Title: Strengthening Cyber Security in Modern Organizations: Threats, Vulnerabilities, and Evidence-Based Mitigation Strategies

Student Name:

Course:

Instructor:

Date:

ABSTRACT

Cyber security is now a core requirement for organizations because critical services, financial operations, and personal data increasingly depend on information systems and connected devices. This paper explains key cyber security concepts and evaluates major security risks that drive today's cyberattacks, including phishing, compromised credentials, exploited vulnerabilities, and supply chain exposures. Using current, credible guidance and research-based reporting, the paper analyzes how attackers achieve intrusion and data breaches, why defenses fail, and what controls best reduce risk. The discussion emphasizes governance, security architecture, threat detection, incident response, and practical prevention measures that safeguard sensitive data and critical infrastructure. The paper concludes with actionable recommendations aligned to recognized frameworks that organizations of different sizes can implement to improve resilience and reduce the likelihood and impact of malicious activity.

Introduction

Cyber security (also written as cyber security) refers to protecting information systems from unauthorized access, intrusion, disruption, and theft. Organizations face expanding security threats because they store a growing amount of data across cloud platforms, employee endpoints, and the Internet of Things, increasing potential vulnerabilities. Cybercriminals exploit technical weaknesses and human behavior to conduct cyberattacks that can lead to data breaches, financial loss, operational shutdowns, and reputational damage. The purpose of this term paper is to explain foundational concepts, describe the current threat landscape, and propose practical mitigation strategies that reduce risk in real organizational environments.

1. Foundational Terms in Cyber Security and Information Security

Information security focuses on protecting information confidentiality, integrity, and availability, while cyber security often emphasizes protecting digital systems, networks, and connected devices from malicious activity. In practice, these areas overlap because modern organizations depend on information technology architecture and information systems to deliver services (NIST, 2024a). Key terms include threat (a potential cause of harm), vulnerability (a weakness), exploit (a method that takes advantage of a vulnerability), intrusion (unauthorized entry), and data breach (unauthorized exposure or theft of sensitive data). Defining these concepts early improves clarity and allows a paper to link problems to controls in a structured way.

2. Why Cyberattacks Work: The Attack Chain and Common Intrusion Paths

Many incidents follow a predictable chain: attackers obtain initial access, expand privileges, move laterally, and then steal data or disrupt operations. Initial access frequently occurs through stolen credentials, phishing, or exploitation of vulnerabilities, after which attackers can maintain persistence and avoid detection. This progression matters because defenses must be layered; stopping one step in the chain can prevent a full-scale incident

(Verizon, 2025). Research-based breach reporting consistently shows that credential misuse and phishing remain high-frequency pathways into organizations, which means basic access controls and authentication discipline are still central to prevention.

3. Current Threat Landscape: What Organizations Face Today

The modern threat landscape includes financially motivated cybercriminals, state-linked actors targeting critical infrastructure, and opportunistic attackers seeking vulnerable systems. Common threats include ransomware, data attacks, and availability attacks that disrupt operations. These issues are not limited to one region or industry; they affect organizations worldwide, with impacts shaped by the value of systems, the sensitivity of data, and the maturity of security programs (European Union Agency for Cybersecurity [ENISA], 2024). A realistic term paper should acknowledge that cyber threats evolve, and that organizations must continuously adapt controls, monitoring, and training to remain effective.

4. Phishing, Credential Theft, And Unauthorized Access

Phishing remains effective because it targets human decision-making and access behaviors, often bypassing technical controls by tricking users into sharing credentials or approving fraudulent logins. Once credentials are compromised, attackers can access systems as “legitimate” users, making intrusion harder to detect (Verizon, 2025). Evidence from the 2025 Data Breach Investigations Report highlights that compromised credentials and phishing are repeatedly associated with breaches across multiple industries, underscoring why multi-factor authentication, identity monitoring, and user training are essential baseline controls.

5. Vulnerabilities, Exploits, And the Reality of Patch Gaps

Vulnerability management is difficult because organizations run diverse systems, legacy applications, and third-party tools across hybrid environments. Attackers scan widely for known weaknesses and exploit unpatched systems, misconfigurations, or weak remote access points. Because cyber vulnerabilities can persist for operational reasons, mitigation must

go beyond patching alone to include secure configuration baselines, network segmentation, least-privilege access, and continuous monitoring (ENISA, 2024). A term paper gains credibility when it explains why vulnerability remediation is delayed and how layered controls reduce exposure even when patching is imperfect.

6. Internet Of Things (Iot) And Connected Devices: Expanding the Attack Surface

The Internet of Things includes sensors, cameras, medical devices, industrial controllers, and other connected devices that create new security risks. IoT devices often increase risk due to inconsistent update mechanisms, limited logging, weak default credentials, and unclear ownership between information technology and operational teams. When insecure devices connect to enterprise networks, they can become entry points for intrusion or enable surveillance of organizational activity (NIST, 2024a). Effective mitigation involves asset inventory, network isolation of device classes, secure configuration, and vendor accountability within the organization's broader cyber security governance.

7. Artificial Intelligence (Ai) And Machine Learning in Threat Detection

Artificial intelligence and machine learning can improve threat detection by analyzing large-scale logs, network traffic, and endpoint signals to identify unusual patterns that might indicate malicious activity. At the same time, attackers also use AI to improve phishing realism, automate reconnaissance, and accelerate exploit development, increasing the speed and sophistication of attacks (ENISA, 2024). Therefore, AI should be viewed as an enabler within a defense-in-depth strategy, not a substitute for governance, secure architecture, and human oversight. A strong paper should explain both the promise and the limitations of AI-enabled security controls.

8. Governance And Framework-Aligned Cyber Security Programs

A major reason security programs fail is not only technical weakness but also weak governance, unclear accountability, and inconsistent policy enforcement. The NIST

Cybersecurity Framework 2.0 emphasizes outcomes that help organizations manage cyber security risk through governance, identification, protection, detection, response, and recovery. Framework alignment helps organizations define priorities, communicate risk to leadership, and measure progress over time (NIST, 2024a). For a term paper, connecting recommendations to a recognized framework strengthens academic rigor and shows that mitigation decisions can be organized systematically rather than being a random list of tools.

9. Incident Response, Forensics, And Organizational Resilience

Even well-defended organizations can experience incidents, so preparation for response and recovery is essential. Effective incident response includes establishing roles, documenting procedures, analyzing incident-related data, containing threats, and learning from events to prevent recurrence (NIST, 2012). Digital forensics supports this process by reconstructing attacker activity, identifying compromised assets, and preserving evidence when legal or regulatory actions are required. A credible term paper should treat incident response as a core capability that reduces impact, shortens downtime, and supports transparency and accountability after a breach.

10. Data Protection: Safeguarding Personal Data and Sensitive Data

Data protection requires both technical and administrative safeguards because breaches can expose personal data, regulated records, and proprietary information. Organizations should classify data, enforce access control, encrypt sensitive data at rest and in transit, and monitor for abnormal access patterns (NIST, 2024a). Because modern enterprises depend on cloud services, collaboration platforms, and remote work, data protection strategies should include identity security, secure sharing controls, and continuous auditing. Effective safeguards reduce both the likelihood of theft and the harm caused if attackers gain access.

11. Supply Chains and Third-Party Risk: Where Security Fails Quietly

Supply chain risk grows when organizations depend on third-party software, managed services, and integrated vendors. Attackers can compromise a trusted supplier to reach many downstream organizations, meaning that one vulnerability can scale into a widespread problem. A strong paper should explain that third-party risk is not only contractual; it requires verification through security requirements, due diligence, monitoring, and contingency planning (ENISA, 2024). Because supply chain threats evolve with technology and procurement practices, governance must treat supplier security as part of core systems security rather than an afterthought.

12. Practical Recommendations: How To Mitigate Cyber Security Risks

This paper recommends a layered strategy that combines governance, prevention, detection, and response. First, strengthen access controls through multi-factor authentication, least privilege, and monitoring of credential misuse to reduce unauthorized access. Second, reduce vulnerabilities through patch management, secure configuration, and network segmentation to limit exploit paths. Third, invest in threat detection with centralized logging, endpoint monitoring, and carefully validated AI-enabled analytics to handle the amount of data generated by modern systems (NIST, 2024a). Fourth, build resilience with tested incident response playbooks, backup and recovery plans, and regular exercises. These steps are achievable for many organizations when aligned to a framework and implemented as an ongoing program rather than a one-time project.

Conclusion

Cyber security challenges persist because attackers continuously adapt, organizations operate complex infrastructures, and human behavior remains a frequent access weakness. This term paper has shown that cyberattacks often succeed through phishing, compromised credentials, unpatched vulnerabilities, and supply chain exposures, leading to intrusion and data breaches that harm operations and public trust. Effective mitigation requires a balanced

approach: strong governance, secure architecture, layered controls, evidence-based threat detection, and mature incident response. When organizations prioritize these measures and continuously improve, they can better safeguard sensitive data, support transparency, and reduce the likelihood and impact of malicious activity worldwide.

References

European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

National Institute of Standards and Technology. (2012). Computer security incident handling guide (Special Publication 800-61 Revision 2). https://csrc.nist.gov/pubs/sp/800/61/r2/final

National Institute of Standards and Technology. (2024a). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Verizon. (2025). 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/