML) are becoming more integrated into the process of identifying and responding to security events in order to achieve improved efficiency. Security systems that are powered by artificial intelligence have the ability to analyze large amounts of data in order to identify patterns and abnormalities that may indicate a possible threat to the security of the organization. The incorporation of artificial intelligence (AI) into security systems has led to a reduction of incident reaction times by as much as 70 percent. As a result, this demonstrates the significant potential that artificial intelligence has to significantly improve security operations.

In addition, implementing security safeguards throughout the software development process, known as DevSecOps, represents a significant step towards preventative security. Integrating security from the beginning allows companies to proactively address vulnerabilities before they become major issues, preventing them from being caught off guard. This approach not only enhances security but also reduces the complexity and cost of ensuring software compliance with security standards throughout the lifecycle (Mitre, 2023).  As a result of the integration of information systems around the world, there has been an increase in vulnerabilities, particularly through supply chains, which cybercriminals are able to control. Given the complex nature of these networks, it is possible that even a minor weakness could result in significant breaches across a number of different systems. The issue of supply chain security has become increasingly concerning. Studies by organizations like Supply Chain Management Review indicate a significant rise in supply chain attacks. These attacks often exploit vulnerabilities in third-party software or services used by businesses. This highlights the critical need for organizations to implement stringent security measures throughout their entire supply chain. The use of cloud computing presents a number of different security challenges, despite the fact that it offers the benefits of scalability and flexibility. When it comes to cloud security, the shared responsibility model emphasizes that cloud providers are accountable for providing the security of the cloud infrastructure, while users are responsible for protecting their data that is stored within the cloud for their own protection. It is possible for security risks to arise as a consequence of this difference if it is not handled correctly. Cloud misconfigurations and weak access controls remain significant contributors to cloud data breaches. According to the *"Cloud Threat Landscape Report 2023"* by the Cloud Security Alliance (CSA), misconfigurations and identity and access management (IAM) failures were the leading causes of cloud breaches in 2022, accounting for 34% of incidents (Cloud Security Alliance, 2023). This emphasizes the importance of robust cloud security practices, including proper configuration management and implementing strong access controls.

In addition, as a result of the extensive availability of data, the protection of customers' and regulators' data privacy has been a significant concern in recent years. The General Data Protection Regulation (GDPR) in Europe and other laws that are very similar to it in other countries are examples of data privacy regulations. These policies enforce severe limits on how data is managed and offer customers access over their own data. By adhering to these standards, businesses not only protect themselves against monetary punishments, but they also foster the confidence of their customers. Seventy-five percent of companies have made significant enhancements to their data security strategy in order to comply with regulatory standards. When it comes to mitigating the impact of security breaches, incident response strategies are absolutely necessary. It is important to have a thorough incident response strategy that includes both immediate containment techniques and long-term preventive activities to reduce the likelihood of another accident occurring. Businesses  who have incident response teams and plans that are effectively formed are able to reduce the financial impact of data breaches by as much as thirty percent. Having this information brings to light the significance of being ready for situations like this.

The concept of "zero trust" has become a core principle in modern cybersecurity. This security model operates on the assumption of "never trust, always verify," regardless of a user, device, or location attempting to access a network. Effective zero trust implementation requires robust multi-factor authentication (MFA), granular access controls that limit access to only what's necessary, and continuous monitoring of network activity for suspicious behavior. Recent research from Palo Alto Networks (Unit 42 Threat Report, 2023) highlights the significant benefits of zero trust. Their report indicates that organizations with a mature zero-trust strategy have experienced a reduction in security incidents by an average of 80%**.**

It is necessary to have security strategies that are equally adaptive because of the ever-changing nature of cyber threats. Ransomware assaults, for instance, have become increasingly sophisticated in recent years. The cybersecurity landscape is constantly evolving, demanding flexible and adaptable security strategies. Ransomware attacks, in particular, have become increasingly complex, often employing "double extortion" tactics. This involves not only encrypting data but also threatening to leak it publicly unless a ransom is paid. This strategy has become a significant concern, with a study by ReliaQuest (2022) revealing that 80% of ransomware incidents they handled in Q4 2022 involved double extortion. (ReliaQuest, 2022).

This highlights the critical need for organizations to implement robust data security measures alongside traditional ransomware protection. Traditional methods can help prevent encryption, but data security measures like strong access controls and data loss prevention can mitigate the impact of data exfiltration threats. The ReliaQuest report (2022) also found a significant increase in ransomware activity in Q4 2022, with 707 "tippers" published (i.e., updates about victims identified on data leak sites). This emphasizes the urgency for organizations to address both aspects of the threat.

Data breaches can have severe consequences beyond public embarrassment. Leaked data can damage an organization's reputation, lead to financial losses due to regulatory fines or lawsuits, and erode customer trust.

This highlights the critical need for organizations to implement robust data security measures alongside traditional ransomware protection. Traditional methods can help prevent encryption, but data security measures like strong access controls and data loss prevention can mitigate the impact of data exfiltration threats.

An ever-increasing necessity for robust cybersecurity measures is being brought about by the ongoing development of technology. Devices connected to the Internet of Things (IoT) that are integrated into routine operations and critical infrastructure provide additional vulnerabilities. Poor security measures within the devices themselves were responsible for forty-five percent of the security breaches that were associated with the Internet of Things.

In a nutshell, in order to maintain the security and dependability of information systems in a digital environment that is always evolving, it is essential to continually be vigilant, flexible, and to make investments in cutting-edge security technologies and procedures. While the complexity of cybersecurity threats continues to rise, it is absolutely necessary that the strategies that are employed to combat them also continue to evolve. Resilience, fast reaction, and compliance with regulatory obligations ought to be high on the list of priorities for these initiatives.

# CHAPTER 2.OBJECT OF STUDY DESCRIPTION

## 2.1. Company Description

Business Media Network of Ukraine (BMN) emerged on February 19, 2022, as a visionary initiative by the Association of Ukrainian Students, UACU University professor, and the co-founder of Economy of Trust, Henry Shterenberg. This conglomerate, structured as a limited liability company, amalgamates attributes of partnership, individual entrepreneurship, and corporation, providing owners with pass-through taxation akin to partnerships while offering limited liability similar to corporations.

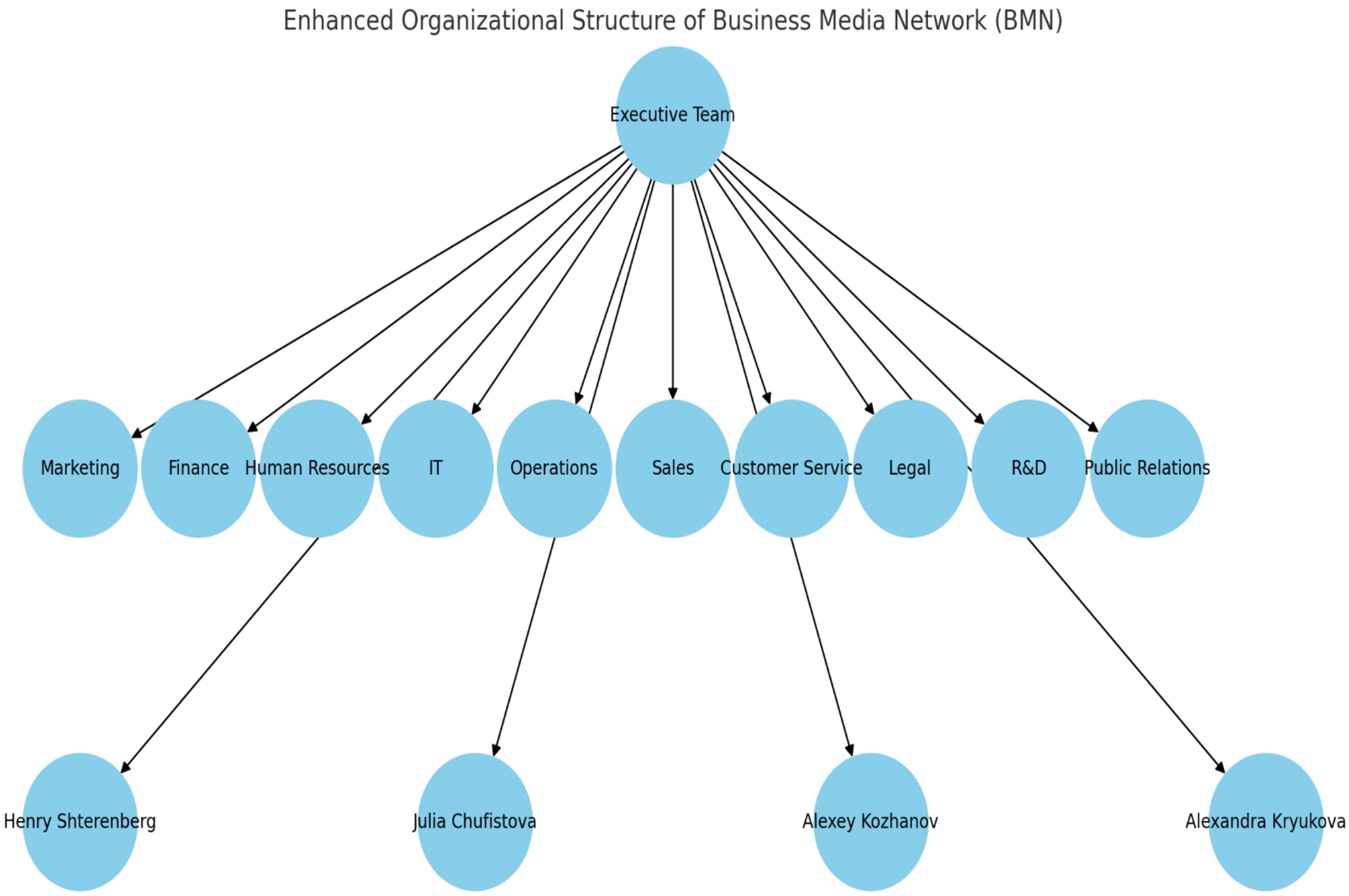


**Figure 3 –** Organizational structure chart for Business Media Network (BMN)

Source: created by author, based on the information retrieved from: https://career.bmnua.com/

Here's the organizational structure chart for Business Media Network (BMN), illustrating the hierarchy and key personnel. The chart positions the Executive Team at the top, with direct connections to ten primary departments like Marketing, Finance, IT, and others. Additionally, key individuals such as Henry Shterenberg, Julia Chufistova, Alexey Kozhanov, and Alexandra Kryukova are shown, emphasizing their strategic roles directly linked to the Executive Team. This layout clearly depicts the linear hierarchy and the crucial interconnections within BMN

BMN's ownership is shared among several key individuals, with Henry Shterenberg and Alex Sheyner as primary proprietors, supported by a dedicated team of students who contribute significantly to the company's vision realization. As a facilitator of trade between legal entities, BMN primarily offers goods and services to corporate clients, operating through its platforms: The Deal Flow, MarketPLace, and City ShowCase.

In response to the Russian invasion of Ukraine, BMN recognized the urgent need for cohesive economic support amidst the chaos and uncertainty gripping the nation. Understanding that economic stability is paramount for national resilience, BMN swiftly took action by establishing The United Students of Ukraine, a strategic initiative designed not only to provide essential working capital to Ukrainian businesses but also to fortify the economic infrastructure and security of the country.

By mobilizing resources and expertise, BMN's initiative aims to bolster the resilience of Ukrainian businesses, ensuring they remain operational despite the disruptions caused by the conflict. Moreover, this concerted effort serves as a testament to BMN's commitment to fostering collaboration and solidarity among various stakeholders, including businesses, government entities, and the broader Ukrainian populace.

In addition to its immediate economic impact, The United Students of Ukraine initiative plays a crucial role in safeguarding the nation's economic security in the face of external threats. By strengthening domestic businesses and supply chains, BMN not only mitigates the adverse effects of the conflict but also reduces Ukraine's dependence on external resources, thereby enhancing its economic sovereignty and resilience against geopolitical pressures.

Furthermore, by channeling financial support to businesses in strategic sectors such as cybersecurity, critical infrastructure, and defense, BMN's initiative contributes to the overall security posture of the nation. By bolstering these key industries, Ukraine can better protect itself against cyber threats, ensure the continuity of essential services, and fortify its defense capabilities in the face of potential cyberattacks or infiltration attempts.

In essence, The United Students of Ukraine initiative represents more than just a humanitarian response to the crisis; it embodies BMN's strategic vision to leverage economic strength as a cornerstone of national security. Through collaborative efforts and targeted interventions, BMN aims to empower Ukrainian businesses, fortify the nation's economic resilience, and safeguard its sovereignty against external threats, thereby contributing to the long-term prosperity and security of Ukraine.

Led by visionary founders including Henry Shterenberg, Julia Chufistova, Alexey Kozhanov, and Alexandra Kryukova, BMN exemplifies a culture of innovation, collaboration, and dedication to Ukraine's business ecosystem. The organizational structure, featuring a linear hierarchy with an Executive Team overseeing ten primary departments, enables efficient decision-making and operational excellence.

BMN's projects, including Marketplace, DealFlow, City Showcase, Mayors Club, and United Students of Ukraine, serve diverse functions aimed at promoting Ukrainian businesses on the global stage, fostering economic growth, and facilitating post-war reconstruction and economic development.

The Business Media Network of Ukraine (BMN) operates through a diverse array of platforms and initiatives aimed at fostering economic growth, promoting collaboration, and showcasing the potential of Ukrainian businesses on the global stage.

The Marketplace platform serves as a dynamic arena for businesses, both domestically and internationally, to showcase their products and services. With a seamless online shop experience, Marketplace facilitates communication and interactions among businesses, promoting trade and networking opportunities across Ukraine and beyond. At the core of Marketplace is the innovative Battery of Trust technology, designed to empower users to make informed decisions by aggregating scores based on legality, social engagement, feedback, and transaction success.

DealFlow stands as a prominent facet of BMN's initiatives, serving as an international platform for weekly publications aimed at spotlighting Ukrainian businesses to a global audience. With a weekly circulation reaching millions of international executives and investors, DealFlow showcases Ukraine's business potential by highlighting up to ten projects across various sectors and cities each week, enhancing visibility and fostering connections on the global stage.

City Showcase embodies BMN's commitment to local communities, encompassing a digital network of websites for cities and territorial communities across Ukraine. These websites provide essential information necessary for implementing innovative projects aimed at enhancing community development and advancement, ultimately reaching over 1,470 cities and territorial communities nationwide.

The Mayors Club, a nationwide public organization, plays a pivotal role in BMN's efforts to facilitate post-war reconstruction and economic growth. By uniting mayors and administrative heads of territorial communities, the Mayors Club serves as a think tank, providing strategic planning support for economic and infrastructure development. Through partnerships with international agencies like the Rebuilding Ukraine Agency, the Mayors Club fosters access to financial institutions and facilitates partnerships to support small and medium-sized businesses.

Integral to BMN's initiatives is the United Students of Ukraine, a non-profit organization dedicated to securing jobs, enhancing supply chains, and providing financial support to businesses during times of conflict. Led by dedicated students from Concordia Ukrainian-American University, this initiative underscores the commitment of young individuals to contribute to the progress and prosperity of Ukraine amidst challenging times.

Through these platforms and initiatives, BMN exemplifies its commitment to promoting economic growth, fostering collaboration, and supporting communities across Ukraine, ultimately contributing to the country's long-term prosperity and resilience.

While BMN's existing platforms and initiatives play a crucial role in promoting economic growth and community development in Ukraine, there are additional options worth considering to further enhance its impact and reach. One such option is to explore partnerships with government agencies and international organizations to access additional resources and expertise. Collaborating with these entities can provide BMN with new opportunities to implement larger-scale projects and initiatives that address pressing economic and social challenges facing Ukraine.

Moreover, BMN could consider expanding its digital presence and leveraging emerging technologies to create innovative solutions for businesses and communities. This could involve developing mobile applications or online platforms that offer tailored services and resources to entrepreneurs, such as access to financing, market intelligence, and business support services. By embracing digital innovation, BMN can reach a wider audience and deliver value-added services that meet the evolving needs of Ukrainian businesses and communities.

Additionally, BMN may explore initiatives focused on sustainability and corporate social responsibility (CSR) to address environmental and social issues while driving economic growth. This could include implementing green business practices, supporting renewable energy projects, or investing in initiatives that promote social inclusion and equality. By integrating sustainability into its business model, BMN can demonstrate its commitment to responsible business practices and contribute to building a more sustainable and resilient economy in Ukraine.

While the overview of Business Media Network (BMN) provides valuable insights into its vision, initiatives, and contributions to Ukraine's business landscape, it is essential to acknowledge that BMN's journey has been short-lived. Despite its ambitious goals and promising initiatives, BMN ceased its operations unexpectedly, leaving students who were eager to apply for internships or pursue bachelor's qualification work related to the company's activities in a state of uncertainty.

The closure of BMN may not be classified as a complete failure, as it undoubtedly made strides in promoting economic growth, fostering collaboration, and supporting communities during its brief existence. However, the sudden cessation of its operations has undoubtedly left a negative impression and raised questions about the company's sustainability and long-term viability.

As students who were introduced to BMN and encouraged to engage with its initiatives, the closure has had a profound impact, leaving us with unanswered questions and unfulfilled opportunities. While BMN's legacy may not be entirely negative, its abrupt exit has undoubtedly left a mark on us, highlighting the unpredictability and volatility of the business world.

Moving forward, it is essential for students and aspiring professionals to reflect on their experiences with BMN, draw lessons from its successes and shortcomings, and channel their energy into pursuing new opportunities and initiatives that align with their goals and aspirations. Despite the challenges posed by BMN's closure, it presents an opportunity for growth, resilience, and the pursuit of new endeavors that contribute to Ukraine's economic development and prosperity.

## 2.2. HR Management for Information Security

In the realm of information security, human resource management plays a pivotal role in shaping the effectiveness and resilience of an organization's security posture. With the increasing sophistication of cyber threats and the growing reliance on technology in modern business operations, organizations must prioritize the recruitment, training, and retention of skilled professionals capable of safeguarding sensitive information and digital assets. Cyber threats pose significant risks to organizations, ranging from data breaches and financial losses to reputational damage and legal liabilities. HRM plays a crucial role in mitigating these risks by ensuring that employees are well-equipped to recognize, respond to, and prevent cyber threats effectively.

One of the primary challenges in HRM related to cyber threats is the human factor. Employees are often the weakest link in an organization's cybersecurity defenses, as they may inadvertently fall victim to social engineering attacks, phishing scams, or other forms of manipulation by malicious actors. For example, an employee may receive a fraudulent email purportedly from a trusted source, prompting them to click on a malicious link or provide sensitive information, thereby compromising the organization's security.

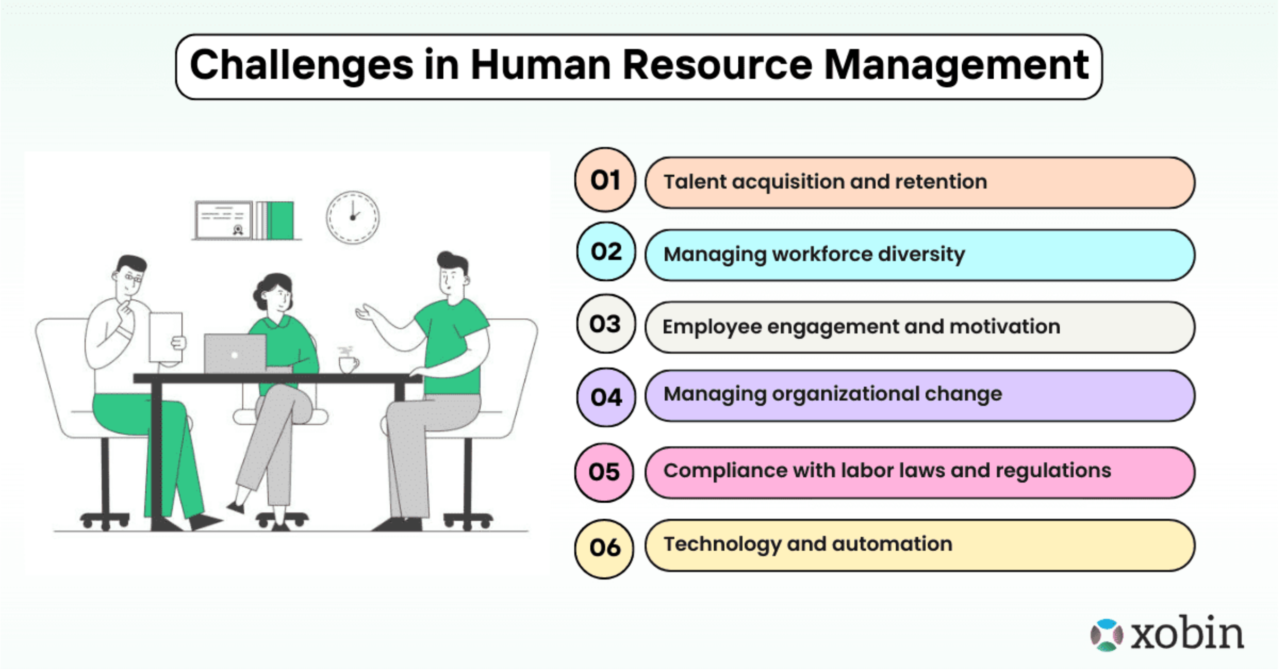
HRM must prioritize cybersecurity awareness training and education for all employees. Training programs should cover topics such as recognizing phishing attempts, identifying suspicious emails or messages, practicing good password hygiene, and understanding the importance of data security protocols. By equipping employees with the knowledge and skills to identify and respond to cyber threats, organizations can significantly reduce the likelihood of successful attacks and minimize the impact of security incidents (InterviewPrep, 2023).

Furthermore, HRM plays a critical role in enforcing security policies and procedures within the organization. HR professionals are responsible for communicating security policies to employees, ensuring that they understand their responsibilities regarding information security, and enforcing compliance with established protocols. This may involve conducting regular security briefings, disseminating relevant information about emerging threats, and monitoring employee adherence to security policies through audits and assessments.

Additionally, HRM is instrumental in managing access control and user privileges within the organization. HR professionals collaborate with IT teams to ensure that employees have appropriate access to systems, applications, and data based on their roles and responsibilities. By implementing robust access control measures, such as least privilege access and multi-factor authentication, HRM can minimize the risk of unauthorized access and insider threats, thereby enhancing the organization's overall security posture (BusinessTechWeekly, 2023).

Moreover, HRM plays a crucial role in incident response and crisis management in the event of a cybersecurity incident. HR professionals collaborate with IT and security teams to develop incident response plans, establish communication protocols, and coordinate the organization's response efforts. This may involve notifying affected employees, liaising with external stakeholders, and providing support and guidance to mitigate the impact of the incident on the organization's operations and reputation. (BusinessTechWeekly, 2023).

One of the fundamental challenges in human resource management for information security lies in the shortage of qualified professionals with specialized skills in cybersecurity. As the demand for cybersecurity expertise continues to outpace the supply of talent, organizations like Business Media Network (BMN) must adopt proactive strategies to attract and retain top talent in the field. This scarcity is fueled by several factors.



Challenges in Human Resource Management

01 Talent acquisition and retention

02 Managing workforce diversity

03 Employee engagement and motivation

04 Managing organizational change

05 Compliance with labor laws and regulations

06 Technology and automation

**Figure 4 –** Challenges in Human Resource Management.

Retrieved from: https://xobin.com/blog/what-is-human-resource-management-challenge-process-role/

The shortage of qualified cybersecurity professionals is exacerbated by the rapidly evolving threat landscape. Cyber threats are constantly evolving, with new threats emerging regularly and existing threats becoming more sophisticated. Cybersecurity professionals must possess up-to-date knowledge and skills to effectively defend against these evolving threats. However, keeping pace with the rapidly changing threat landscape requires continuous learning and professional development, which can be challenging for both aspiring and experienced cybersecurity professionals.

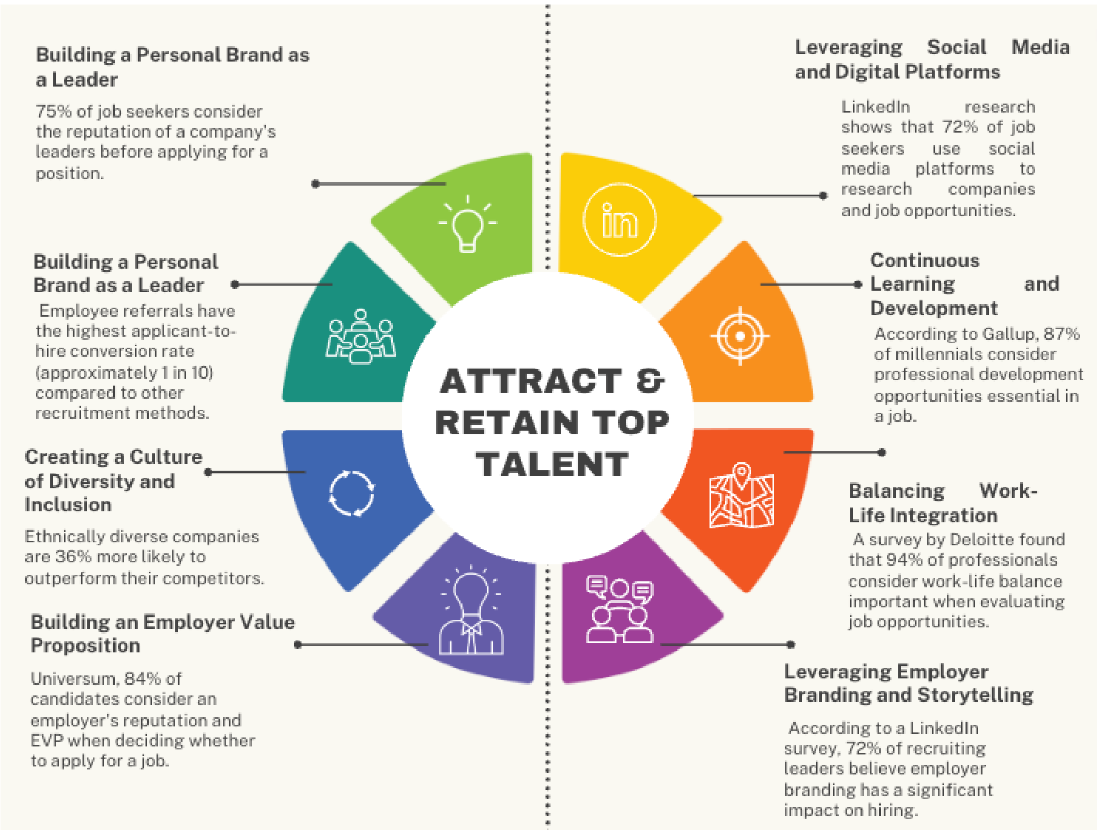
Additionally, there is a lack of formal education and training programs that adequately prepare individuals for careers in cybersecurity. Many academic institutions struggle to keep pace with the rapidly evolving nature of cybersecurity, resulting in outdated curricula and limited opportunities for hands-on experience. Furthermore, there is a shortage of standardized certification programs that validate the skills and expertise of cybersecurity professionals, making it difficult for employers to assess the qualifications of potential candidates.

The competition for cybersecurity talent is intense, with organizations across various industries vying for top talent. Large tech companies and government agencies often have greater resources and incentives to offer competitive salaries, benefits, and career advancement opportunities, making it challenging for smaller organizations like BMN to compete for top talent.

Moreover, there is a significant skills gap in cybersecurity, with many job openings requiring specialized technical skills such as threat detection, incident response, penetration testing, and secure coding. Additionally, soft skills such as communication, problem-solving, and teamwork are also essential for success in cybersecurity roles but may be overlooked in traditional education and training programs.

To address the shortage of cybersecurity professionals, organizations like BMN must adopt proactive strategies to attract, develop, and retain top talent. This includes investing in education and training programs, partnering with academic institutions, fostering a culture of continuous learning, offering competitive compensation and benefits, and emphasizing diversity and inclusion initiatives.

By adopting these proactive strategies, BMN can mitigate the impact of the cybersecurity skills shortage and build a talented and resilient cybersecurity team capable of effectively protecting the organization's information assets and digital infrastructure. Through these efforts, BMN can strengthen its information security posture and better position itself to address the evolving cybersecurity threats facing modern organizations.



**Building a Personal Brand as a Leader**

75% of job seekers consider the reputation of a company's leaders before applying for a position.

**Building a Personal Brand as a Leader**

Employee referrals have the highest applicant-to-hire conversion rate (approximately 1 in 10) compared to other recruitment methods.

**Creating a Culture of Diversity and Inclusion**

Ethnically diverse companies are 36% more likely to outperform their competitors.

**Building an Employer Value Proposition**

Universum, 84% of candidates consider an employer's reputation and EVP when deciding whether to apply for a job.

**Leveraging Social Media and Digital Platforms**

LinkedIn research shows that 72% of job seekers use social media platforms to research companies and job opportunities.

**Continuous Learning and Development**

According to Gallup, 87% of millennials consider professional development opportunities essential in a job.

**Balancing Work-Life Integration**

A survey by Deloitte found that 94% of professionals consider work-life balance important when evaluating job opportunities.

**Leveraging Employer Branding and Storytelling**

According to a LinkedIn survey, 72% of recruiting leaders believe employer branding has a significant impact on hiring.

**Figure 5 –** Attract & Retain Top Talent Chart.

Created by: Andzelika Bendoraityte, retrieved from: https://www.linkedin.com/pulse/how-become-talent-magnet-strategies-attracting-top-bendoraityte-/

Additionally, effective human resource management for information security necessitates the establishment of clear roles, responsibilities, and reporting structures within the organization. By defining job roles and expectations, organizations can ensure that employees understand their responsibilities regarding information security and are equipped with the necessary tools and resources to fulfill their duties effectively. Moreover, clear reporting structures enable employees to escalate security incidents and concerns promptly, facilitating timely response and resolution.

Training and awareness programs are also integral components of human resource management for information security. Employees are often the weakest link in an organization's security defenses, as they may inadvertently fall victim to social engineering attacks or engage in risky behavior that compromises security. Therefore, organizations must invest in comprehensive training programs to educate employees about the importance of information security, common cyber threats, and best practices for safeguarding sensitive information. Regular security awareness training can empower employees to recognize and respond to security threats effectively, thereby reducing the organization's overall risk exposure.

Furthermore, effective human resource management for information security involves implementing robust policies and procedures governing access control, data handling, and incident response. These policies serve as the foundation for a proactive and systematic approach to information security, providing clear guidelines for employees to follow and ensuring consistency in security practices across the organization. By enforcing adherence to security policies and holding employees accountable for their actions, organizations can strengthen their overall security posture and minimize the risk of security breaches.

HR management plays a very important role in ensuring the effectiveness and resilience of information security programs within organizations like BMN. By prioritizing the recruitment, training, and retention of skilled professionals, establishing clear roles and responsibilities, providing comprehensive training and awareness programs, and enforcing robust policies and procedures, organizations can enhance their ability to protect sensitive information and digital assets from evolving cyber threats.

Training for human resource management in information security can be approached through a multifaceted and comprehensive strategy that addresses the diverse needs of employees at all levels of the organization. Role-based training, awareness programs, technical training, certification programs, simulation exercises, continuous learning initiatives, and metrics and evaluation methods are key components of an effective training program.

Effective training programs enhance employee awareness, skills, and confidence in managing security threats, ultimately strengthening the organization's resilience to cyber threats and ensuring the protection of sensitive information assets. Through ongoing investment in training and professional development, organizations can empower their human resource management teams to effectively manage information security risks and contribute to the overall success of the organization.

### 2.3. Marketing and Logistics for Information Security

Marketing and logistics play crucial roles in promoting and delivering effective information security solutions within organizations like BMN. These functions are instrumental in raising awareness about cybersecurity risks, promoting security products and services, and ensuring the efficient distribution and implementation of security measures.

In the context of information security, marketing involves communicating the value proposition of security products and services to internal stakeholders, such as employees and management, as well as external clients and partners. This includes creating marketing campaigns, developing educational materials, and organizing awareness events to highlight the importance of cybersecurity and promote best practices for protecting sensitive information. Marketing campaigns play a vital role in promoting cybersecurity within organizations like BMN, as well as in the broader business landscape (FasterCapital, 2024). These campaigns are essential for raising awareness about cybersecurity risks and the importance of implementing robust security measures to protect sensitive information and digital assets.

In the context of BMN, marketing campaigns can be tailored to address the specific needs and concerns of internal stakeholders, such as employees and management. For example, campaigns may focus on educating employees about the latest cyber threats, such as phishing attacks or malware infections, and providing them with practical tips and best practices for safeguarding their devices and data. By empowering employees with the knowledge and tools to recognize and respond to security threats, organizations can significantly reduce the risk of security breaches and data loss (BusinessTechWeekly, 2023).

Additionally, marketing campaigns can be used to showcase the security features and benefits of BMN's products and services to clients, partners, and other stakeholders. This may involve highlighting the organization's commitment to protecting customer data, complying with industry regulations, and implementing state-of-the-art security technologies. By effectively communicating the value proposition of BMN's security solutions, marketing campaigns can help build trust and credibility with customers and differentiate the organization from competitors.

Plus, in the larger framework of "marketing and logistics for information security," the importance of cybersecurity cannot be emphasized. In today's digital world, where cyber attacks are getting more complex and common, businesses must consider cybersecurity as a key component of their company strategy. Marketing activities must match with this aim by emphasizing security's important role in protecting sensitive information, keeping consumer trust, and ensuring operational resilience.

Besides, marketing efforts can be an effective method for increasing cybersecurity awareness and education among organizations and individuals. Organizations may develop a security-conscious and resilient culture by raising knowledge of prevalent cyber risks, advocating best practices for cybersecurity hygiene, and emphasizing the need of investing in robust security solutions.

Overall, marketing plays a crucial role in promoting cybersecurity both internally within organizations like BMN and externally in the broader business ecosystem. By leveraging marketing campaigns to raise awareness, educate stakeholders, and promote the value of security, organizations can strengthen their security posture, mitigate cyber risks, and protect sensitive information assets from evolving threats.

Certainly, in the realm of cybersecurity, effective marketing efforts extend beyond simply raising awareness of security risks; they also involve showcasing specific security solutions and technologies to address those risks. This can include demonstrating how these solutions align with the organization's security needs and business objectives, as well as highlighting their effectiveness in mitigating cyber threats.

For instance, in the case of BMN, marketing efforts may focus on promoting the features and benefits of specific security products or services offered by the conglomerate. This could involve highlighting how these solutions address common security challenges faced by businesses, such as data breaches, malware infections, or insider threats. By showcasing the capabilities of these security solutions and illustrating their real-world impact, organizations can effectively communicate the value proposition of their security offerings to potential clients, partners, and stakeholders.

Moreover, demonstrating the effectiveness of security solutions through case studies, testimonials, or industry certifications can further bolster their credibility and appeal. This helps build trust and confidence in the organization's ability to deliver reliable and robust security solutions that meet the needs of clients and partners.

Overall, by incorporating a focus on specific security solutions and technologies into their marketing efforts, organizations like BMN can not only raise awareness of cybersecurity issues but also drive adoption of security measures that enhance the overall resilience and security posture of the organization.

Logistics, on the other hand, focuses on the practical aspects of implementing information security solutions, ensuring that they are deployed effectively and efficiently. This includes activities such as procuring security products and services, managing inventory, coordinating installations and configurations, and overseeing maintenance and updates.

Supply chain security is a critical component of logistics in the context of information security, particularly for organizations like BMN that rely on third-party vendors and suppliers for various goods and services. These vendors and suppliers may have access to sensitive information or provide critical functions that are integral to the organization's operations, making them potential targets for cyber attacks or vulnerabilities in the supply chain.

To mitigate these risks, organizations must establish rigorous procurement processes and vendor management practices to ensure that vendors meet security standards and adhere to best practices. This may involve conducting thorough assessments of vendors' security controls, certifications, and compliance with relevant regulations. Additionally, organizations should incorporate security requirements into vendor contracts and agreements to enforce accountability and establish clear expectations for security responsibilities.

Implementing ongoing monitoring and oversight of third-party vendors is crucial to maintaining the security of information assets. Regular audits, assessments, and performance reviews help organizations identify any security issues or vulnerabilities that may arise over time. By conducting these evaluations, organizations can ensure that vendors adhere to security standards and fulfill their contractual obligations. This proactive approach allows organizations to address potential risks promptly, strengthening their overall security posture and safeguarding against potential threats stemming from third-party relationships.

By taking a proactive approach to supply chain security and implementing robust logistics practices, organizations can reduce the risk of supply chain attacks, safeguard sensitive information, and maintain the integrity of their information security infrastructure. This ultimately enhances the overall resilience and security posture of the organization in the face of evolving cyber threats and vulnerabilities (InterviewPrep, 2023).

Furthermore, logistics plays a vital role in incident response and disaster recovery, ensuring that organizations can quickly and effectively respond to security incidents and restore normal operations in the event of a breach or disruption. This may involve establishing incident response plans, defining roles and responsibilities, and coordinating with internal teams and external partners to minimize the impact of security incidents on the organization.

Effective marketing and logistics are essential components of a comprehensive information security strategy. By raising awareness, promoting security solutions, and ensuring efficient implementation and management of security measures, organizations can strengthen their security posture, mitigate cyber risks, and protect sensitive information assets from evolving threats.

# CHAPTER 3. PROPOSALS FOR ENHANCING INFORMATION SECURITY MANAGEMENT

## 3.1. Recommendations for Improving Information Security Management in BMN

In light of the insights gained from the internship at Business Media Network (BMN) and the thorough analysis of its operations, several key recommendations emerge for enhancing information security management within the organization. These recommendations aim to address existing weaknesses, capitalize on strengths, and capitalize on opportunities while mitigating potential threats, ultimately fortifying BMN's information security posture.

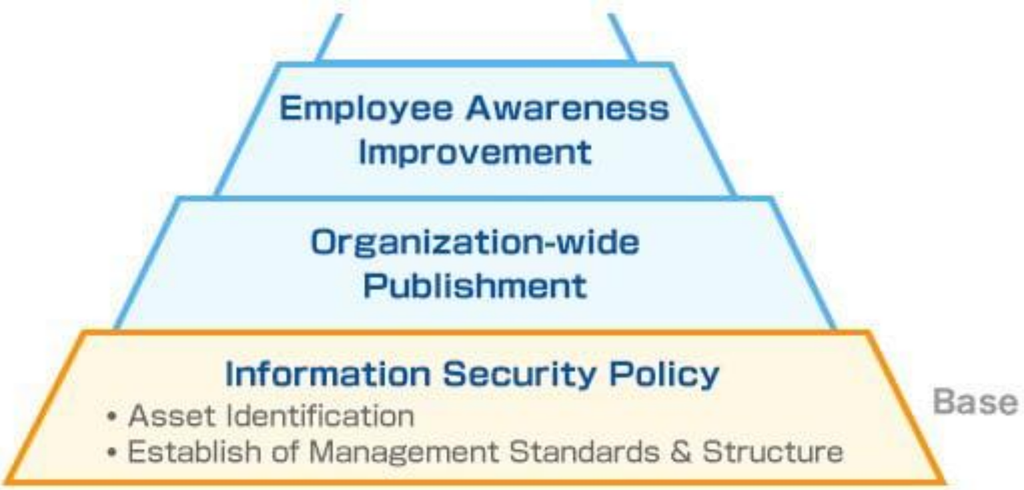

Employee Awareness Improvement
Organization-wide Publishment
Information Security Policy
• Asset Identification
• Establish of Management Standards & Structure
Base

**Figure 6 –** Information Security Policy Overview.

Retrieved from: https://www.nri-secure.com/security-consulting/security-policy-development-support

1. Strengthen Employee Training Programs:

BMN's reliance on student involvement presents a distinctive opportunity to cultivate a workforce characterized by fresh perspectives and innovative thinking. However, it also poses challenges in terms of ensuring that these students possess the necessary skills and knowledge to navigate the complexities of information security effectively. To address this, BMN should prioritize the development of comprehensive employee training programs specifically tailored to the unique needs of its workforce.

These training programs should encompass a wide range of topics, including cybersecurity fundamentals, data protection principles, and incident response procedures. Employees should receive instruction on identifying common cyber threats such as phishing attacks, malware infections, and social engineering tactics, as well as strategies for mitigating these risks effectively. Additionally, training should cover compliance requirements relevant to BMN's industry, ensuring that employees understand their obligations regarding the protection of sensitive information and adherence to relevant regulations such as GDPR.

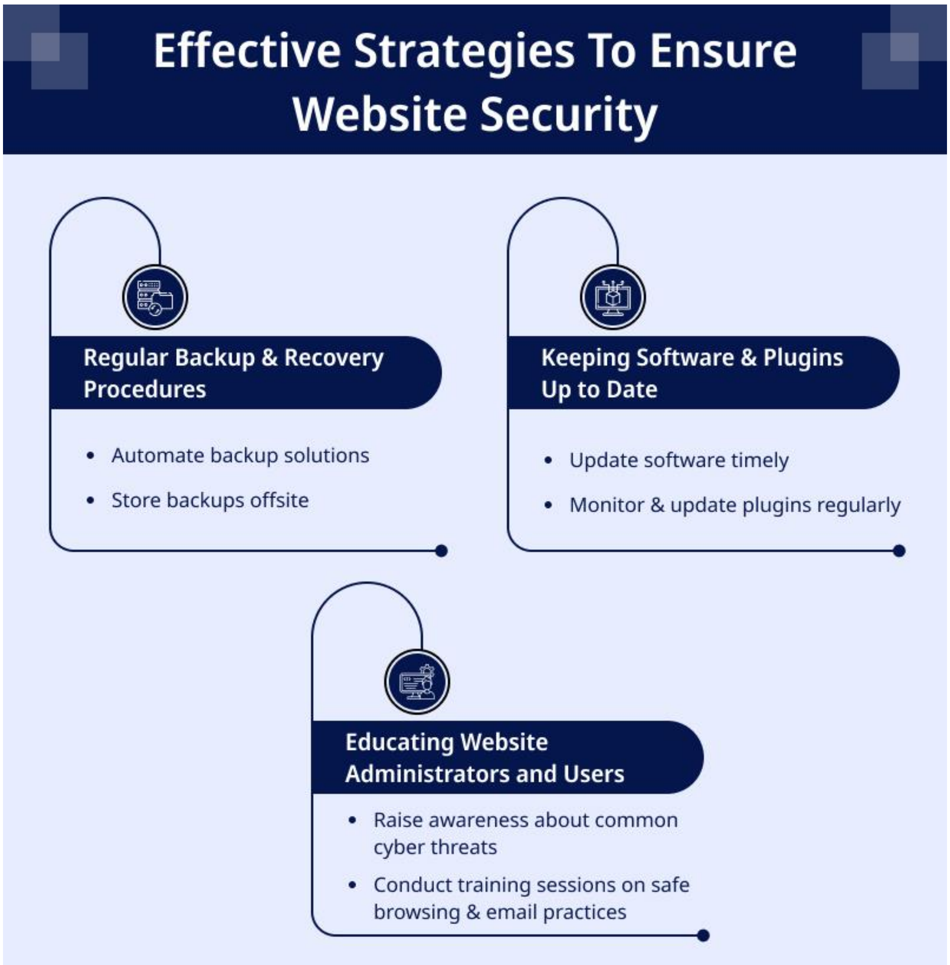
Also, BMN should use dynamic and engaging training methods including workshops, simulations, and hands-on exercises to reinforce learning and improve information retention. By delivering practical, real-world scenarios and chances for active participation, BMN may increase employee engagement while also ensuring that training content is effectively assimilated.
Beyond that, continual training and professional development opportunities should be provided to staff at all levels of the business, allowing them to stay current on developing threats, emerging technologies, and best practices in information security. This may include access to online courses, certifications, and industry conferences, as well as mentorship programs and peer-to-peer learning initiatives.

By investing in comprehensive employee training programs, BMN can equip its workforce with the skills, knowledge, and confidence necessary to effectively safeguard sensitive information, mitigate cyber risks, and contribute to the overall resilience of the organization's information security program. Additionally, fostering a culture of continuous learning and professional development can enhance employee satisfaction, retention, and organizational effectiveness, ultimately positioning BMN as a leader in information security excellence.

2. Enhance Website Security Measures:

BMN's website serves as a critical touchpoint for engaging with stakeholders, promoting its services, and facilitating business transactions.

However, the presence of security errors on the website introduces significant risks to the organization's reputation, financial stability, and regulatory compliance. To address this vulnerability effectively, BMN should prioritize the enhancement of website security measures to safeguard against cyber threats and unauthorized access attempts.



Effective Strategies To Ensure Website Security

Regular Backup & Recovery Procedures

- Automate backup solutions
- Store backups offsite

Keeping Software & Plugins Up to Date

- Update software timely
- Monitor & update plugins regularly

Educating Website Administrators and Users

- Raise awareness about common cyber threats
- Conduct training sessions on safe browsing & email practices

**Figure 6 –** Effective Strategies to Ensure Website Security.

Retrieved from: https://www.valuecoders.com/blog/software-engineering/shield-your-website-from-cyber-threats-with-web-security/

First and foremost, BMN should conduct regular security audits and vulnerability assessments to identify and remediate any weaknesses or vulnerabilities present in its website infrastructure. These assessments should involve comprehensive scans of web applications, servers, and network infrastructure to identify potential security flaws, misconfigurations, or outdated software that could be exploited by malicious actors. By proactively identifying and addressing security issues, BMN can reduce the risk of data breaches, website defacement, and other cyber attacks.

In addition to regular assessments, BMN should consider implementing penetration testing, also known as ethical hacking, to simulate real-world cyber attacks and assess the effectiveness of existing security controls. Penetration testing involves authorized security professionals attempting to exploit vulnerabilities in the website's defenses to identify weaknesses and assess the organization's ability to detect and respond to security incidents. By conducting penetration tests regularly, BMN can identify and address security gaps before they can be exploited by malicious attackers.

Furthermore, BMN should prioritize the adoption of industry-standard encryption protocols, such as HTTPS, to ensure the confidentiality and integrity of data transmitted between users and the website. HTTPS encrypts data in transit, protecting it from interception and unauthorized access by third parties. Additionally, implementing secure coding practices, such as input validation, output encoding, and proper error handling, can help prevent common web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), and remote code execution.

Moreover, deploying web application firewalls (WAFs) can provide an additional layer of defense against cyber threats by filtering and monitoring incoming web traffic for malicious activity. WAFs can help detect and block suspicious requests, protect against known vulnerabilities, and provide granular control over access to sensitive resources. By implementing a WAF, BMN can enhance the resilience of its website and mitigate the risk of common web-based attacks.

Overall, enhancing website security measures is essential for safeguarding BMN's online presence, protecting sensitive information, and preserving stakeholder trust. By prioritizing regular security assessments, adopting encryption protocols, implementing secure coding practices, and deploying web application firewalls, BMN can strengthen its website's defenses against cyber threats and demonstrate its commitment to information security excellence.

3. Establish a Strong Social Media Presence: Establishing a strong social media presence is not only crucial for brand visibility and engagement but also plays a significant role in information security management for BMN. With the increasing prevalence of cyber threats and data breaches, organizations must effectively communicate their commitment to security and build trust with their audience through digital channels.

One way BMN can leverage social media in the context of information security is by sharing educational content, industry insights, and best practices related to cybersecurity. By disseminating timely information about emerging threats, security trends, and protective measures, BMN can raise awareness among its audience and empower them to make informed decisions about their online security posture. This proactive approach not only positions BMN as a thought leader in the field but also fosters a community of security-conscious individuals who are more resilient to cyber attacks.

Moreover, social media platforms provide BMN with an opportunity to engage directly with its audience and address their concerns or inquiries about information security. By actively monitoring social media channels for mentions, messages, and comments related to security issues, BMN can demonstrate responsiveness and transparency in handling security-related matters. This real-time interaction not only enhances customer satisfaction but also helps BMN identify potential security incidents or vulnerabilities early on, allowing for prompt remediation and risk mitigation.

Additionally, BMN can use social media as a platform to promote its security initiatives, certifications, and compliance efforts to reassure clients, partners, and stakeholders about its commitment to information security. By highlighting its adherence to industry standards, regulatory requirements, and best practices, BMN can instill confidence in its audience and differentiate itself from competitors in the market. This can be particularly impactful in industries where trust and credibility are paramount, such as finance, healthcare, and government sectors.

Furthermore, active participation in relevant online communities, industry forums, and cybersecurity events can help BMN expand its network, forge partnerships, and stay abreast of the latest developments in information security. By engaging with like-minded professionals, sharing insights, and collaborating on security-related projects, BMN can enhance its industry presence and influence while gaining valuable knowledge and expertise to inform its security strategies and initiatives.

4. Foster a Culture of Security Awareness:

Fostering a risk-conscious culture is critical for BMN to improve its information security management processes and reduce the risk of data breaches and cyber threats. While technology solutions are critical for protecting digital assets, human behavior remains an important aspect in an organization's overall security posture. As a result, BMN must prioritize efforts to educate and empower its staff to identify, prevent, and respond to threats to security efficiently.

One key aspect of cultivating a strong security culture is through ongoing security awareness training programs. These programs should cover a wide range of topics, including common cyber threats, phishing attacks, social engineering techniques, password hygiene, and data handling best practices. By providing employees with the knowledge and skills needed to identify potential security threats and adopt secure behaviors, BMN can significantly reduce the likelihood of security incidents stemming from human error or negligence.

Regular communication of security policies and procedures is another essential component of building a security-aware workforce. BMN should ensure that its employees are familiar with the organization's security policies, including acceptable use policies, data classification guidelines, incident response procedures, and reporting protocols. Clear and concise communication of these policies through employee handbooks, training materials, email communications, and internal portals helps reinforce expectations and accountability regarding information security responsibilities.

Moreover, BMN should establish reporting channels for employees to report suspected security incidents or breaches promptly. Employees should feel empowered to raise concerns or report unusual activities without fear of reprisal. By creating a culture of openness and transparency, BMN can encourage timely reporting of security incidents, enabling the organization to respond quickly and mitigate potential damage to its information assets.

In addition to formal training and communication efforts, BMN can raise security awareness through a variety of initiatives, including cybersecurity awareness campaigns, interactive workshops, simulated phishing exercises, and employee recognition programs for outstanding security practices. These efforts not only involve employees in the security awareness process, but they also foster a sense of collective responsibility for safeguarding sensitive information and achieving the organization's security goals.

Finally, by instilling a security culture in its personnel, BMN can transform them into proactive defenders of information security, increasing the organization's resistance to cyber threats and protecting the confidentiality, integrity, and availability of its data assets.

Through continuous education, communication, and reinforcement, BMN can cultivate a security-conscious workforce capable of effectively addressing the evolving challenges of the digital landscape.

5. Implement Continuous Monitoring and Improvement:

Implementing continuous monitoring and improvement processes is essential for BMN to stay ahead of emerging cyber threats and maintain a robust information security posture. Continuous monitoring involves the ongoing surveillance of the organization's IT infrastructure, networks, and digital assets to detect and respond to security incidents in real-time. By deploying advanced threat detection technologies, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) solutions, BMN can proactively identify and mitigate potential security breaches before they escalate into full-blown attacks.

Furthermore, BMN should establish a comprehensive incident response readiness program to ensure swift and effective responses to security incidents when they occur. This includes defining incident response procedures, establishing incident response teams, and conducting regular tabletop exercises and simulations to test the organization's incident response capabilities. By practicing coordinated incident response protocols, BMN can minimize the impact of security breaches, contain incidents, and prevent further damage to its information assets and reputation.

Performance metrics tracking is another critical aspect of continuous monitoring and improvement for information security management at BMN. BMN should define key performance indicators (KPIs) and metrics to measure the effectiveness of its information security program and track progress over time. These metrics may include indicators such as the number of security incidents detected and resolved, average incident response times, compliance with security policies and regulations, and employee awareness and training completion rates. In addition to these metrics, BMN should also track the following performance indicators related to information security:

Mean Time to Detect (MTTD): This metric measures the average time it takes for BMN to detect security incidents from the moment they occur. A low MTTD indicates efficient detection capabilities, enabling BMN to respond promptly to security threats and minimize their impact.

Mean Time to Respond (MTTR): MTTR measures the average time it takes for BMN to respond to and resolve security incidents once they have been detected. A low MTTR indicates effective incident response processes and the ability to contain and mitigate security breaches quickly.

Security Incident Severity Levels: Classifying security incidents based on their severity levels allows BMN to prioritize response efforts and allocate resources accordingly. Severity levels can range from low-risk incidents with minimal impact to high-risk incidents that pose a significant threat to the organization's operations and data.

Compliance Adherence Score: This metric evaluates BMN's adherence to relevant security standards, regulations, and industry best practices. It assesses the organization's level of compliance with requirements such as GDPR, PCI DSS, ISO/IEC 27001, and other applicable frameworks. Achieving and maintaining high compliance scores demonstrates BMN's commitment to protecting sensitive information and maintaining regulatory compliance.

Phishing Resilience Rate: Phishing attacks remain a prevalent threat to organizations, often exploiting human vulnerabilities to gain unauthorized access to sensitive data. By tracking the phishing resilience rate, BMN can measure the effectiveness of its employee awareness and training programs in identifying and mitigating phishing attempts. A high resilience rate indicates that employees are vigilant and able to recognize and report phishing emails effectively.

Patch Management Effectiveness: Vulnerabilities in software and applications can expose BMN to security risks if left unpatched. Tracking the effectiveness of patch management processes, such as patch deployment times and patch coverage rates, helps BMN ensure that critical security patches are applied promptly to mitigate potential vulnerabilities and reduce the risk of exploitation by attackers.

Security Training Engagement: Monitoring employee engagement with security training programs, including attendance rates, completion rates, and performance on security awareness assessments, provides insight into the effectiveness of BMN's security awareness initiatives. High levels of engagement indicate that employees are actively participating in training activities and are committed to enhancing their cybersecurity knowledge and skills.

These additional metrics provide BMN with comprehensive insights into its information security program's performance, enabling proactive decision-making and continuous improvement efforts in safeguarding sensitive information assets from evolving cyber threats.

Besides, BMN should conduct frequent security assessments, audits, and reviews to determine the efficacy of its security controls, policies, and processes. Vulnerability assessments, penetration testing, compliance audits, and security architecture reviews are examples of assessments used to discover flaws and areas of noncompliance. By conducting thorough assessments and acting on the results, BMN may close security gaps, mitigate vulnerabilities, and improve its overall security posture.

Finally, by adopting continuous monitoring and improvement processes, BMN can successfully respond to the changing threat landscape, develop its cyber defenses, and keep the trust and confidence of its stakeholders.

Through proactive surveillance, incident response readiness, performance metrics tracking, and regular assessments, BMN can uphold its commitment to information security excellence and safeguard its valuable data assets from potential threats and breaches.

### 3.2. Current State and Proposals for IT Management and Information Security

In the modern digital world, IT management and information security are immersed in a fluid and daunting environment, with an onslaught of cyber threats that is constant and ever-changing. Navigating this difficult landscape requires leveraging insights gained from the most recent research endeavors and in-depth analysis, such as those contained in the Microsoft Digital Defense Report. At the heart of the issue is a multidimensional landscape riddled with numerous issues, each presenting its own unique set of barriers to successful IT management and information security. One of the most significant of these concerns is the increasing sophistication of cyber attacks.

Cybercriminals, equipped with cutting-edge tactics and technologies, continuously devise novel methods to infiltrate systems, perpetrate malicious activities, and wreak havoc on organizational infrastructure.

Moreover, the efficacy of traditional defense measures is increasingly called into question in the face of these evolving threats. Despite the proliferation of cybersecurity solutions and frameworks, many organizations struggle to implement and maintain robust defenses capable of withstanding sophisticated cyber assaults. This gap between available security tools and their effective utilization underscores the pressing need for a paradigm shift in cybersecurity strategies.

Current Challenges

The contemporary IT environment grapples with a myriad of challenges stemming from the pervasive and ever-evolving nature of cyber threats. These challenges, which permeate across various sectors and industries, encompass:

1. Sophisticated Cyber Attacks**:** Sophisticated cyber attacks represent a formidable challenge for organizations across industries, driven by the relentless innovation and adaptation of cybercriminals. One prominent example is ransomware, a type of malware that encrypts files or systems, rendering them inaccessible until a ransom is paid. Ransomware attacks have become increasingly prevalent and sophisticated, with cybercriminals employing tactics such as double extortion, where they not only encrypt data but also threaten to leak sensitive information if the ransom demands are not met.

In addition to ransomware, organizations must contend with advanced persistent threats (APTs), which are stealthy and prolonged cyber attacks orchestrated by highly skilled adversaries. APT actors often target specific organizations or industries, conducting extensive reconnaissance and employing sophisticated techniques to infiltrate networks, evade detection, and exfiltrate valuable data over an extended period. These attacks can have far-reaching consequences, compromising sensitive information, disrupting operations, and causing significant financial and reputational damage.

To combat the growing threat posed by sophisticated cyber attacks, organizations must adopt a proactive and multi-layered approach to cybersecurity. This includes implementing robust perimeter defenses, such as firewalls and intrusion detection systems, to detect and prevent unauthorized access to network resources. Moreover, organizations should invest in endpoint security solutions, such as antivirus software and endpoint detection and response (EDR) systems, to protect individual devices from malware and other malicious activities.

Additionally, increasing employee knowledge and training is critical for reducing the likelihood of successful cyber attacks. Human mistake remains a significant contributor to security breaches, as hackers frequently exploit weaknesses discovered through phishing attacks or social engineering approaches. Organizations may dramatically minimize the likelihood of successful attacks by teaching staff on cybersecurity best practices, as well as identifying and reporting suspicious activity.

*Table 1.3 - Current State of IT Security Challenges*

| Challenge | Description | Statistical Data Reference | Mitigation Strategies |
|---|---|---|---|
| Sophisticated Cyberattacks | - Evolving cyber threats (Ransomware, APTs) | - Ransomware: Sophos reports a 13% increase in attacks from 2022 to 2023 [3]. | - Robust perimeter defenses (firewalls) - Endpoint security solutions (EDR) - Security awareness training |
| Data Breaches | - Accidental or malicious exposure of sensitive information | - IBM: The average cost of a data breach in 2023 is estimated at $4.35 million (https://www.ibm.com/reports/data-breach) | - Data encryption - Access controls - Incident response planning |
| Skills | - Lack of | - (ISC)²: Cybersecurity | - Increased investment |

| | | | |
|---|---|---|---|
| Shortage | qualified cybersecurity professionals | workforce gap is projected to reach 3.4 million by 2024 (https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap) | in cybersecurity education and training - Collaboration with academic institutions |
| Cloud Security | - Growing adoption of cloud computing introduces new security challenges | - Gartner: By 2025, 99% of security breaches will be the customer's fault, not the cloud provider's (https://www.gartner.com/en/cybersecurity/topics/cloud-security) | - Cloud security posture management (CSPM) - Secure coding practices - Regular security assessments |
| Legacy Systems | - Outdated systems with known vulnerabilities | - Help Net Security: Legacy systems are a major target for cyberattacks due to unpatched vulnerabilities (https://sync-sys.com/5-ways-your-legacy-systems-may-add-to-cybersecurity-risks/) | - System modernization - Risk mitigation strategies for legacy systems - Prioritization for patching |

Source: created by author, based on the information, received from the sources, that are in references. (Links are in the table too).

This table summarizes the key challenges facing IT management and information security in 2024, along with statistical data references, mitigation strategies, and relevant sources. It provides a snapshot of the evolving cybersecurity landscape and highlights areas where organizations can focus their efforts to improve their security posture.

In overall, sophisticated cyber attacks pose a persistent and evolving danger to organizational security and stability. Organizations may effectively limit the risk presented by these attacks and preserve their assets and operations by understanding cybercriminals' methods and approaches, deploying strong defense mechanisms, and cultivating a cybersecurity culture.

2. Insufficient Cyber Defense Measures:

Despite notable advancements in cybersecurity technologies, many organizations continue to struggle with the implementation of robust defense measures. The prevalence of insufficient cyber defense measures underscores the persistent challenges that organizations face in effectively safeguarding their digital assets against evolving threats. Several factors contribute to this vulnerability, including the complexity of IT environments, resource constraints, lack of awareness and expertise, and dependency on legacy systems.

Addressing the issue of insufficient cyber defense measures requires a multifaceted approach. Organizations should conduct regular risk assessments to identify and prioritize potential threats and vulnerabilities across their IT infrastructure. By understanding their unique risk profile, organizations can allocate resources more effectively and implement targeted security measures to mitigate identified risks.

Investment in cybersecurity education and training initiatives plays a critical role in enhancing cybersecurity awareness among employees at all levels of the organization. Providing employees with the knowledge and skills to recognize and respond to cyber threats can significantly reduce the likelihood of successful attacks stemming from human error or negligence.

Integrating security-by-design principles into the development and procurement of IT systems and applications can help organizations build security into their digital infrastructure from the outset. By considering security requirements and implications throughout the development lifecycle, organizations can minimize the risk of vulnerabilities and ensure that security is an inherent component of their technology stack.

Collaboration among organizations, government agencies, and cybersecurity vendors is essential for addressing the complex and evolving nature of cyber threats. Sharing threat intelligence, best practices, and resources can help organizations strengthen their cyber defense capabilities and respond more effectively to emerging threats.

3. Underutilization of Security Features**:** Despite the availability of advanced security features and tools, a considerable proportion of organizations fail to leverage them effectively. Microsoft's research highlights the underutilization of essential security features such as multi-factor authentication (MFA), which represents a critical line of defense against unauthorized access and credential-based attacks. Failure to implement such security measures significantly heightens the risk of successful cyber intrusions and compromises.

To address the underutilization of security features like MFA, organizations must prioritize cybersecurity awareness and education initiatives. Decision-makers should understand the benefits of MFA and its role in enhancing overall security posture. Additionally, organizations should seek out user-friendly MFA solutions that integrate seamlessly with existing IT infrastructure and provide clear guidance on implementation and user training.

On top of that, regulatory and industry norms may increasingly compel the usage of MFA as part of compliance frameworks. Compliance-driven programs can encourage firms to use MFA and other critical security measures to meet regulatory obligations and reduce the risk of noncompliance penalties.

Overall, increasing the adoption of security features such as MFA necessitates a combination of education, user-friendly solutions, regulatory incentives, and effective change management tactics. Organizations can improve their cyber defenses and secure sensitive information from unauthorized access and cyber attacks by addressing adoption hurdles and publicizing the benefits of MFA.

What can be improved or changed ?

To address the complex challenges facing IT management and information security, the following proposals are posited for consideration:

1. Comprehensive Cyber Defense Strategies**:** Organizations must have comprehensive and proactive cyber security plans, including threat intelligence, vulnerability management, incident response, and continuous monitoring. Organizations can improve their resilience to a wide range of cyber threats by combining these elements into a unified security system.

2. Threat intelligence is fundamental to any effective cyber defense strategy. This entails obtaining, analyzing, and implementing intelligence on possible and current cyber threats. Organizations can proactively discover vulnerabilities and manage risks by staying up to date on emerging threats, attack vectors, and adversarial techniques. Additionally, threat intelligence enables organizations to prioritize security efforts and allocate resources effectively, focusing on the most pertinent threats.

Vulnerability management is an important component of cyber protection. This includes detecting, assessing, and resolving vulnerabilities in software, hardware, and network infrastructure. Organizations can detect holes before hostile actors exploit them by performing frequent vulnerability assessments and penetration testing. Implementing robust patch management protocols ensures that security patches are applied quickly, decreasing the window of opportunity for attackers to exploit known vulnerabilities.

Despite our greatest efforts to prevent cyber attacks, events may nevertheless occur. As a result, organizations must have strong incident response procedures in place to mitigate the effects of security breaches. Incident response is a concerted effort to detect, respond to, and recover from security incidents. This includes establishing clear escalation procedures, defining roles and responsibilities, and conducting regular incident response drills and simulations to ensure readiness.

A swift and well-executed incident response can mitigate the damage caused by cyber attacks and minimize disruption to business operations.

3. Promotion of Security Best Practices:

One fundamental aspect of security best practices is the implementation of robust access controls. This involves restricting access to sensitive data and critical systems based on the principle of least privilege. By ensuring that users only have access to the resources necessary for their roles, organizations can minimize the potential impact of insider threats and unauthorized access attempts. Additionally, implementing strong authentication mechanisms, such as multi-factor authentication (MFA), adds an extra layer of security by requiring users to provide multiple forms of verification before accessing sensitive information.

Regular Security Assessments: Regular security assessments are essential for identifying vulnerabilities and weaknesses in an organization's infrastructure and applications. These assessments can take various forms, including vulnerability scans, penetration testing, and security audits. By conducting these assessments regularly, organizations can proactively identify and address security gaps before they can be exploited by malicious actors. Furthermore, leveraging automated tools and technologies can streamline the assessment process, allowing organizations to stay ahead of emerging threats and compliance requirements.

Employee Training and Awareness Programs: Human error remains one of the most significant vulnerabilities in cybersecurity. Therefore, organizations must invest in comprehensive employee training and awareness programs to educate staff about potential security risks and best practices. Training programs should cover topics such as phishing awareness, password hygiene, and social engineering tactics. By empowering employees to recognize and report suspicious activities, organizations can significantly reduce the likelihood of successful cyber attacks originating from within the organization.

Adoption of Emerging Technologies: As cyber threats continue to evolve, organizations must embrace emerging technologies to strengthen their security posture. One such technology is the zero-trust security architecture, which operates on the principle of "never trust, always verify." By assuming that every user, device, and network resource is untrustworthy until proven otherwise, zero-trust architectures minimize the risk of lateral movement and privilege escalation in the event of a security breach. Additionally, technologies such as artificial intelligence (AI) and machine learning  can enhance threat detection and response capabilities by analyzing vast amounts of data in real-time and identifying patterns indicative of malicious activity.

Lastly, promoting and implementing security best practices is critical for firms looking to reduce the risk of cyber attacks and secure their digital assets. Organizations may build a strong cybersecurity foundation and protect sensitive information from cyber attacks by implementing rigorous access controls, conducting regular security assessments, investing in staff training and awareness initiatives, and adopting emerging technologies.

4. Collaborative Information Sharing:

Governments have a vested interest in promoting cybersecurity resilience within their jurisdictions and across national borders. To this end, many governments establish information sharing platforms and frameworks that enable public and private sector entities to exchange threat intelligence and cybersecurity best practices. These initiatives often involve partnerships with industry stakeholders, law enforcement agencies, and international cybersecurity organizations to foster a coordinated response to cyber threats.

Industry consortiums and sector-specific organizations also play a vital role in promoting collaborative information sharing. By bringing together companies within the same industry or supply chain, these organizations create forums for sharing threat intelligence, vulnerabilities, and incident response strategies. Additionally, industry consortiums often develop sector-specific best practices and guidelines to address common cybersecurity challenges and enhance collective defense capabilities.

Speaking of organizations, specifically Cybersecurity organizations, such as Computer Emergency Response Teams (CERTs) and Information Sharing and Analysis Centers (ISACs), serve as hubs for collaborative information sharing among stakeholders. These organizations aggregate and analyze threat intelligence from various sources, including government agencies, private sector partners, and international entities, to identify emerging threats and disseminate actionable

insights to their members. By participating in these information sharing networks, organizations gain access to timely and relevant threat intelligence, enabling them to better understand the evolving threat landscape and strengthen their cyber defenses accordingly.

What are the benefits of the information sharing?

Well, collaborative information sharing offers several benefits to participating organizations. First and foremost, it enables stakeholders to gain visibility into emerging threats and vulnerabilities that may affect their operations. By sharing information about known threats and attack techniques, organizations can collectively identify and mitigate security risks before they escalate into full-blown cyber incidents. Additionally, collaborative information sharing promotes the adoption of cybersecurity best practices and standards across sectors, fostering a culture of continuous improvement and resilience.

Collaborative information sharing initiatives are essential for promoting collective defense and enhancing cyber resilience in an increasingly interconnected world. By leveraging government initiatives, industry consortiums, and cybersecurity organizations to facilitate the exchange of threat intelligence and best practices, stakeholders can proactively identify and mitigate cyber threats, thereby strengthening overall cybersecurity posture.

And what about training?

Governments, educational institutions, and private enterprises should invest in cybersecurity education and training programs to cultivate a skilled workforce capable of addressing evolving cyber threats. By providing access to specialized training courses, certifications, and hands-on experience, organizations can equip cybersecurity professionals with the knowledge and skills required to defend against sophisticated adversaries effectively.

5. Advancements in Cybersecurity Technologies: AI-driven Threat Detection Systems: Artificial intelligence (AI) and machine learning (ML)

technologies play a pivotal role in modern cybersecurity defenses. AI-driven threat detection systems leverage algorithms to analyze vast amounts of data and identify patterns indicative of malicious activity. These systems can detect previously unseen threats, such as zero-day exploits and polymorphic malware, enabling organizations to respond swiftly to emerging cyber threats.

Behavioral Analytics Platforms: Behavioral analytics platforms monitor user and entity behavior to detect anomalies indicative of potential security breaches. By establishing baselines of normal behavior for users, devices, and applications, these platforms can identify deviations from the norm that may indicate a security incident. Behavioral analytics solutions enable organizations to detect insider threats, credential misuse, and other suspicious activities that traditional security controls may overlook.

Secure-by-design Frameworks: Secure-by-design frameworks promote the integration of security principles and controls throughout the entire software development lifecycle. By incorporating security considerations from the initial design phase, organizations can minimize the risk of introducing vulnerabilities into their systems and applications. Secure coding practices, threat modeling, and automated security testing are key components of secure-by-design frameworks, ensuring that security is an integral part of software development processes.

Encryption Technologies: Encryption technologies are crucial in protecting sensitive data from illegal access and interception. End-to-end encryption, data-at-rest encryption, and transport layer security (TLS) encryption are prominent methods for protecting data in transit and at rest. Furthermore, advances in quantum-resistant encryption aim to protect cryptographic methods from new risks posed by quantum computing.

Benefits of Cybersecurity Technological Advancements: The continual advancement of cybersecurity technologies offers numerous benefits to organizations seeking to bolster their cyber defenses. AI-driven threat detection systems enable organizations to detect and respond to cyber threats in real-time, reducing the time to detect and mitigate security incidents. Behavioral analytics platforms provide insight into user behavior, helping organizations identify and mitigate insider threats and advanced persistent threats. Secure-by-design frameworks promote the development of secure software and applications, reducing the likelihood of security vulnerabilities. Encryption technologies safeguard sensitive data from unauthorized access, ensuring confidentiality and integrity.

In short, developments in cybersecurity technology are critical for improving enterprises' ability to protect against growing cyber threats. Businesses may increase their cyber defenses and reduce the risk of cyber assaults by implementing AI-driven threat detection systems, behavioral analytics platforms, secure-by-design frameworks, and encryption technologies.

6. Regulatory Measures**:** Regulatory measures encourage firms to emphasize cybersecurity and compliance. As cyber dangers advance and represent substantial risks to organizations and individuals alike, governments throughout the world are progressively creating and enforcing strong legislation to address these issues. These legislation frequently contain obligatory reporting requirements for cyber incidents, requiring firms to promptly disclose any breaches or security incidents to appropriate authorities and affected individuals.

Additionally, governments establish cybersecurity standards and frameworks to guide organizations in developing and implementing effective security measures. Compliance with these standards helps organizations strengthen their security posture, identify vulnerabilities, and implement best practices to mitigate the risk of cyber attacks. Moreover, regulatory measures may involve the enforcement of penalties for non-compliance, such as fines, legal actions, or sanctions. This proactive approach not only helps prevent cyber attacks but also enables timely detection and response to security incidents, minimizing their impact on individuals, businesses, and critical infrastructure. Ultimately, these regulatory efforts contribute to safeguarding sensitive information, protecting digital assets, and upholding trust and confidence in digital ecosystems.

# CONCLUSION

In conclusion, the combination of insights from the three chapters emphasizes the importance of strong information security measures and Business Media Network (BMN) methods in today's digital landscape. The increasing sophistication of cyber attacks needs comprehensive cybersecurity frameworks that include threat intelligence, vulnerability management, incident response, and ongoing monitoring. These defense measures are critical in strengthening organizational resilience against various cyber threats while also preserving the integrity and reliability of digital infrastructures. Furthermore, promoting security best practices, collaborative information sharing initiatives, and technological breakthroughs in cybersecurity are critical components of efficient information security management. Organizations can reduce risks and improve their ability to identify, prevent, and respond to cyber threats by developing a cybersecurity awareness and vigilance culture.

The implementation of BMN strategies is paramount in effectively navigating the dynamic and rapidly evolving digital business landscape, especially amidst the ever-present threat of cyber attacks. In today's interconnected and technology-driven world, organizations face constant pressure to adapt their business models to stay relevant, competitive, and secure. This necessitates a proactive approach to managing risks, seizing emerging opportunities, and maintaining agility in response to market shifts and technological advancements.

To successfully navigate the digital business landscape, organizations must prioritize agile decision-making and strategic foresight. This entails the ability to quickly assess changing market dynamics, identify potential disruptions, and make informed decisions to capitalize on emerging trends or mitigate risks. By embracing a proactive approach to business model adaptation, organizations can stay ahead of the curve and position themselves for sustained success in the digital era.

Also, strong BMN depends on the use of digital technology to improve operational efficiency and value proposition. Embracing cutting-edge technologies like artificial intelligence, data analytics, cloud computing, and the Internet of Things, or IoT for short, allows businesses to streamline processes, increase productivity, and provide better consumer experiences. Organizations that leverage the power of digital transformation can open up new revenue sources, broaden their market reach, and create long-term success.

Furthermore, BMN enables companies to capitalize on market trends and consumer preferences by constantly monitoring industry developments and modifying their business models accordingly. This proactive approach enables firms to anticipate changes in customer behavior, industry rules, and competitive landscapes, allowing them to remain flexible and adaptable to changing market situations. Organizations can establish themselves as industry leaders and gain long-term competitive advantages by aligning their business models with changing market trends.

In general, BMN strategies must be implemented not just for navigating the intricacies of the digital business ecosystem, but also to ensure long-term resilience and competitiveness. Organizations that embrace agility, innovation, and proactive adaptation may prosper in a more turbulent and uncertain business environment, enabling long-term growth and value creation.

In the quickly changing digital ecosystem, the synergy between strong information security management and strategic practices is essential for safeguarding organizational assets, ensuring business continuity, and promoting long-term success. Organizations face a multitude of issues in today's dynamic and linked digital economy, from market disruptions to cyber attacks. To effectively reduce risks, capitalize on new opportunities, and foster a culture of resilience and innovation, businesses must place a high priority on continual innovation, collaboration, and adaptability.

To thrive in the digital era, organizations must adopt a holistic approach that integrates information security measures seamlessly into their overarching business strategies. By aligning information security initiatives with BMN principles, organizations can proactively identify and address potential vulnerabilities, ensuring the protection of sensitive data and critical assets. Moreover, strategic BMN practices enable organizations to anticipate market shifts, technological advancements, and regulatory changes, allowing them to pivot swiftly and capitalize on emerging trends.

Furthermore, fostering a culture of innovation and collaboration is essential for driving organizational agility and responsiveness in the face of evolving threats and opportunities. By encouraging cross-functional collaboration and empowering employees to contribute ideas and insights, organizations can leverage collective intelligence to identify innovative solutions and adapt to changing circumstances effectively. Additionally, promoting a culture of resilience and adaptability enables organizations to navigate uncertainties with confidence, turning challenges into opportunities for growth and differentiation.

Lastly, the integration of effective information security management and strategic techniques is critical for companies seeking to succeed in today's digital landscape. Organizations that embrace innovation, collaboration, and adaptability can improve their cyber resilience, promote sustainable growth, and position themselves for long-term success in an increasingly complex and interconnected business environment.

## REFERENCES

1. Kidd, D. (2023). Cybersecurity defense in depth: Layered strategies for comprehensive protection. URL: https://www.linkedin.com/pulse/cybersecurity-defense-depth-layered-strategies-protection-david-kidd

2.Cybersecurity FAQs. (2024). URL: https://learnq.co.uk/faqs/business-compliance/cybersecurity

3. InterviewPrep Career Coach. (2023). Information systems security officer interview-questions.
URL: https://interviewprep.org/information-systems-security-officer-interview-questions/

4. Norris, S. (2023). 10 essential steps to handle cyber security incidents. URL: https://digitalsecurityworld.com/how-to-handle-cyber-security-incidents/

5. InterviewPrep Career Coach. (2023). 30 information security specialist interview questions and answers. URL: https://interviewprep.org/information-security-specialist-interview-questions/

6.Valency Networks.(2013). Mobile app security testing.
URL:https://www.valencynetworks.com/penetration-testing-services/mobile-app-testing/mobile-app-testing-process.html

7. FasterCapital. (2024). How to comply with the relevant laws and regulations and maintain professional standards and ethics.
URL: https://fastercapital.com/topics/how-to-comply-with-the-relevant-laws-and-regulations-and-maintain-professional-standards-and-ethics.html

8. Antonenko, D. (2023). Enhancing security: Establishing secure remote site network-connections.
URL: https://www.businesstechweekly.com/cybersecurity/data-security/secure-network-connection-at-a-remote-site/

9. Packetlabs Pty Ltd. (2023). Understanding zero-day exploits: The emerging cybersecurity-threat. URL:https://www.linkedin.com/pulse/understanding-zero-day-exploits-emerging-cybersecurity-threat

10. Norris, S. (2023). Test your cyber security knowledge. URL:https://digitalsecurityworld.com/cyber-security-quiz-for-students/

11. Shdow-Security. (2023). Creating a comprehensive electronic security strategy. URL:http://www.shdowsecurity.com/2023/05/23/c-2/

12. FasterCapital. (2024). Comprehensive employee training programs. URL:https://fastercapital.com/keyword/comprehensive-employee-training-programs.html

13.BusinessTechWeekly.(2023).URL:https://www.businesstechweekly.com/cybersecurity/data-security/cyber-security-by-design/

14. Khan, T. (2024). Simplifying cloud computing compliance: Key strategies. URL:https://informationsecuritybuzz.com/cloud-computing-compliance-strategies/

15. Antonenko, D. (2023). Implementing access control best practices. URL:https://www.businesstechweekly.com/cybersecurity/password-security/access-control-best-practices/

16. Ziolkowski, K. (2013). Peacetime regime for state activities in cyberspace. URL:https://cryptome.org/2014/01/nato-peacetime-cyberspace.pdf

17. Agrawal, R. (2023). The vital role of technology in e-commerce security. URL:https://remotestate.com/blogs/the-vital-role-of-technology-in-e-commerce-Security

18. PrivacySense.net. (2023). General data protection regulation. URL:https://www.privacysense.net/terms/gdpr/

19. DigiALERT. (2023). Cyber security attacks prediction of 2024. URL:https://www.linkedin.com/pulse/cyber-security-attacks-prediction-2024-digialert

20. Acronis. (2018). What is data security and how does it work?. URL:https://www.acronis.com/en-us/blog/posts/data-security/

21. Equivioasm. (2023). Security layers: Best way to keep your data safe. URL:https://avexir.com/security-layers/

22. Sameer, H. (2023). Securing Docker registries: Safeguarding containerized environments.

URL:https://www.linkedin.com/posts/hasansameer_docker-security-tech-activity-7071009941775409152-VJ4F

23. Sharma, S. (2023). How to prevent broken access control?. URL:https://www.tutorialspoint.com/how-to-prevent-broken-access-control

24. Securium Solutions. (2023). Endpoint detection and response. URL:https://securiumsolutions.com/blogs/define-endpoint-detection-response/

25.OWASP.(2023).Secure product design. URL:https://cheatsheetseries.owasp.org/cheatsheets/Secure_Product_Design_Cheat_Sheet.html

26. Ijlal, T., Dutta, T., & Jain, A. (2024). What are the best techniques for managing cloud access control? URL:https://www.linkedin.com/advice/3/what-best-techniques-managing-cloud-access-control-4awlf

27. AI for Social Good. (2023). Artificial intelligence's revolutionary impact on cyber security. URL:https://aiforsocialgood.ca/blog/artificial-intelligences-revolutionary-impact-on-cyber-security

28. Kravcuk, O., Varis, I., & Dorosh, M. (2021). The effects of budgeting for human resource management in global socio-economic changes' conditions. URL:https://economyandsociety.in.ua/index.php/journal/user/setLocale/en_US?source=%2Findex.php%2Fjournal%2Farticle%2Fview%2F769

29. Anant, V., Donchak, L., Kaplan, J., & Henning, D. (2020). The consumer-data opportunity and the privacy imperative. URL:https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

30. Dzhekishev, B. (2023). Big data security best practices. URL:https://maddevs.io/blog/big-data-security-best-practices/

31. Frontegg. (2024). Access control in security: Methods and best practices URL:. Retrieved from https://frontegg.com/guides/access-control-in-security

32. InterviewPrep Career Coach. (2023). Security analyst interview. URL:https://interviewprep.org/junior-security-analyst-interview-questions/

33. Antonenko, D. (2023). Understanding Microsoft identity and access management.

URL:https://www.businesstechweekly.com/cybersecurity/passwordsecurity/microsoft-identity-and-access-management/

34. Deloitte Malaysia. (2020). 91 percent of all cyber attacks begin with a phishing email to an unexpected victim.

URL: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

35. Tessian (2023). Examples of Social Engineering Attacks.

URL:https://www.tessian.com/blog/examples-of-social-engineering-attacks/

36. CompTIA (2016). Internet of Things insights and opportunities.

URL: https://www.comptia.org/content/research/internet-of-things-insights-and-opportunities

37. Mitre. (2023). DevSecOps practices.

URL: https://www.mitre.org/news-insights/publication/devsecops-security-and-test-automation-briefing

38. Cloud Security Alliance. (2023). Cloud Threat Landscape Report 2023. URL: https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning

39. Palo Alto Networks. (2023). Unit 42 Threat Report.

URL: https://unit42.paloaltonetworks.com/

40. ReliaQuest. (2022). Ransomware Report: Q4 2022.

URL:https://www.reliaquest.com/blog/q4-2023-ransomware/

41. Gartner. (2022, June 06). Gartner Security & Risk Management Summit 2022. URL https://www.gartner.com/en/conferences/na/security-risk-management-us

42. CISA. (2022, August 09). Stop Ransomware. CISA (.gov). URL: https://www.cisa.gov/stopransomware/ransomware-101

43. Sophos. (2023, February 21). The State of Ransomware 2023. Sophos. URL:https://www.sophos.com/en-us/content/state-of-ransomware

44. National Institute of Standards and Technology. (2023, September 17). Special Publication 800-30 Revision 1. National Institute of Standards and Technology (.gov). URL:https://www.nist.gov/privacy-framework/nist-sp-800-30

45. SANS Institute. (2023). SANS Institute Information Security Training. SANS Institute. URL:https://www.sans.org/

46. (ISC²). (2023, May 25). (ISC)² Cybersecurity Research. (ISC²). URL:https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap

47. CompTIA. (2023, May 18). CompTIA Security Jobs. CompTIA. URL:https://www.comptia.org/faq/security/what-jobs-can-i-get-with-comptia-security-certification

48. Gartner. (2022). Cloud Security.
URL:https://www.gartner.com/en/cybersecurity/topics/cloud-security

49. Help Net Security. (2023). Legacy Systems Security Challenges. Help Net Security.
URL:https://sync-sys.com/5-ways-your-legacy-systems-may-add-to-cybersecurity-risks/