Human Factors in Addressing Cybersecurity Incidents

Safae Ali Ait Kassou

Laurea University of Applied Sciences

Human Factors in Addressing Cybersecurity Incidents

Safae Ali Ait Kassou

Safety, Security & Risk Management

Bachelor's Thesis

July, 2025

Laurea University of Applied Sciences
Safety, Security and Risk Management
Bachelor of Business Administration

Safae Ali Ait Kassou

Abstract

Human factors in addressing cybersecurity incidents.

Year 2025 Number of pages 38

Cybersecurity incidents are an escalating global challenge, with human factors remaining the leading cause of breaches despite significant advances in technical defenses. This thesis explores how individual behaviors, organizational practices, and cultural attitudes contribute to cybersecurity vulnerabilities. Through a qualitative approach, the research combines a structured literature review with in-depth analysis of three major case studies—WannaCry, Sony Pictures, and Equifax—to identify recurring patterns of human error, such as weak passwords, insufficient training, and poor communication.

Drawing on established frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001, as well as behavioral models including the Theory of Planned Behavior and Human Error Models, the study demonstrates that technology alone cannot address the full spectrum of cybersecurity risk. The findings reveal that effective resilience depends on integrating human-centered strategies: tailored employee training, simplified security policies, and fostering a robust security culture that aligns with real-world workflows and cognitive limitations.

By emphasizing the interplay between human behavior and technical systems, this thesis offers actionable recommendations for organizations seeking to reduce risk and improve incident response. The research underscores the necessity of treating human factors as a foundational element of cybersecurity, not a supplementary concern. Ultimately, the study contributes to a more balanced and resilient approach to digital security—one that recognizes people as both a source of vulnerability and a critical line of defense.

Keywords: Cybersecurity incidents, Cybersecurity, Human factors, Cybersecurity framework, Cybersecurity awareness.

Table of content

1 Introduction

Cybersecurity incidents have become a critical global concern, with attacks increasing in frequency, scale, and sophistication. Organizations and governments face a rapidly evolving threat landscape, as cyberattacks—from data breaches to ransomware—disrupt essential services and impact millions of individuals worldwide. Despite significant investments in advanced technical safeguards such as firewalls, encryption, and intrusion detection systems, the human factor remains a leading vulnerability. According to the World Economic Forum, a substantial majority of cybersecurity breaches—up to 82% in recent years—are attributable to human elements, including errors, lapses in judgment, and susceptibility to social engineering attacks. (World Economic Forum 2022.)

These findings highlight that technology alone cannot fully address cybersecurity risk, and that empowering individuals through continuous training, fostering a culture of security awareness, and reducing complexity in systems are essential strategies for building true cybersecurity resilience. (World Economic Forum 2024.)

Indeed, human behavior plays a pivotal role in the success or failure of cybersecurity defenses. Mistakes such as clicking on phishing links, using weak passwords, neglecting updates, or failing to follow proper procedures can compromise even the most secure systems. These errors often stem from broader issues such as insufficient training, low awareness, cognitive overload, or the absence of a security-conscious organizational culture. As a result, addressing human error is not merely a supplementary task—it is a core component of building resilient cybersecurity defenses. (Sasse & Flechais 2005.)

This thesis explores the intersection between human factors and cybersecurity incident response. It investigates how individual actions, organizational practices, and cultural attitudes toward security contribute to vulnerabilities within digital environments. Drawing on academic literature, real-world case studies, and international standards like the NIST Cybersecurity Framework and ISO/IEC 27001, the theis seeks to uncover patterns and root causes of human error in cybersecurity incidents to advance a nuanced understanding of the mechanisms by which such incidents arise and persist.

By emphasizing a human-centered approach, the thesis aims to offer actionable insights that organizations can use to enhance both their preventive and responsive cybersecurity measures. Ultimately, the study aimes to contribute to a more balanced understanding of cybersecurity—one that values not only technological advancement but also the critical importance of human behavior in maintaining digital safety.

Perplexity and ChatGPT were used in this thesis to edit the language of the text.

1.1 Research commissioner

The thesis commissioner is Project DYNAMO, an ambitious European initiative aimed at strengthening cybersecurity resilience across critical sectors such as energy, healthcare, and transportation. In response to the growing complexity of cybersecurity threats and the rapid pace of digitalization, DYNAMO seeks to provide innovative solutions that ensure business continuity and mitigate the impact of cybersecurity incidents. By focusing on recovery and resilience, the project addresses one of the most vulnerable aspects of modern infrastructures.

Some of DYNAMO's key achievements and commitments include:

- Expertise in cybersecurity solutions: DYNAMO delivers cutting-edge tools and services that help organizations detect, prevent, and respond to cybersecurity incidents effectively.

- Focus on the human factor: Recognizing that people are often the weakest link in cybersecurity, DYNAMO places strong emphasis on human-centered approaches, offering tailored training programs and awareness campaigns to reduce human error and improve security behavior.

- Collaborative success: DYNAMO has worked with both private companies and public sector institutions, supporting them in improving risk assessments, implementing best practices, and enhancing overall security posture.

- Innovation and research: DYNAMO actively contributes to research and policy development, participating in national and international discussions to shape a safer and more resilient digital environment.

- Commitment to continuous improvement: Through constant innovation and a proactive approach, DYNAMO remains dedicated to staying ahead of evolving cybersecurity threats and sharing its expertise with the broader community.

DYNAMO's mission and values make it a fitting and supportive commissioner for this thesis, which focuses on exploring the human factors behind cybersecurity incidents and identifying practical strategies to strengthen organizational resilience. (DYNAMO 2022.)

1.2 Choice of topic and background

The decision to focus this thesis on human factors in cybersecurity arose from an increasing awareness within the field that technical defenses—while essential—are not sufficient on their own to prevent cybersecurity incidents. Initial discussions with the thesis commissioner highlighted a shared concern: organizations continue to experience significant breaches, not

due to technological failure alone, but because of human behavior. Mistakes such as poor password practices, falling victim to phishing attempts, or neglecting security policies frequently undermine even the most advanced security systems.

As cybersecurity threats grow more sophisticated, understanding the human element behind security failures has become more urgent. This thesis addresses that need by exploring the behavioral and organizational dimensions of cybersecurity, with the aim of identifying how human actions and decision-making processes influence vulnerability. The goal is to support organizations in shifting from purely technology-focused solutions to more balanced approaches that integrate people-centered strategies.

To guide this exploration, the thesis is structured around three key questions:

- What are the primary human factors that contribute to cybersecurity vulnerabilities?
- What lessons can be learned from real-world cybersecurity incidents regarding the impact of human behavior on security breaches and responses?
- What practical, human-centered strategies can organizations implement to reduce cybersecurity risks and improve resilience?

By addressing these questions, the thesis aims to produce recommendations that bridge the gap between theory and practice, offering insights that can help organizations strengthen their cybersecurity posture through both behavioral awareness and improved internal practices.

2 The Importance of Addressing Human Factors in Cybersecurity Frameworks

Human factors play a significant role in cybersecurity risks, often serving as a key contributor to security breaches. Despite advancements in technology, individuals remain integral to the operation and interaction with security systems, making the human element a critical aspect of cybersecurity. However, cybersecurity frameworks frequently emphasize technical measures such as encryption, access controls, and intrusion detection systems, while the human dimension is often underrepresented. This focus creates a gap, as many cybersecurity incidents are rooted in human actions, including falling for phishing attacks, system misconfigurations, or delayed software updates. In 2022 a study conducted by Stanford University Professor Jeff Hancock, in collaboration with the cybersecurity firm Tessian, revealed that employee mistakes account for roughly 88% of data breaches. This highlights that human error continues to be a significant factor behind the majority of cybersecurity issues. (Sjouwerman 2024.)

Cybersecurity frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 provide structured approaches for managing risks, but the inclusion of strategies addressing behavioral and cognitive aspects of human actions can offer a more holistic understanding of security vulnerabilities. For example, human behavior significantly influences the effectiveness of protocols designed to prevent phishing attacks, one of the most common methods of cybersecurity intrusion. Reports, such as Verizon's Data Breach Investigations Report (DBIR)(2024), show that many attacks succeed due to users' lack of awareness or difficulty in identifying fraudulent communications. (Verizon 2024.)

The interplay between humans and systems also highlights the importance of designing security measures that align with cognitive and behavioral patterns. Tasks requiring repetitive actions or complex decision-making processes are often prone to errors, particularly under stress or time pressure. The design and implementation of automated systems, simplified interfaces, and pre-configured security settings are key areas where human interaction with technology significantly influences cybersecurity outcomes. (Verizon 2024).

In addition, the broader organizational context shapes how human factors influence security. Cultural elements, such as the prioritization of cybersecurity, communication practices, and collective attitudes toward security protocols, impact the effectiveness of security frameworks. Research indicates that organizations with a strong focus on cybersecurity culture tend to experience fewer breaches and recover more efficiently when incidents occur. (Spizner 2024.)

By examining how human behavior interacts with technology and organizational practices, cybersecurity frameworks can offer insights into the underlying causes of breaches. This perspective underscores the critical role of human factors in the overall effectiveness of cybersecurity measures and highlights the interconnected nature of technical systems and human behavior in managing security risks.

2.1 Defining Human Factors in Cybersecurity

In the context of cybersecurity, human factors encompass the ways individuals interact with systems and how their decisions, habits, and awareness levels can either introduce vulnerabilities or strengthen defenses. This includes not only personal behaviors but also organizational influences that shape user conduct. These elements are complex and interconnected, involving not just individual actions and mental processes, but also the broader organizational context in which people operate. Even the most sophisticated technical systems can be compromised by human mistakes, carelessness, or intentional

wrongdoing, making the human element one of the most critical—and often most vulnerable—aspects of cybersecurity. (Kraemer, Carayon & Clem 2009.)

At the individual level, human factors involve behaviors such as the use of weak or reused passwords, falling victim to social engineering tactics like phishing, and neglecting to follow established security protocols. Personal cognitive limitations—such as inattention, stress, or fatigue—can impair judgment and increase the likelihood of errors. These vulnerabilities can manifest in various ways, including unintentional actions like clicking on malicious links, forgetting critical updates, or misinterpreting the legitimacy of a request. Understanding these different types of human error is crucial for developing effective cybersecurity strategies that account for natural human limitations and improve individual resilience to cybersecurity threats. (Reason 1990.)

From an organizational perspective, human factors encompass workplace culture, training initiatives, and communication practices that shape employee behavior in relation to cybersecurity. Effective security systems and policies must be not only technically sound but also practical and user-friendly. When security measures are overly complex or perceived as punitive, employees are more likely to bypass them, increasing vulnerability to breaches. Therefore, organizations should aim to strike a balance between stringent security requirements and human usability. Promoting a culture of awareness, accountability, and continuous learning is essential to ensure compliance and reduce the likelihood of security incidents caused by human error. (Sasse & Flechais. 2005.)

Cybersecurity frameworks, such as the NIST Cybersecurity Framework, increasingly recognize the role of human factors. These frameworks highlight the importance of measures such as regular training, creating clear policies, and promoting a security-conscious environment. By integrating human considerations into their guidelines, these frameworks aim to address the interplay between people, processes, and technology.

Understanding and addressing human factors is critical because the majority of cybersecurity incidents involve a human element. Whether it is an employee inadvertently clicking on a malicious link, a team failing to communicate effectively during a cybersecurity incident, or an organization neglecting to provide adequate training, human behavior can significantly impact security outcomes. Therefore, integrating insights from human-computer interaction, cognitive psychology, and organizational behavior into cybersecurity practices is essential to mitigating risks and enhancing resilience. (Sasse, & Flechais 2005.)

2.2 Human Behavior in the NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) serves as a widely recognized model for managing cybersecurity risks, emphasizing the importance of a systematic approach to securing organizational assets. Initially developed to enhance the security of critical infrastructure, the framework's applicability has expanded globally, offering organizations a flexible structure to address a broad range of cybersecurity challenges. The NIST framework organizes cybersecurity efforts into five ongoing functions: identifying risks, protecting assets, detecting intrusions, responding to threats, and recovering from incidents. (NIST 2018.)

Human behavior is inherently tied to several aspects of the NIST Framework, particularly in its emphasis on the Protect and Respond functions. The Protect function involves activities like access control and employee training, acknowledging the role of individuals in preventing unauthorized actions and maintaining the confidentiality and integrity of systems. Similarly, the Respond function underscores the need for well-coordinated human actions during incidents, where decisions under pressure often determine the effectiveness of containment and recovery efforts. (NIST 2018.)

The framework implicitly recognizes the impact of human behavior on its implementation, as the success of security measures often depends on employees' adherence to policies and their ability to identify and react to potential threats. For example, the Identify function requires individuals to accurately map organizational risks and vulnerabilities, a task that can be influenced by subjective judgment or gaps in knowledge. Although the framework provides a technical and procedural foundation, its reliance on human action and decision-making highlights the complex interplay between human factors and cybersecurity practices. (NIST 2023.)

2.3 Human Factors in the ISO/IEC 27001 Framework

ISO/IEC 27001 provides a standardized model for creating and maintaining an organization's information security system, emphasizing risk assessment and management, thus the Information Security Management System (ISMS). Widely adopted across industries, the framework includes a detailed set of domains that address both technical and organizational measures. These domains, such as access control, incident management, and awareness and training, reflect the interconnected roles of systems, policies, and human actors in maintaining cybersecurity. (ISO 2022.)

Human behavior is integral to the framework's implementation and effectiveness.
The Awareness and Training domain highlights how individuals' understanding and attitudes

toward security practices influence the overall security posture. For instance, an organization's ability to prevent or mitigate incidents depends significantly on employees' knowledge of potential threats and their willingness to follow established protocols. Similarly, the Incident Management domain emphasizes the importance of human actions in identifying, reporting, and responding to breaches, where delays or missteps can exacerbate the consequences of an incident. (ISO 2022.)

The framework's focus on leadership and organizational culture further underscores the role of human factors in shaping cybersecurity outcomes. Leadership commitment, as outlined in ISO/IEC 27001, not only drives compliance but also fosters a security-conscious environment where individuals feel empowered to prioritize security. However, the structured nature of the framework sometimes overlooks the nuanced and unpredictable elements of human behavior, such as cognitive biases or stress-induced errors, that influence responses to cybersecurity incidents. This dynamic underscore the critical connection between human actions and the framework's practical application, highlighting the need to understand behavior within the broader context of cybersecurity management. (Svobodova 2023.)

2.4 Behavioral Theories Relevant to Cybersecurity

Understanding human behavior is crucial in cybersecurity because human actions frequently play a significant role in causing or exacerbating security breaches. While technological defenses like firewalls and encryption are critical, they cannot fully safeguard against the vulnerabilities introduced by human error. To address these human factors, behavioral theories such as the Theory of Planned Behavior (TPB) and Human Error Models offer valuable insights into understanding and predicting security-related behaviors. By integrating these theories, organizations can develop strategies that account for the human element in cybersecurity and design interventions that reduce the risk of breaches caused by human actions.

2.4.1 Theory of Planned Behavior

The Theory of Planned Behavior (TPB), as developed by Icek Ajzen (1991), is a psychological model that explains how intentions to perform a behavior are formed and how those intentions lead to actual behavior. According to the researcher, an individual's intention to engage in a specific action is influenced by three primary factors: their attitude toward the behavior (personal evaluation), subjective norms (perceived social pressure), and perceived behavioral control (the sense of confidence or capability in performing the behavior). These

three elements collectively shape intentions, which are the strongest predictors of actual behavior—provided that the individual has sufficient control over the action. (Ajzen 1991.)

- Attitude towards the behavior refers to an individual's positive or negative evaluation of performing a specific action. For instance, if an employee believes that using a strong password enhances security, they are more likely to adopt this behavior.
- Subjective norms involve the social pressures or expectations that influence an individual's behavior. If colleagues, supervisors, or organizational culture emphasize the importance of maintaining security protocols, employees are more likely to follow security guidelines.
- Perceived behavioral control reflects an individual's belief in their ability to perform a behavior. In cybersecurity, this refers to whether employees feel confident in their ability to use security tools or follow complex protocols.

The application of the Theory of Planned Behavior (TPB) provides a framework for understanding the factors that influence security behaviors. Attitudes toward cybersecurity, shaped by perceptions of the benefits and importance of secure practices, play a critical role in determining behavior. Similarly, subjective norms, such as the influence of organizational culture and peer expectations, contribute to individuals' adherence to security protocols. Perceived behavioral control, or individuals' confidence in their ability to follow security guidelines, is another key factor that impacts their actions. Research has demonstrated that TPB effectively predicts online safety behaviors, highlighting its relevance as a model for examining how individuals approach cybersecurity practices and decisions. (Burns & Roberts 2013.)

2.4.2 Human Error Models

Human Error Models are particularly valuable in understanding the ways in which human mistakes contribute to security vulnerabilities. These models categorize errors into different types, helping to pinpoint the causes of security lapses. Broadly, errors in cybersecurity are classified into two categories: skill-based errors and decision-based errors. (Keepnet Labs 2023.)

- Skill-based errors are unintentional mistakes that occur when performing routine tasks. These errors typically happen when an individual's attention lapses or they become distracted. For example, a user may accidentally click on a phishing link or fail to notice a warning about a security threat. These errors are often the result of a mismatch between the human cognitive capabilities and the complexity of the task at hand.

- Decision-based errors, on the other hand, occur when individuals make incorrect decisions due to lack of knowledge, incorrect assumptions, or misjudgment. In cybersecurity, this could involve misconfiguring security settings, failing to update software patches, or disregarding security alerts. Such errors are typically the result of poor decision-making processes, often under stress or time pressure, and can lead to significant security breaches.

Understanding these types of errors provides valuable insights into designing security systems that account for human limitations. Skill-based errors, which often arise during routine tasks, can be linked to lapses in attention or distractions. These errors highlight the importance of designing interfaces and processes that align with users' cognitive capabilities, ensuring that tasks are less prone to mistakes. Decision-based errors, on the other hand, stem from incorrect choices due to limited knowledge or misjudgment, often under stressful or time-sensitive conditions. These errors emphasize the significance of clear protocols and accessible decision-making resources to support individuals in critical situations. (IBM 2019.) (IBM Security 2023.)

The integration of the Theory of Planned Behavior and Human Error Models provides a framework for analyzing both the behavioral and cognitive factors that contribute to cybersecurity vulnerabilities. These models reveal the root causes of security lapses by clarifying how individuals interact with technology and protocols. By examining these aspects, it becomes possible to gain a deeper understanding of how human behavior impacts cybersecurity and to identify patterns that contribute to a security-conscious organizational culture. This understanding highlights the central role of human factors in shaping the overall effectiveness of cybersecurity measures. (Burns & Roberts 2013.)

3 Current Legislative Frameworks in the European Union

Evaluating current legislative frameworks in the EU is crucial for understanding how legal regulations influence cybersecurity practices, especially concerning human factors. While technological measures are often prioritized, existing laws like the General Data Protection Regulation and the NIS2 Directive focus more on data protection and infrastructure than on addressing human-related vulnerabilities, such as poor decision-making or lack of training. By analyzing these frameworks, this thesis can identify gaps in current legislation and propose improvements to better address the human element in cybersecurity, ensuring that legal frameworks evolve to mitigate the risks associated with human error and behavior.

3.1 The NIS2 Directive (Directive (EU) 2022/2555)

The NIS2 Directive marks a significant evolution in the European Union's approach to cybersecurity, with a strong focus on mitigating risks associated with human error. The directive sets forth comprehensive requirements that organizations must implement to build resilience and reduce vulnerabilities stemming from both technical and human factors.

A core requirement of NIS2 is the provision of regular cybersecurity awareness training for all employees, including senior management, to address persistent risks such as phishing, weak password practices, and mishandling of sensitive information. This training must be ongoing and tailored to evolving threats, ensuring that staff at every level are equipped to recognize and respond to cyber risks effectively. By embedding cybersecurity awareness into the organizational culture, NIS2 aims to reduce the likelihood of breaches caused by human mistakes and foster a workforce that is alert to the latest threats and best practices. (DataGuard 2025.)

The directive also highlights the importance of fostering a security-conscious culture through the promotion of strong cyber hygiene practices. Organizations are expected to implement structured processes and ongoing awareness initiatives that encourage behaviors like regular password changes, the use of multi-factor authentication, and strict adherence to secure protocols. These measures are designed to make secure habits part of daily routines, minimizing opportunities for human error and reinforcing the importance of cybersecurity at every organizational level. Leadership is expected to model and reinforce these practices, ensuring that cyber hygiene becomes second nature to all staff members. (Stegmaier 2025.)

NIS2 obliges organizations to conduct regular risk assessments that specifically address the human element, including monitoring digital footprints and credential exposure to reduce the "human attack surface." The directive also requires the establishment of clear incident response procedures, assigning defined roles and responsibilities to employees during cyber incidents. Regular simulations and exercises are mandated to ensure preparedness and reinforce correct behaviors under pressure, ultimately reducing the likelihood that human error will escalate a security event. (DataGuard 2025.) (Stegmaier 2025.)

To effectively implement NIS2's requirements, organizations must ensure that personnel at all levels—decision makers, IT operations, security operations, and technical leadership—receive targeted training that matches their roles. CompTIA emphasizes the importance of a pathways-based approach to skills development, recommending that organizations adopt structured certification and training programs to build a learning culture and support continuous professional development. This approach ensures that everyone, from non-technical leaders to technical specialists, is equipped to contribute to the organization's cybersecurity resilience and compliance with NIS2 minimum measures. (CompTIA 2025.)

3.2 The EU Cybersecurity Act

The EU Cybersecurity Act, adopted in June 2019, is a cornerstone in the Union's strategy to address not only technical but also human-related vulnerabilities in cybersecurity. By granting the European Union Agency for Cybersecurity (ENISA) a permanent mandate and expanded resources, the Act ensures that the agency can coordinate and support Member States in building robust cybersecurity cultures, where human behavior is recognized as a critical risk factor.

A central feature of the Act is the establishment of an EU-wide cybersecurity certification framework for ICT products, services, and processes. This framework sets consistent standards that require manufacturers and service providers to implement security measures specifically designed to address common human errors, such as weak passwords, poor access controls, and inadequate user training. Certification schemes guide organizations to adopt best practices in user authentication, data protection, and access management—areas where human mistakes frequently lead to breaches. (European Commission 2023.)

By certifying digital products and services, the Act increases trust in the digital ecosystem, assuring businesses and individuals that certified solutions incorporate safeguards against the most prevalent human-related vulnerabilities. This approach not only raises the baseline for technical security but also compels organizations to prioritize user awareness, training, and clear security policies as part of their compliance efforts.

Ultimately, the EU Cybersecurity Act bridges the gap between technology and human factors by mandating that both are addressed in the design, certification, and operation of ICT systems. This comprehensive strategy directly targets the reduction of human errors in cybersecurity, making the Act a vital tool for improving resilience across the European Union. (ENISA 2022.)

3.3 The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) does not explicitly refer to "human error," but it addresses the concept through its emphasis on data security and risk management. Article 5(1)(f) establishes that personal data must be processed in a way that ensures protection against accidental loss, destruction, or unauthorized access—scenarios often resulting from human mistakes. Similarly, Article 32 requires data controllers and processors to implement appropriate technical and organizational measures, such as encryption, access controls, and ongoing evaluation of security practices, to safeguard against risks that may arise from unintentional actions.

Additionally, Article 33 obliges organizations to report personal data breaches within 72 hours of becoming aware of them, a requirement that frequently applies to incidents caused by human error, such as accidental data disclosure or mishandling. Recital 83 further supports this approach by encouraging organizations to assess and mitigate risks related to both accidental and unlawful data processing. These provisions, while not directly naming human error, establish a regulatory framework that implicitly recognizes its role in cybersecurity and mandates preventive and responsive measures to reduce its impact. (GDPRhub 2025.)

4 Methodology

This research employs a qualitative methodology to explore how human factors influence cybersecurity incidents and to develop strategies for addressing related vulnerabilities. A qualitative approach is appropriate for this study because it allows for a detailed analysis of documented cases, theoretical frameworks, and existing literature to understand the impact of human behavior on cybersecurity.

The research methods include a comprehensive literature review, case study analysis, and secondary data analysis. The literature review focuses on academic articles, industry reports, and theoretical frameworks related to human factors and cybersecurity. Case study analysis examines documented cybersecurity incidents, such as data breaches or social engineering attacks, to identify recurring patterns and the role of human behavior in these events. Secondary data analysis utilizes existing datasets and reports from cybersecurity organizations to evaluate trends and provide evidence-based insights.

This approach ensures a thorough examination of the topic by leveraging existing knowledge and documented experiences. By synthesizing insights from multiple sources, the research aims to develop actionable strategies to address vulnerabilities associated with human factors in cybersecurity, bridging the gap between theory and practice.

4.1 Literature review

Literature review is a critical and systematic examination of existing research and published sources related to a specific topic. Its purpose is to provide an overview of what is already known, identify key theories, findings, and gaps in the current knowledge, and place the current study within a broader academic context. In a thesis, the literature review helps demonstrate the researcher's understanding of the topic, highlight the relevance of the research questions, and justify the chosen methodology. (Ridley 2012.)

In this thesis, the literature review forms a foundational component, providing a critical and structured examination of existing research on the role of human factors in cybersecurity incidents. As cybersecurity challenges increasingly emerge from the intersection of advanced technologies and human behavior, it is essential to explore the psychological, cognitive, and organizational dimensions of these issues.

Drawing on peer-reviewed academic articles, industry reports, and policy documents, this review investigates how human behavior influences cybersecurity outcomes. The ISO/IEC 27001 standard was used as a foundational reference for information security management systems. It provided essential guidance on the integration of organizational and technical controls, highlighting how policy and structure can address human vulnerabilities, such as improper access control and poor documentation practices. The NIST Cybersecurity Framework was also included for its flexible, widely adopted approach to managing cybersecurity risk. Its emphasis on training, awareness, detection, and response was served in exploring how organizations can systematically address human error.

In addition to these standards, other academic sources, such as Parsons, McCormac, Butavicius, Pattinson, and Jerram (2021), Arevalo, Valarezo, Fuertes and Cazares (2023), Khadka and Ullah (2025), and the ScienceDirect (2023), were utilized in the literature review for their systematic review on cybersecurity awareness frameworks. These sources were selected because they provided strong empirical and theoretical support for understanding the complexities of human error in cybersecurity. They offered insights into user attitudes, decision-making under stress, phishing detection challenges, and the effectiveness of awareness training—all of which aligned closely with the goals of this research.

Hancock's (2022) research report published by Tessian provided a current industry perspective, illustrating how human error remains a dominant cause of cybersecurity incidents in organizational environments. Capaccioli (2022) contributed a psychological and educational perspective, discussing how long-term behavioral change and structured awareness efforts are essential to sustainable security culture. In addition to others, these sources helped frame a balanced view that accounts for both strategic and psychological dimensions of user behavior.

Materials that focused exclusively on technical implementations—such as software performance, cryptographic algorithms, or malware engineering—were intentionally excluded. This was done to maintain a clear and focused scope that aligns with the research objectives: understanding and mitigating human error in cybersecurity through behavioral, educational, and organizational strategies.

4.2 Case Study Analysis

Analyzing real-world cybersecurity incidents involves an in-depth examination of documented cases to understand the role of human behavior in causing or exacerbating breaches. Case studies are a qualitative research method that focuses on specific, real-life examples to uncover patterns, insights, and lessons that can inform future practices. This approach is particularly suitable for this thesis because it allows for the exploration of complex human interactions and organizational responses within the dynamic context of cybersecurity incidents.

The case studies selected for analysis are the 2017 WannaCry ransomware attack, the 2014 Sony Pictures hack, and the 2017 Equifax data breach. These incidents were chosen for their clear demonstration of critical and varied forms of human error in cybersecurity. Each case offers unique insights into different types of human-related vulnerabilities: WannaCry reveals the consequences of neglecting timely security updates, Sony Pictures exposes the risks tied to phishing and insider threats, and Equifax highlights failures in vulnerability management and internal coordination. Together, they represent a wide range of organizational and individual shortcomings that contributed to significant security breaches. Their widespread impact and the availability of comprehensive documentation—including post-incident analyses and industry reports—make them particularly valuable for examining how human behavior influences cybersecurity outcomes. The analysis involves a systematic review of each case, including the events leading up to the breach, the actions taken by individuals and organizations during the incident, and the outcomes. By critically evaluating these cases, the research aims to identify recurring behavioral patterns, organizational challenges, and decision-making failures. This will be complemented by insights into successful interventions and lessons learned from the incidents.

A systematic review was conducted to support the analysis of the selected case studies by identifying and synthesizing existing research on human error in major cybersecurity incidents. This review followed a structured approach, including predefined inclusion and exclusion criteria, to ensure the relevance and quality of the sources. Academic publications, industry reports, and post-incident analyses were examined to extract recurring themes related to human factors, such as poor patch management, phishing susceptibility, and breakdowns in internal communication. The findings were categorized thematically and used to compare patterns of human error across the WannaCry, Sony Pictures, and Equifax breaches. This method provided a comprehensive and evidence-based foundation for analyzing how individual and organizational behaviors contributed to each incident, offering insights into systemic vulnerabilities and potential strategies for mitigation. (Kitchenham 2004.)

4.2.1 Case Study 1: The 2017 WannaCry Ransomware Attack

The WannaCry ransomware attack took place in May 2017, spreading rapidly to compromise more than 200,000 computers across over 150 countries. The attack impacted a wide range of sectors, including healthcare, financial services, telecommunications, and government agencies. The WannaCry ransomware spread by taking advantage of unpatched security flaws in Microsoft Windows. Once a system was infected, the malware locked access to user files and demanded a ransom in Bitcoin to restore functionality. One of the most heavily impacted institutions was the United Kingdom's National Health Service (NHS), which faced major disruptions to patient care. The incident revealed how ransomware can severely disrupt critical infrastructure and essential services, with estimated global damages reaching billions of dollars. (Akbanov, Vassilakis & Logothetis 2019.)

WannaCry exploited a vulnerability in Microsoft Windows operating systems, known as Eternal Blue, which allowed the ransomware to spread automatically between computers without user interaction. This exploit had been developed by the U.S. National Security Agency (NSA) and was leaked online by the hacker group Shadow Brokers in early 2017. Microsoft had issued a security patch (MS17-010) in March 2017, but many systems remained unpatched by May, allowing WannaCry to spread rapidly through networks. The ransomware particularly targeted older and unsupported versions of Windows, such as Windows XP, amplifying the attack's impact. (Prevezianou 2021.)

A critical element behind the success of the WannaCry attack was a combination of human error and organizational neglect. One major factor was the failure in patch management, as many organizations, including the NHS, did not apply the security updates released by Microsoft, leaving their systems vulnerable to exploitation. This oversight reflected poor IT governance and a lack of prioritization for cybersecurity measures. Additionally, the use of outdated legacy systems like Windows XP, which had reached its end-of-support period, further exacerbated the situation by eliminating the possibility of receiving vital security updates. The lack of cybersecurity awareness also contributed, as frontline employees, including hospital staff, were not adequately trained to recognize the warning signs of ransomware or follow protocols to contain the infection. Finally, resource constraints in many public sector organizations, such as limited budgets, hindered their ability to upgrade aging infrastructure or invest in necessary cybersecurity measures. (Smart 2018.)

The WannaCry attack caused over 19,000 appointments to be cancelled, including urgent cancer treatments and surgeries, and several hospitals were forced to divert ambulances and patients to other facilities. Beyond the immediate healthcare impact, the attack also caused financial losses, with the NHS estimating damages of around £92 million, covering both direct costs and long-term recovery efforts. Globally, major corporations such as FedEx, Telefónica,

and Renault were also affected, experiencing disrupted operations and financial losses. (Smart 2018.)

In this case, a widespread cyberattack exploited an unpatched vulnerability in widely used software, despite the availability of security updates prior to the incident. This scenario reflects the Theory of Planned Behavior in several ways. Employees and decision-makers may have exhibited negative attitudes toward timely patching, perceiving it as low-priority or disruptive to operations. Subjective norms within the organization likely reinforced complacency, especially if similar behavior was common or tolerated. Additionally, perceived behavioral control may have been low among IT personnel, particularly if they lacked the autonomy or resources to implement patches without higher-level approval. From the perspective of human error models, the failure to act on critical updates constitutes a rule-based mistake, where known procedures were misapplied due to incorrect risk assessment.

4.2.2 Case Study 2: The 2014 Sony Pictures Hack

In November 2014, Sony Pictures Entertainment became the target of a highly destructive cyberattack carried out by a group known as the Guardians of Peace (GOP). The attack was widely suspected to be state sponsored, allegedly with ties to North Korea, reportedly in retaliation for the release of The Interview, a satirical film depicting the assassination of North Korean leader Kim Jong-un. The breach resulted in the theft of a vast array of sensitive information, including confidential employee data, private emails, unreleased films, and proprietary corporate material. The stolen information was subsequently released to the public, severely damaging Sony's reputation and incurring financial losses in the millions. The attack was not only an act of cybercrime but also a significant geopolitical incident. (Steinberg, Stepan & Neary 2020.)

The technical mechanisms behind the Sony Pictures hack involved multiple methods, including exploiting weak password practices and social engineering tactics. The attackers gained initial access to the company's network by leveraging weak and easily guessable passwords used by employees, which provided them with an entry point into the system. From there, they were able to move laterally through Sony’s IT infrastructure with minimal resistance. In addition, the attackers used phishing emails and other social engineering techniques to further infiltrate and escalate their access, enabling them to steal and exfiltrate sensitive data without being detected for an extended period. The lack of robust security defenses and proactive monitoring allowed the attackers to exploit these vulnerabilities and maintain control over Sony's systems for weeks. (Steinberg et al. 2020.)

In this scenario, The Theory of Planned Behavior helps explain how employees' attitudes—such as prioritizing ease of access over security—contributed to risky behavior. Subjective norms likely failed to promote secure practices, and perceived behavioral control may have been low, particularly if employees were not adequately trained or if security policies were unclear. In terms of human error, the behaviors observed can be classified as violations, where individuals knowingly deviated from established protocols, and slips, where security-related actions were improperly executed despite good intentions. These types of errors highlight how both conscious and unconscious human actions can undermine organizational security when not addressed through adequate training and enforcement.

4.2.3 Case Study 3: The 2017 Equifax Data Breach

The Equifax data breach, which occurred in 2017, is regarded as one of the most significant cybersecurity incidents in history. The incident led to the compromise of personal records belonging to roughly 147 million people, which included critical identifiers such as Social Security numbers, dates of birth, and credit card data. This massive breach highlighted serious gaps in the company's data protection practices. The breach occurred because attackers exploited a vulnerability in the Apache Struts framework, a popular open-source software used for web applications. Although a patch for this vulnerability had been available for several months prior to the attack, Equifax failed to implement it, leaving its systems vulnerable to exploitation. The breach's scale and impact highlighted serious weaknesses in Equifax's cybersecurity practices and its ability to prevent and respond to cybersecurity threats. (EPIC 2020.)

The technical vulnerability behind the Equifax data breach was located in the Apache Struts framework, which Equifax used in its web applications. Attackers were able to exploit a known vulnerability in this framework, which had a publicly available patch released by the Apache Software Foundation months before the breach. Equifax's failure to apply the patch allowed the attackers to gain unauthorized access to their systems, where they were able to extract sensitive personal data on a massive scale. This breach illustrates the critical importance of timely patch management, and the potential risks organizations face when updates are neglected. The exploitation of a known vulnerability in widely used software, combined with the company's failure to act on available fixes, exposed severe gaps in Equifax's cybersecurity processes. (Breachsense 2024.)

In this case, according to the Theory of Planned Behavior, this inaction may have stemmed from attitudes that did not view cybersecurity risks as urgent, subjective norms that tolerated delays in technical maintenance, and limited perceived behavioral control, where employees may have lacked clear guidelines or authority to act. From a human error

standpoint, this reflects a knowledge-based mistake, where individuals may not have fully understood the consequences of the unpatched vulnerability. It may also indicate a lapse in organizational processes, such as poor asset tracking or unclear roles, which contributed to the failure to act in time. These errors underscore the importance of aligning individual responsibilities with systemic support and organizational awareness. (Burns & Roberts 2013.)

4.2.4 Comparing patterns of human errors across the case studies

Case study	Key human Errors Identified	Error Type (Model)	Explanation
WannaCry (2017)	- Failure to apply known security patch - Use of outdated systems (Windows XP) - Lack of staff training and awareness	Rule-based mistake Skill-based error	Patch was available but ignored; staff lacked training to respond; outdated systems increased vulnerability
	-Poor IT governance and Prioritization	Organizational error	Cybersecurity not prioritized; resource constraints hindered upgrades
Sony Pictures (2014)	- Use of weak and guessable passwords - Susceptibility to phishing - Lack of incident response preparedness	Slips and violations (intended deviations)	Employees knowingly bypassed good practices: phishing not recognized; delayed detection of breach
	- Poor cybersecurity culture and training	Organizational failure	Security seen as low priority; limited enforcement and awareness

Equifax (2017)	- Ignored patch availability (Apache Struts) - Communication breakdown - Delayed breach detection	Knowledge-based mistake Decision error	Employees unaware or lacked urgency; roles unclear; poor monitoring delayed response
	- Lack of accountability and unclear roles	Organizational/process error	Weak internal coordination led to failure in applying critical patches

5 Results

The following section presents the findings drawn from the literature review and the analysis of major cybersecurity case studies. The goal is to deliver a well-rounded understanding of how human error contributes to cybersecurity incidents and how organizations can strengthen their defenses. By combining insights from academic research and real-world examples, the section highlights central patterns and emerging themes.

The results explore key topics such as the underlying human factors behind cybersecurity breaches, the influence of organizational practices and employee awareness, and critical lessons identified from recent high-profile incidents. This combined approach offers both conceptual and practical perspectives, providing a nuanced view of the challenges posed by human error in cybersecurity and identifying pathways to improve resilience across industries.

5.1 Human Error as a Critical Factor in Cybersecurity

Academic research consistently shows that human error is a leading contributor to cybersecurity incidents across a wide range of industries, including higher education, healthcare, and small businesses. Human actions—such as lapses in judgment, lack of awareness, and routine mistakes—frequently create vulnerabilities that cybersecurity attackers exploit. Common weaknesses across organizations include inadequate staff training, poor password hygiene, and a widespread inability to recognize phishing attempts. Arevalo et al. (2023) provide a comprehensive analysis of the cognitive and human factors involved in phishing detection, revealing that users often rely on superficial cues rather than critical,

analytical thinking when assessing the legitimacy of emails. This insight highlights the importance of developing interventions that promote deeper cognitive engagement, moving beyond basic awareness campaigns to strategies that foster more thoughtful and informed user behavior. (Arevalo, Valarezo, Fuertes & Cazares 2023.)

5.2 Sector-Specific Patterns

Research reveals distinct sector-specific patterns in human-error-related cybersecurity incidents, driven by the operational environments and workforce characteristics of each industry. In healthcare, for example, human error is a significant contributor to breaches, with incidents often resulting from misconfigured access controls, accidental data sharing, and poor email hygiene among clinical staff working under high-pressure conditions. (Pollini, Callari, Tedeshi, Ruscio, Save, Chiarugi & Guerri 2021.)

The retail sector, meanwhile, reports some of the highest rates of breaches with 80% of retailers experienced cyberattacks in the past year, identifying human error as the leading factor in these breaches. With factors such as high employee turnover, temporary staff hiring, insufficient cybersecurity training, understaffing or over-extension of teams, and the prioritization of customer service over security checks leading to frequent mistakes like phishing susceptibility and weak password practices, 52% of retailers report being at growing risks of cybersecurity attacks. (VikingCloud Team 2025.)

In education, human error is considered a leading cause of cybersecurity incidents, with recent studies indicating that it accounts for approximately 35% of breaches. The education sector is uniquely vulnerable due to its large, diverse user base—including students, faculty, and administrative staff—who frequently access networks with personal or unmanaged devices. Factors such as insufficient cybersecurity training, lack of awareness, and the widespread use of bring-your-own-device (BYOD) policies significantly increase the risk of accidental data exposure, misconfigured access controls, and susceptibility to phishing attacks. Notably, surveys show that 30% of users in the education sector have fallen for phishing scams, and 60% of respondents to the surveys were unaware of institutional cybersecurity policies or their responsibilities to protect university resources, despite policies existing. (Amorosa & Yankson 2023.)

Human error is a major contributor to cybersecurity incidents in the telecommunications sector, consistently identified as one of the leading causes of service disruptions and breaches. According to the European Union Agency for Cybersecurity (ENISA), security incidents caused by human error in telecom increased from 18% in 2018 to 26% in 2019, with fixed telephony and internet services being the most affected—50% and 45% of incidents in these areas, respectively, were attributed to mistakes by personnel. These errors include misconfigurations, failure to follow procedures, improper software updates, and accidental

disclosure of sensitive information. ENISA also notes that the impact of such incidents is significant, resulting in hundreds of millions of user hours lost and highlighting a trend of increasing human-error-related incidents since 2012. (Awwad 2020.)

Industry-wide studies reinforce these findings: Verizon's 2023 Data Breach Investigations Report and IBM's 2024 CISO survey both indicate that human error is responsible for a substantial proportion of breaches in critical infrastructure sectors, including telecommunications. Everyday mistakes—such as using weak passwords, neglecting system updates, or clicking on phishing links—are cited as common entry points for attackers. Social engineering attacks, particularly business email compromise, exploit the human element, and a lack of cybersecurity skills among telecom staff further exacerbates the risk. Surveys show that up to 83% of industry professionals believe there is a serious skills gap, and 80% consider human error the biggest risk to their control systems. (Gregory 2024.)

The financial services sector faces a dual challenge: deliberate policy violations and malicious insider actions account for a notable share of incidents, reflecting the high-stakes environment and the elevated access privileges of many employees. Small businesses are also acutely vulnerable, with a substantial portion of incidents attributed to basic errors like downloading suspicious attachments, poor backup practices, and inadequate access controls. These sectoral differences underscore the importance of tailored mitigation strategies that address the specific human-factor risks present in each industry.

5.3 Importance of Training and Awareness

Research across various sectors highlights the critical importance of investing in robust cybersecurity training and awareness initiatives. Effective programs, when tailored to the specific needs of an organization, not only help employees recognize potential threats but also improve day-to-day security practices and reduce the likelihood of costly errors. However, as Parsons et al. (2021) emphasize in their study Cybersecurity Awareness Training Programs: An Empirical Evaluation, training alone is not sufficient. Its effectiveness depends heavily on how well it engages users and addresses their underlying attitudes, knowledge, and behavioral habits. Their findings underscore that meaningful training must go beyond simply delivering information—it must actively challenge risky behaviors and foster a security-conscious culture.

The study by Parsons et al. provides both strong empirical and theoretical support for understanding the complexities of human error in cybersecurity. Empirically, the authors conducted a large-scale evaluation using validated instruments such as the Human Aspects of Information Security Questionnaire (HAIS-Q) to assess the impact of awareness training on actual cybersecurity behavior across multiple organizations. Their results demonstrated a

clear relationship between training interventions and improvements in secure practices, including password hygiene and access control, providing measurable evidence of behavioral change. Theoretically, the study is grounded in established behavioral models, particularly the Theory of Planned Behavior, which links individual attitudes, subjective norms, and perceived behavioral control to specific cybersecurity actions. By integrating this framework, the authors not only identify which behaviors changed but also explain the psychological and social mechanisms behind these changes. This combination of quantitative evidence and behavioral theory makes the study a valuable resource for analyzing human error in cybersecurity, especially in environments that manage sensitive data or operate under limited cybersecurity resources. (Parsons, McCormac, Butavicius, Pattinson & Jerram 2021.)

5.4 The Role of Policy and Organizational Culture

Effective cybersecurity policies that integrate human factors are key to reducing human error. Research by Michael Mncedisi Willie (2023) underscores the importance of designing policies that consider employee behavior, organizational culture, and real-world decision-making processes. Policies should not only focus on technical measures but also prioritize creating a culture where security awareness is embedded at every level of the organization. This approach encourages accountability, reinforces good security habits, and helps reduce the risk of breaches caused by human mistakes.

The research by Willie (2023) highlights that a security-first organizational culture fundamentally shapes how employees perceive and adhere to cybersecurity protocols. When security values are woven into the fabric of daily operations—supported by visible leadership commitment and continuous education—employees are more likely to internalize and follow security policies. This cultural integration transforms security from a perceived barrier into a shared responsibility, making employees active participants in risk management rather than passive rule-followers.

Ultimately, aligning cybersecurity policies with organizational culture creates a resilient environment where human factors are leveraged as strengths rather than vulnerabilities. By fostering open communication, encouraging reporting of potential threats, and providing practical, ongoing training, organizations can minimize human error and strengthen their overall security posture. Willie’s (2023) work makes it clear that the most effective cybersecurity strategies are those that balance robust technical controls with a deep understanding of human and organizational dynamics. (Willie 2023.)

5.5 Designing Systems for Human Limitations

Khadka and Ullah (2025) introduce a comprehensive conceptual framework that situates human factors at the core of cybersecurity risk management. Their model reflects a shift away from purely technical defenses, emphasizing that many security breaches stem from psychological and organizational vulnerabilities. By embedding human behavior into the foundation of cybersecurity planning, the framework acknowledges that understanding how people respond to stress, workload, and confidence levels is essential for reducing cybersecurity risks.

The framework systematically identifies stress, excessive workload, and overconfidence as primary contributors to human error in digital environments. Stress, often arising in high-pressure work settings or during incident response, can impair cognitive function, reduce vigilance, and lead to lapses in judgment—factors that increase susceptibility to phishing and social engineering. Similarly, excessive workload and multitasking fragment attention and contribute to security fatigue, causing individuals to skip protocol or overlook critical updates. Overconfidence, particularly among experienced or senior personnel, may result in underestimating threats, ignoring warnings, or neglecting basic cybersecurity practices.

By integrating these dimensions, Khadka and Ullah present a holistic model of how psychological and environmental pressures interact to heighten the risk of human error. Their framework offers practical, targeted interventions that organizations can implement to address these issues, including stress management programs, workload balancing strategies, and routine training that challenges overconfidence. These measures aim to embed human-awareness into cybersecurity systems, thereby reducing the likelihood of human-induced breaches and strengthening overall organizational resilience. (Khadka & Ullah 2025.)

5.6 Overall Implications

Human error remains a central cybersecurity vulnerability, often overlooked in favor of purely technical solutions. However, cognitive lapses such as stress-related misjudgments, inattention, and overconfidence continue to expose organizations to significant risks, even when advanced security systems are in place. Incident data and cross-sector analyses consistently show that neglecting the human element allows vulnerabilities to persist, undermining overall security efforts. This highlights the need for a fundamental shift in cybersecurity strategy—one that places human factors at the core of risk management, rather than treating them as secondary concerns.

To mitigate these risks, organizations must integrate behavioral awareness with technical defenses through three pillars:

- Training Transcending Awareness: Programs must evolve beyond basic phishing literacy to reshape attitudes and habits, using evidence-based models like Icek Ajzen's Theory of Planned Behavior (1991) to foster critical thinking under pressure.

- Policy-Culture Alignment: Security protocols should mirror real-world workflows, as Willie (2023) demonstrates, embedding accountability through leadership-driven cultures that transform security from a compliance task to shared responsibility.

- Human-Centric System Design: Architectures must preempt psychological triggers—simplifying interfaces for high-stress roles (e.g., healthcare), automating safeguards against fatigue-induced errors, and countering overconfidence through continuous feedback loops.

Adopting this holistic framework—where technology, tailored training, culture, and ergonomic design converge—reduces human-error incidents by addressing root causes. Organizations can thus convert human vulnerability into resilience, turning employees into active defense layers rather than passive risks. This approach not only curbs breach frequency but also minimizes operational disruption, as seen in sectors implementing Khadka and Ullah's (2025) stress-workload mitigation strategies. Ultimately, cybersecurity maturity hinges on treating human factors as infrastructure, not an afterthought.

5.7 Lessons from the WannaCry Attack

The WannaCry ransomware attack stands among the most consequential cybersecurity incidents of the past decade, revealing critical weaknesses in human behavior, organizational practices, and technical safeguards. Examined through the lens of established cybersecurity frameworks such as the NIST Cybersecurity Framework (NIST CSF) and ISO/IEC 27001, this cases exposes clear areas where effective implementation could have mitigated risks and improved outcomes.

In this case, a major vulnerability stemmed from failures in patch management. The NIST CSF's "Protect" function and ISO/IEC 27001's clause A.12.6.1 both highlight the necessity of timely vulnerability management to maintain system resilience. Despite Microsoft releasing a patch months before the attack, many organizations, including the UK's National Health Service (NHS), had not applied it—reflecting systemic gaps in proactive security measures and governance.

Key lessons from WannaCry case include:

- Prioritize patch management: Organizations must adopt disciplined, well-resourced patch management practices to close known vulnerabilities promptly.
- Upgrade legacy systems: Relying on outdated or unsupported software in critical operations exposes institutions to major security risks.
- Invest in cybersecurity training: Regular staff training is essential to help employees recognize phishing attempts, malware signs, and correct response actions.
- Strengthen public-private cooperation: Governments and tech companies need to work closely together to share information on emerging vulnerabilities and threats.

In response to these lessons, the NHS and other impacted organizations have invested in system upgrades, improved patching protocols, and launched cybersecurity awareness programs to strengthen their overall resilience. (Smith 2018.)

5.8 Lessons from the Sony Pictures Hack

The Sony Pictures hack resulted in substantial financial losses and significant reputational damage. Attackers stole and leaked a vast trove of sensitive information, including employee records, private emails, and unreleased films. The financial impact was severe, with millions spent on recovery efforts, operational disruptions, and legal liabilities. However, the breach also revealed serious weaknesses in Sony's cybersecurity strategy, highlighting the need for not just technical defenses but also a strong organizational culture centered around cybersecurity awareness and preparedness.

Human error and organizational failures played a critical role in both the success and the severity of the attack. One of the primary issues was poor password hygiene—employees used weak and easily guessable passwords, making it easier for attackers to gain access to key systems. In addition, low levels of cybersecurity awareness among staff meant that phishing emails and other social engineering tactics went largely undetected, allowing attackers to infiltrate the network with little resistance.

The breach was further intensified by Sony's lack of a robust security culture. The company did not have a comprehensive or proactive incident response plan, which led to delays in detecting, containing, and mitigating the breach. This allowed attackers to maintain prolonged access to critical systems, amplifying the extent of the damage. Moreover, Sony's limited transparency during the incident—particularly its slow and inadequate communication with employees and the public—exacerbated the crisis and further eroded trust in the organization. (Steinberg et al. 2020.)

Key lessons from the Sony hack include:

- Strengthen password policies: Organizations must enforce robust password requirements and eliminate the use of weak or easily guessable passwords across all levels.

- Improve employee cybersecurity training: Regular and targeted training is essential to help staff recognize phishing attempts and social engineering tactics.

- Develop a comprehensive incident response plan: Organizations should establish and regularly test response plans to ensure swift containment and recovery from breaches.

- Promote a security-focused culture: Building an organizational mindset that values cybersecurity at every level is crucial to reducing risks and improving resilience.

In the aftermath of the attack, Sony faced significant internal restructuring and increased investment in cybersecurity measures to address the organizational weaknesses that allowed the breach to escalate (Steinberg et al. 2020.)

5.9 Lessons from the Equifax Data Breach

The Equifax data breach had far-reaching consequences, compromising the personal and financial information of millions and inflicting significant reputational and financial damage on the company. As one of the largest credit reporting agencies, Equifax's failure not only threatened the privacy and security of affected individuals but also undermined public trust in its role as a guardian of sensitive financial data. The breach led to extensive financial repercussions, including regulatory fines, class-action settlements, and compensation payments to impacted consumers.

At the heart of the breach were critical human errors and organizational failures. The primary cause was Equifax’s failure to apply a known security patch, despite being alerted to the vulnerability. This highlights serious flaws in the company's patch management process, where updates were not consistently prioritized or implemented. The situation was worsened by poor interdepartmental communication—information about the vulnerability and the necessary patch did not reach the responsible teams in a timely manner.

Equifax’s lack of accountability in managing system vulnerabilities, along with its failure to respond to both internal and external warnings, significantly amplified the breach’s severity. Moreover, the breach went undetected for several months, revealing serious deficiencies in the company’s monitoring and detection systems. This allowed attackers to quietly extract data over an extended period without being discovered. (Breachsense 2024.)

Crucially, the incident underscored the importance of robust cybersecurity practices, proactive risk management, and clear communication in the event of a breach. Equifax's delayed public disclosure and inadequate communication strategy worsened the public fallout, amplifying the damage to its reputation and credibility.

Key lessons from the Equifax breach include:

- Prioritize proactive security measures: Regular patching, vulnerability management, and system updates are essential to prevent exploitation of known flaws.
- Enhance monitoring and detection capabilities: Organizations must invest in tools and processes to detect breaches early and minimize potential damage.
- Ensure transparent and timely communication: Prompt, clear, and effective communication with the public and affected stakeholders is critical during cybersecurity incidents.
- Build accountability into organizational processes: Clear lines of responsibility and strong interdepartmental communication help ensure that critical security updates are applied without delay.

Following the breach, Equifax implemented significant improvements in its security practices, monitoring systems, and public communication strategies to rebuild trust and reduce future risks. (Breachsense 2024.)

5.10 Focus on Human Error in EU Cybersecurity Regulations

European regulations, particularly the General Data Protection Regulation (GDPR), place significant emphasis on human factors in data protection and cybersecurity. Under Article 32 of the General Data Protection Regulation (GDPR), organizations are required to put in place safeguards—both technical and administrative—to ensure the security of personal data. These include steps to prevent unauthorized access, accidental loss, or data breaches. The regulation has been in force since May 2018. This explicitly includes:

- Staff training
- Access controls
- Processes to identify, report, and handle breaches

The General Data Protection Regulation (GDPR) recognizes that human error — such as accidental data leaks, misconfigurations, or poor access management — is often at the heart

of data breaches. Organizations are required to address both technical and organizational vulnerabilities, which includes human behavior, not just system weaknesses. (GDPRhub 2025.)

In addition to the GDPR, the NIS Directive (Directive (EU) 2016/1148) establishes a comprehensive legal framework for achieving a high common level of security of network and information systems across the European Union. It requires that operators of essential services and digital service providers implement appropriate and proportionate technical and organizational measures to manage risks to the security of their systems and services. The Directive also mandates the notification of significant incidents to national competent authorities, aiming to enhance preparedness and resilience against cyber threats, including those originating from human error. (EUR-Lex 2022.)

The Directive obligates essential service operators and digital service providers to adopt a culture of risk management and incident reporting. By setting out cooperation mechanisms such as the NIS Cooperation Group and the network of national computer security incident response teams (CSIRTs), it ensures that both technical and organizational risks—including those related to human factors—are systematically addressed at both national and EU levels. (Think Tank 2020.)

Furthermore, the NIS 2 Directive (Directive (EU) 2022/2555) builds on the original NIS Directive by broadening its scope and strengthening requirements for risk management. It requires essential and important entities to adopt appropriate and proportionate technical, operational, and organizational measures to manage cybersecurity risks, with a clear focus on minimizing incidents arising from human mistakes. The directive mandates an "all-hazards" approach, ensuring that organizations are prepared to address a wide range of threats, including those caused by human error, and emphasizes the importance of ongoing risk assessment, training, and continuous improvement to maintain robust security postures. (NIS 2 Directive 2024.)

6 Conclusions

The evidence presented throughout this thesis demonstrates that human factors are central to both the occurrence and prevention of cybersecurity incidents. Despite significant advancements in technical safeguards—such as firewalls, encryption, and intrusion detection systems—case studies like WannaCry, Sony Pictures, and Equifax highlight that breaches are often triggered or worsened by human errors. These errors range from insufficient training and weak password practices to lapses in communication and a lack of a security-conscious organizational culture. In each case, technical vulnerabilities were present, but it was human

behavior that ultimately enabled attackers to succeed. This pattern is not unique to these examples; it is echoed across industries and reinforced by research.

Sector-specific analyses reveal that the challenge of aligning security practices with real-world human behavior is universal but manifests in distinct ways across different industries. In healthcare, high-pressure environments and frequent staff turnover contribute to mistakes like misconfigured access controls and accidental data sharing. In retail and education, limited training, the use of personal devices, and prioritization of convenience over security lead to frequent breaches through phishing and poor password hygiene. Telecommunications and financial services face their own unique risks, such as insider threats and policy violations, but the underlying issue remains the same: security frameworks often underestimate the complexity of human behavior and the influence of organizational culture on compliance and vigilance. These findings underscore that technical solutions alone are insufficient; effective cybersecurity must address the psychological, social, and operational realities of the workforce.

While legislative frameworks like the NIS2 Directive, EU Cybersecurity Act, and GDPR have made progress in mandating awareness training, risk assessments, and incident reporting, they often fall short of systematically embedding human-centric strategies into daily operations. These regulations recognize the importance of human factors but typically treat them as supplementary rather than foundational. The research in this thesis emphasizes that cybersecurity is inherently a socio-technical challenge, requiring the integration of behavioral, cognitive, and organizational insights into every layer of defense. Only by prioritizing human factors—through continuous education, a security-first culture, and systems designed for usability and psychological realities—can organizations achieve true resilience against evolving cyber threats. This holistic approach transforms employees from potential vulnerabilities into active defenders, fundamentally strengthening the organization’s security posture.

7 Recommendations

To effectively mitigate the impact of human factors in cybersecurity incidents, organizations must move beyond traditional, compliance-focused training and embrace a culture of continuous improvement. Ongoing, interactive education programs tailored to specific roles and evolving threat landscapes are essential. These programs should incorporate real-world simulations, behavioral feedback, and scenario-based exercises to help employees develop critical thinking skills and adaptive responses, especially under stress. By making training

relevant and engaging, organizations can ensure that security awareness becomes an integral part of daily operations rather than a one-time obligation.

Cultivating a security-first culture is equally vital. Cybersecurity values should be embedded into organizational norms, leadership behaviors, and everyday workflows. This involves clear and consistent communication of policies, establishing open channels for reporting incidents and near-misses, and recognizing employees who demonstrate secure practices. When leadership models and reinforces these values, employees are more likely to internalize them, fostering a sense of shared responsibility and vigilance throughout the organization.

Additionally, organizations should design systems and processes that acknowledge and accommodate human limitations. Simplifying user interfaces, automating routine security tasks, and implementing decision-support tools can help reduce cognitive overload, particularly during high-pressure situations. Regular risk assessments should be conducted to address sector-specific challenges, ensuring that both policies and technical controls are aligned with the unique human dynamics of each environment. Incident response plans must be updated to explicitly consider both technical failures and human errors, with frequent drills that test not only procedural readiness but also communication and decision-making under realistic conditions. By integrating these strategies, organizations can transform employees from potential vulnerabilities into active defenders, thereby significantly strengthening their overall cybersecurity posture.

References

Ajzen. I, (1991). The theory of planned behavior. Accessed 19 December 2024. https://www.sciencedirect.com/science/article/abs/pii/074959789190020T

Akbanov, M., Vassilakis, V G. & Logothetis,M D. (2019). Ransome detection and mitigation using software-defined networking: The case of WannaCry. Accessed 25 December 2024. www.sciencedirect.com/science/article/abs/pii/S0045790618323164

Amorosa,K., Yankson,B. (2023). Human Error – A Critical Contributing Factor in Data Breaches: A Case study of Higher Education. Accessed 17 June 2025. https://www.researchgate.net/publication/371849122_Human_Error_-_A_Critical_Contributing_Factor_to_the_Rise_in_Data_Breaches_A_Case_Study_of_Higher_Education

Arevalo,D., Valarezo,D., Fuertes, W., Cazares, M. F. (2023). Human and Cognitive Factors Involved in Phishing Detection: A Literature Review. ACM Computing Surveys. Accessed 20 November 2024 https://www.researchgate.net/publication/379714394_Human_and_Cognitive_Factors_involved_in_Phishing_Detection_A_Literature_Review

Awwad, R. (2020). ENISA: Human error is one of the major causes of security incidents. Accessed 17 June 2025. https://insidetelecom.com/enisa-human-error-is-one-of-the-major-causes-of-security-incidents/

Breachsense. (2024). Equifax Data Breach Explained: A Case Study. Accessed 16 January 2025. www.breachsense.com/blog/equifax-data-breach/

Burns. S, Roberts. L.D, (2013). Applying The Theory of Planned Behavior to Predicting Online Safety Behavior. Accessed 25 December 2024. https://www.researchgate.net/publication/235666025_Applying_the_Theory_of_Planned_Behaviour_to_predicting_online_safety_behaviour

Capaccioli, A. (2022). Human Affected Cyber Security (HAKS) Framework. Accessed 16 January 2025. https://ergonomics.org.uk/resource/human-affected-cyber-security-framework.html

CompTIA. (2025). Understanding the skills and training requirements of NIS2.Accessed 18 June 2025. https://www.comptia.org/en/blog/understanding-the-skills-and-training-requirements-of-nis2/

DYNAMO. (2022). Horizon Dynamo project: Building a resilient cybersecurity ecosystem. Accessed 4 March 2025. https://horizon-dynamo.eu

EPIC (Electronic Privacy Information Center) (2020). "Equifax Data Breach.". Accessed 15 December 2024. https://archive.epic.org/privacy/data-breach/equifax/

EUR-Lex. (2022). The Cybersecurity Regulation/ DIRECTIVE (EU) 2022/2555. Accessed 25 November 2024. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Union Agency for Cybersecurity (ENISA). (2022). European Cybersecurity Skills Framework (ECSF). Accessed 17 June 2025.
https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

European Commission. (2023). Shaping Europe's Digital Future-The EU Cybersecurity Act. Accessed 17 June 2025.
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

GDPRhub. (2025). Article 32 GDPR – Security of processing. Accessed 17 June 2025.
https://gdprhub.eu/Article_32_GDPR

Gregory, J. (2024). CISOs list human error as their top cybersecurity risk. Accessed 16 June 2025.
https://www.ibm.com/think/insights/cisos-list-human-error-top-cybersecurity-risk

Hancock, J. (2022). Psychology of Human Error: Understand the mistakes that compromise your company's cybersecurity. Tessian Research. Accessed 25 December 2024.
https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian-Research-Reports/%5BTessian%20Research%5D%20Psychology%20of%20Human%20Error%202022.pdf

IBM. (2019). The Role of Human Error in Cybersecurity Breaches. IBM Security. Accessed 15 October 2024.
https://www.ibm.com/blog/human-error-security-breach

IBM Security. (2023). Cost of a Data Breach Report 2023. Accessed 5 December 2024.
https://www.ibm.com/security/data-breach

ISO/IEC 27001:2022. Information Security Management Standards. Accessed 6 February 2025.
https://www.iso.org

Keepnet Labs. (2023). The Role of Human Error in Successful Cyber Security Breaches. Accessed 15 March 2025.
https://keepnetlabs.com/blog/the-role-of-human-error-in-successful-cyber-security-breaches

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. International Journal of Information Security, 24, Article 119. Accessed 20 November 2024.
https://link.springer.com/article/10.1007/s10207-025-01032-0

Kitchenham, B. (2004). Procedures For Performing Systematic Review. Accessed 16 June 2025.
https://www.researchgate.net/publication/228756057_Procedures_for_Performing_Systematic_Reviews

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. Applied Ergonomics, 40(4), 450–456. Accessed 24 December 2024.

NIS 2 Directive. (2024). The NIS 2 Directive|Updates, Compliance, Training. Accessed 25 March 2025.
https://www.nis-2-directive.com

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. Accessed 16 February 2025.
https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

NIST. (2023). Cybersecurity Framework Version 2.0: Integrating Human Factors. Accessed 22 December 2024.
https://www.nist.gov

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2022). Cybersecurity Awareness Training Programs: An Empirical Evaluation. Journal of Cybersecurity, 8(1). DOI Accessed 2 March 2025.
https://doi.org/10.1093/cybsec/tyac001

Prevezianou. M F. (2021). WannaCry as a Creeping Crisis. Accessed 25 December 2024.
https://www.researchgate.net/publication/351455866_WannaCry_as_a_Creeping_Crisis

Pollini. A, Callari. T.C, Tedeshi. A, Ruscio. D, Save. L, Chiarugi. F, Guerri. D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. Accessed 17 June 2025.
https://pmc.ncbi.nlm.nih.gov/articles/PMC8195225/

Reason, J. (1990). Human Error. Cambridge University Press. Accessed 22 December 2024. doi.org/10.1017/CBO9781139062367.

Ridley, D. (2012). The Literature Review: A Step-by-Step Guide for Students (2nd ed.). SAGE Publications. Accessed 25 December 2024

Sasse, M. A., Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? In L. Cranor & S. Garfinkel (Eds.), Security and Usability: Designing Secure Systems that People Can Use (pp. 13–30). O'Reilly Media. Accessed 12 December 2024.

ScienceDirect (2023). A Critical Review on Cybersecurity Awareness Frameworks and Training Programs. Procedia Computer Science, 207, 832-839 Accessed 22 November 2024.
https://www.sciencedirect.com/science/article/pii/S1877050924008329

Sjouwerman, S. (2024). Stanford Research: 88% Of Data Breaches Are Caused by Human Error. Accessed 23 December 2024.
https://blog.knowbe4.com

Smart, W. (2018). Lessons learned review of the WannaCry Ransomware Cyber Attack. Department of Health and Social Care, United Kingdom. Accessed 5 January 2025.
https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Steinberg, S., Stepan, A., & Neary, K. (2020). The Hacking of Sony Pictures: A Columbia University Case Study. Accessed 12 January 2025.
https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

Stegmaier, L. (2025). NIS2 and the human factor: your first line of defence against cyber attacks. Accessed 18 June 2025.
https://www.bechtle.com/de-en/about-bechtle/newsroom/it-solutions/2025/nis-2-and-the-human-factor

Svobodova, K. (2023). ISO/IEC 27001: The Scope, Purpose, and How to Comply. Accessed 5 November 2024.
https://www.safetica.com/blog/iso-27001-iec-27001-the-scope-purpose-and-how-to-comply

Think Tank European Parliament. (2020). Directive on security of network and information systems (NIS Directive). Accessed 24 January 2025.
https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198

Verizon. (2024). 2024 Data Breach Investigations Report. Accessed 18 March 2025. https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf

VikingCloud Team. (2025). Retail Cybersecurity Stats, Threats and Solutions For 2025. Accessed 17 June 2025. https://www.vikingcloud.com/blog/retail-cybersecurity-stats-threats-and-solutions

Willie, M M. (2023). The role of organizational culture in cybersecurity: building a security-first culture. Accessed 05 May 2025. https://ritha.eu/storage/336/5_jorit_WillieMM.pdf

World Economic Forum (2022). How user experience and behavioral science can guide smart cybersecurity. Accessed 2 November 2025. https://www.weforum.org/stories/2022/11/how-user-experience-and-behavioural-science-can-guide-smart-cybersecurity/

World Economic Forum (2024). We must reduce complexity to ensure strong cybersecurity. Here's why. Accessed 2 November 2025. https://www.weforum.org/stories/2024/10/strong-cybersecurity-reduce-complexity-risk-cyber/

Perplexity and ChatGPT were used in this thesis to edit the language of the text.