International Journal of Business and Technology Management
e-ISSN: 2682-7646 | Vol.6, No. 3, 226-241, 2024
http://myjms.mohe.gov.my/index.php/ijbtm

Understanding the Root Cause of Cybersecurity Incidents Through DuPont's Dirty Dozen Framework

Allen Peter Diman[1*], Titik Khawa Abdul Rahman[1]

[1] School of Graduate Studies, Asia e University, Selangor, Malaysia

*Corresponding Author: C70105150001@aeu.edu.my

Received: 18 May 2024 | Accepted: 20 August 2024 | Published: 1 September 2024

DOI: https://doi.org/10.55057/ijbtm.2024.6.3.22

Abstract: *Cybersecurity incidents, such as data breaches, pose a significant threat to organisations. Shockingly, 95% of these incidents occur due to human errors. Despite organisations making substantial efforts to reduce the likelihood of such occurrences through technological and non-technological means, the frequency of these incidents has been increasing. Previously, organisations relied on technology as the primary barrier to minimise cybersecurity incidents and achieve their objectives. Although research indicates that humans are the weakest link in an organisation's efforts to combat cybersecurity incidents, organisations still consider technology as the key to improving security defences. Therefore, the researchers suggest improving human interventions should precede technological means to overcome the problem. They propose that existing information security plans should consider human factors in cybersecurity risk management. Prioritising an understanding of human factors in managing information security can help organisations identify the relationships between various dimensions of human errors and cybersecurity incidents. To achieve this, the paper suggests solving the human factor problem in cybersecurity incidents by explaining how DuPont's Dirty Dozen framework, commonly used in aviation, can help understand why cybersecurity incidents and accidents occur. The framework lists twelve human behaviours that can be used to understand the relationships between various dimensions of human errors and cybersecurity incidents. By understanding these relationships, organisations can improve their cybersecurity strategies by anticipating, mitigating, and resolving issues more effectively and efficiently.*

Keywords: Cybersecurity, Cybersecurity Incidents, Dirty Dozen, Human Errors, Human Factors

1. Introduction

Data and information are organisations' two most valuable assets and, as such, must be securely guarded. For this reason, they are willing to undertake all possible measures to ensure that the security of the information remains intact. Thus, it is not surprising that these valuable data have been the target of cybercriminals. Cybercriminals' unauthorised access to helpful information has often led to numerous cybersecurity incidents. According to reports by Jurgens and Dal Cin (2024) and Natalucci et al. (2024), cybersecurity incidents remain a significant threat to many organisations globally. Jurgens and Dal Cin (2024) further highlighted that in 2023, almost one million cybersecurity incidents were reported around the globe, with Western Europe and the USA being the geographical areas with the most reported incidents. The same

institution also noted that the trends of cybersecurity incidents have increased yearly at an average of 20%. This shows that cybersecurity incidents will remain a threat for the foreseeable future. On the other hand, Patterson et al. (2023) mentioned that cybersecurity incidents can be catastrophic for business entities and government agencies. In this sense, the effect of such incidents can lead to financial losses, loss of competitiveness and damage to reputation. Patterson et al. (2023) quoted several examples that reflect this phenomenon. Among them is Facebook, which in 2021 suffered 533 million personal data breaches, while Google also suffered data breaches between 2015 and 2018 that resulted in USD350 million in court settlement. In both cases, Facebook and Google acknowledged that the incidents have eroded public perception of their business conduct. In addition, several examples (Table 1) of significant cybersecurity incidents have caught the attention of many in recent years.

Table 1: Recent Global Cases of Cybersecurity Incidents

Organisations	Description of Cybersecurity Incidents
Microsoft Exchange Server Hafnium Exploit: 2021	A state-sponsored threat actor using the name 'Hafnium' had successfully exploited vulnerabilities in Microsoft Exchange Server software, affecting thousands of organisations worldwide. Although the vulnerabilities were found in the software, the incident highlights the difficulty of responding quickly and patching known vulnerabilities, often hindered by human factors such as resource constraints and prioritisation decisions.
Verkada Camera Hack: 2021	Hackers have recently discovered that the login details of a super admin account were openly available on the internet. This allowed them to gain access to more than 150,000 security cameras across a range of locations, including prisons, hospitals, schools, and companies such as Tesla and Cloudflare. This incident highlights the significant risks associated with poor password management and the importance of imposing strict controls on privileged user accounts.
Accellion FTA Data Breach: 2020-2021	The incidents involve using The Accellion File Transfer Appliance (FTA), a file transfer service that has been around for a while. Unfortunately, attackers exploited the service to access sensitive information from many organisations. This incident highlighted the dangers of neglecting to update or replace outdated and vulnerable software. This human error is related to underestimating cybersecurity risks and can have serious consequences.
SolarWinds Orion Software Supply Chain Attack: 2020	A widespread cyber espionage campaign impacted various government agencies and private sector organisations globally. The perpetrators introduced malicious code into SolarWinds Orion software, a commonly used network management tool. Although it was mainly a complex supply chain attack, the incident highlighted the significance of implementing strict security measures in software development and the supervision of third-party vendors. These are areas where human oversight can have significant implications.
Twitter Bitcoin Scam: 2020	Several Twitter accounts, including those belonging to President Barack Obama, Vice President Joe Biden, and Elon Musk, were hacked. The attackers used social engineering techniques to lure Twitter employees into gaining access to the systems. Subsequently, hackers used the compromised accounts to promote a Bitcoin scam. This incident has underscored organisations' vulnerability to social engineering attacks and the importance of providing employees with practical security training and awareness programs.

Source: Center for Strategic and International Studies

A similar rise in cybersecurity incidents has also been reported locally. The Star Newsportal quoted a report by CyberSecurity Malaysia, which stated that 842.84GB of data losses were reported in the first half of 2023 (Yeoh, 2023). This is a significant increase of 27% compared to a similar period in 2022. The same article also gave several examples of notable cybersecurity incidents in 2022 and 2023. Among them include data breaches at Telekom

Malaysia, which resulted in data breaches involving 250,248 Unifi Mobile account holders. Another example is the hacking of the Maxis database, although the later investigation confirmed that no data leaks were reported in the incident. Also not spared are several government agencies. These include The Social Security Organisation (Perkeso) and the Election Commission (EC). In the case of EC, the agency reported that almost 13 million personal data were stolen from their database. For Perkeso, the incident has compromised more than one million of personal data.

To understand why cybercriminals managed to infiltrate the security measures put forth by the organisations, researchers looked at several perspectives as the probable causes of such incidents. In that sense, their studies can be categorised as looking at the issue from technical and non-technical perspectives. From a technical perspective, researchers looked at the technological elements that can enhance sensitive information and data scrutiny. This includes looking at the effectiveness of e-mail filters (Makkar et al., 2023) and firewalls (Mazzolin & Samueli, 2020), both of which can be used to prevent access to the information system using the technique of phishing e-mails. However, despite advancements in applying preventive technologies to deter cybercrime, the findings from various academic and non-academic sources indicate that such measures are yet to show their effectiveness in actual settings. This led researchers in the field of information security to look at the perspective of human characteristics and behaviour as the potential cause of cybercrime incidents. In that sense, previous researchers have looked at the elements of cybersecurity training to determine its effectiveness (Sabillon, 2021), the effect of demographics such as age, gender and level of knowledge (Branley-Bell et al., 2022) and personality differences (Kalhoro et al., 2022).

While many researchers agree that most cybersecurity incidents are due to human contribution and recent studies point to human errors as the leading cause (El-Bably, 2021; Triplett, 2022), the actual root causes behind such incidents remain largely unanswered. As highlighted by Hakimi et al. (2024), humans are still committing errors that lead to cybersecurity incidents despite getting the necessary training to prevent such incidents. Rahman et al. (2021) argued that demographic effects such as age, gender and level of knowledge have no significant role in cybersecurity incidents. However, a review of recent literature revealed that several researchers are in unison that one of the main contributing factors in cybersecurity incidents is the errors being committed by humans when dealing with the information system. This is supported by the fact that more than 95% of the successful cyber-attacks in 2022 were due to some form or a combination of several types of human errors (Patterson et al., 2023). Patterson et al. (2023) also highlighted that the ever-increasing complexity of cybersecurity environments further amplified the phenomenon humans face. Moreover, in recent times, cyber attackers have been able to exploit the vulnerabilities of computer system users by using various techniques and technologies. Instead of attacking the computer system directly, they manipulate users' minds using social engineering and cognitive hacking methods. According to Maalem Lahcen et al. (2020), attackers have successfully used these techniques to gain unauthorised access to many computer systems and networks globally.

2. Literature Review

In cybersecurity, studies involving human factors are usually associated with research that studies human capabilities and limitations and how the two aspects eventually lead to individual ‘actions’ or ‘inactions’ that can ultimately cause cybersecurity incidents (Pollini et al., 2021). Pollini et al. (2021) also added that any unmanaged or mismanaged errors committed from human behaviour's ‘actions’ or ‘inactions’ would frequently lead to undesired events such

as data breach incidents. In such instances, errors in handling information systems tend to increase the probability of cybersecurity incidents. Elaborating further, Kadena and Gupi (2021) and Rahman et al. (2021) stated that these errors can be spontaneous or part of an error chain. Thus, human factors researchers seek to understand information system users' physical, behavioural, cognitive, and social characteristics and their interaction with the systems. Recognising that information security issues are often caused by human error or decision-making mistakes is essential, as this can potentially become one of the most significant vulnerabilities for organisations (Kadena & Gupi, 2021). In light of this, Kadena and Gupi (2021) recommended that information protection solutions consider the possibility of human error and flawed decision-making when defending against cyberattacks.

Elaborating on human errors in cybersecurity incidents, Rahman et al. (2021) stressed that regardless of the type of error, the consequences of such errors would often depend very much on whether the information systems users would be able to detect and respond to the error before it leads to an undesired outcome or vice-versa. For this reason, cybersecurity practitioners should understand the reasons that could lead information systems users to commit errors before the incidents happen. This is important because, from the cybersecurity perspective, any potential human errors detected promptly and promptly responded to (i.e., adequately managed) will have the slightest tendency to cause cybersecurity incidents (Rahman et al., 2021). Also, proper human error management will often translate into increased human performance related to cybersecurity defence mechanisms. Therefore, by properly managing and understanding human factors in cybersecurity, cybersecurity practitioners can develop or enhance both learning and training mechanisms or methodologies related to cybersecurity (Rahman et al., 2021). In that respect, capturing the root causes of errors committed in cyberspace is as important, if not more important, than capturing the different error types committed by individuals (Pollini et al., 2021). It is interesting to see the chain of events that finally led to humans committing the errors. According to Pollini et al. (2021), some root causes that led to the undesired events can be quickly detected and resolved, thus becoming operationally inconsequential, while others can go undetected or mismanaged. If not detected and resolved, an undetected or mismanaged error can become a gap in cybersecurity defence and allow attackers to exploit such weaknesses. As such, organisations should put in place a comprehensive strategy that enables them to properly manage the cybersecurity environment with a strong emphasis on understanding human factors as a barrier to mitigating human errors. Literature offers rich resources that organisations can adapt for such purposes.

Over the past decade, several researchers (E.g., El-Bably, 2021; Hakimi et al., 2024; Nobles, 2022; Triplett, 2022) have conducted studies that focused on the relationships between human errors and cybersecurity incidents, and several conclusions can be derived from the findings of those studies. Human errors are a significant cause of cybersecurity incidents, and among the most common types of errors committed by individuals that lead to such incidents are accessing suspicious websites, oversharing information on social media, indiscriminately clicking on links, opening attachments from untrusted sources, sharing passwords, reusing passwords across multiple accounts, not securing personal electronic devices physically, using unauthorised external media, sending sensitive information via mobile networks, and failing to update software (El-Bably, 2021). El-Bably (2021) gave the example that organisations usually have a policy that prohibits sharing passwords and that those passwords must be unique and have some level of difficulty in guessing by external parties. However, findings revealed that 63% of the respondents routinely shared their passwords with others despite knowing that such actions could lead to incidents such as data leaks and, at the same time, violating the organisational policy on password management. El-Bably (2021) has also made similar

remarks regarding the sharing of passwords. Users of information systems often take the easy route when it comes to passwords, using weak passwords and the same one for different websites. Sharing passwords with others is also a common mistake that can lead to financial exploitation, especially for older adults who may be vulnerable to such attacks. As a result, it is advised that older adults be cautious and avoid trusting strangers on the internet. However, younger adults are also prone to sharing passwords, particularly for streaming services. These younger users who are so-called 'tech-savvy' may see cybersecurity as a hurdle to overcome. Sharing passwords is a significant security risk, as cybercriminals can use them on different websites once they can access one system. Therefore, it is crucial to use unique passwords for each website and avoid sharing them with anyone.

On the other hand, clicking on phishing e-mails is another type of human error routinely committed by information system users (Nobles, 2022). In cybersecurity, phishing e-mail is a type of e-mail that appears to be from a well-known source. However, its real intention is to target unsuspicious recipients either to reply to the e-mail or to open the attachments that came together with the e-mail (Maalem Lahcen et al., 2020). Doing so will open the attackers' access to the user's computer. Previous related studies have shown that individuals are easily tempted by the technique used in phishing e-mails. One example is a study by (Sarno & Neider, 2021), who discovered that over half of the participants in a phishing e-mail experiment fell trapped in phishing e-mails. Meanwhile, another study by Baillon et al. (2019) found that over 30% of government employees who have provided passwords click on the links in the experiment involving phishing e-mails. According to Baillon et al. (2019), one of the main reasons individuals clicked on phishing e-mails was the error of not paying attention to the characteristics of phishing e-mails. Baillon et al. (2019) further elaborated that this error could be caused by factors such as being distracted by other tasks and their lack of knowledge to identify phishing e-mails effectively. Separately, a study by Nobles (2022) revealed that individual complacency when handling e-mails was the primary cause of them likely clicking on phishing e-mails.

Another popular error humans commit that results in cybersecurity incidents is the delay in installing the necessary security updates in their software applications (Nwankpa & Datta, 2023). According to Nwankpa and Datta (2023), the outcomes of not installing updates on their software applications have caused many cases of infiltration by cybercriminals who have been able to manipulate the outdated security systems of users' information systems. This has resulted in the stealing of data and confidential information. In many cases, this occurred without the users' knowledge as the cybercriminals broke the weak defensive security system while surfing the Internet (Patterson et al., 2023). In some instances, the incidents occurred because the user's software application systems could not detect the potential dangers of exploited software applications such as trojan and worm viruses, which entered the computer system when the users clicked on the suspicious e-mails containing the viruses. Information systems users' negligence in updating software applications is the most detrimental human error. Furnell et al. (2020) revealed that most information breaches in U.K. companies resulted from standard outdated software protection systems. In a recent experiment on decision-making behaviour, Kuraku et al. (2023) found that people who take more risks are more likely to delay installing software updates. This discovery implies that risk-taking behaviour may contribute to software update procrastination. It is worth noting that installing software updates has received less attention than other security issues, such as sharing passwords and phishing.

Meanwhile, Triplett (2022) found that carelessly handling sensitive data is another common type of human error that can lead to cybersecurity incidents. The authors gave an example of

human error cases in this category where users were storing sensitive data without encryption, sending it over unsecured channels (like email or messaging apps) or neglecting to use secure protocols like HTTPS, which can expose the data to interception by unauthorised parties. The Office of the Australian Information Commissioner (OAIC) recently released a report highlighting the main reasons behind organisation data breaches. According to the report, careless actions such as sending personal information via email, accidental release or publication of personal information, and failing to use the 'blind carbon copy' (BCC) function while sending group e-mails are the most common causes of data breaches (Office of the Australian Information Commissioner, 2024). Clear policies must be provided to staff to prevent human error-causing security breaches (De Silva, 2023). This can be accomplished by categorising different data types as confidential or restricted, internal-only or public. In such cases, each category must be provided with specific guidelines that clearly instruct the staff on handling, transmitting, storing, and disposing data.

Finally, inadequate cybersecurity awareness among the users of information systems is also a common cause of cybersecurity incidents (Zwilling et al., 2020). For example, individuals with low-security awareness tend to be deceived by phishing e-mails by making them click on links or open attachments in e-mails (Zwilling et al., 2020). This act is hazardous as it could cause the person to accidentally install malware, thus exposing the organisation to an attack. Additionally, Zwilling et al. (2020) highlighted that giving unauthorised access to an organisation's device is another instance of low cybersecurity awareness. The rise of remote workplaces has brought a new challenge to company security, as it is possible for employees to unknowingly put their company's security at risk by allowing their family members to use corporate devices. While this may seem harmless, family members can take actions that could compromise the device's security, such as modifying settings and configurations, accessing confidential corporate data, installing unauthorised software and downloading malicious files. Therefore, educating employees about only allowing themselves to use corporate devices is crucial. In addition, it is essential to emphasise that these guidelines are not a reflection of the motives of their family members but rather an acknowledgement that people may unintentionally undermine security controls. Employees must also avoid sharing their device passwords with anyone (El-Bably, 2021).

Although the studies mentioned above have revealed that human errors were the primary causes behind the cybersecurity incidents, the current authors believe more in-depth studies must be carried out for several reasons. Firstly, no established human factors framework was applied in those studies. This can be a disadvantage as information security practitioners need a greater understanding of the root causes of why such incidents occur. In other words, readers of those articles are left with the question, 'What are the root causes or reasons that have led to those cybersecurity incidents? For example, in their study, El-Bably (2021) stated that the incident that led to data breaches might have been due to poor password management, while Furnell et al. (2020) suggested that outdated software protection systems may be the primary reason behind the information breaches incidents in many organisations. In both instances, questions need to be answered: what are the root causes behind poor password management and outdated software protection systems? Secondly, while past studies have applied some human factor elements as proposed in the paper, they are generally used without considering the whole list covered by the chosen framework. Thus, readers cannot discover whether those missed elements may have a role in cybersecurity incidents. Therefore, there is a need for a paper that can provide further explanation in a broader scope that encompasses a complete spectrum of human factors elements to describe why individuals may have made an error in the cases of cybersecurity incidents.

3. DuPont's Dirty Dozen Framework

DuPont's Dirty Dozen framework was first developed by Gordon Dupont in 1993 and aimed to aid aircraft maintenance personnel in identifying aviation incidents/accidents caused by human factors (Zafar, 2024). In this context, Dupont argued that through understanding human factors in those incidents/accidents, appropriate actions can be taken to reduce the errors, thus minimising the rate and severity of those incidents or accidents. This was done by listing twelve common human errors (thus comes the term 'Dirty Dozen), such as lack of communication, complacency, lack of knowledge and fatigue, which, if not mitigated properly, can lead to incidents and accidents (Zafar, 2024). In other words, these elements, according to DuPont, are the root causes that can explain 'why' such incidents or accidents occur. While DuPont's Dirty Dozen framework was initially conceptualised for use in the aviation industry, the framework has seen its application in other disciplines such as healthcare (Chatzi & Malliarou, 2023) and finance (Satyanarayana & Veluchamy, 2023) industry. Similarly, as mentioned earlier, several framework elements have also been applied in cybersecurity (e.g., Chowdhury et al., 2020; Triplett, 2022); however, to the current authors' knowledge, previous studies have not applied the framework in its entirety, but rather segmentally. As such, this paper attempts to fill the gap by applying all twelve framework elements as the potential root causes to explain the occurrence of cybersecurity incidents.

3.1 Lack of Communication

According to Maalem Lahcen et al. (2020), a lack of communication within an organisation can significantly undermine its cybersecurity defences, leading to incidents that could otherwise be prevented or mitigated. As such, Maalem Lahcen et al. (2020) argued that effective communication is essential at all levels, from IT teams to executive leadership, and across all departments to ensure that everyone is aware of potential cybersecurity threats and understands their role in maintaining security, and knows how to respond in the event of a security incident. In that sense, when cybersecurity teams or individuals fail to communicate about emerging threats, other parts of the organisation remain unaware of potential risks. This lack of shared threat intelligence means that employees might not be on the lookout for specific types of phishing e-mails, malware, or other attack vectors currently being used by cybercriminals. In addition, Maalem Lahcen et al. (2020) also commended that different departments may implement security policies inconsistently without effective communication. This inconsistency can create vulnerabilities, as attackers often target the weakest link in an organisation's security chain. Lack of communication will also diminish any effective enforcement of cybersecurity policies and controls, which usually require clear communication about employees' expectations, including acceptable use of company resources, password policies, and data protection guidelines (Safitra et al., 2023). Without this communication, employees might unknowingly engage in risky behaviours that can compromise security.

3.2 Complacency

On the other hand, complacency towards cybersecurity can be a significant factor leading to incidents, as it often results in a false sense of security, neglect of best practices, and underestimation of potential risks (Nwankpa & Datta, 2023). Nwankpa and Datta (2023) further highlighted that complacency can leave organisations vulnerable to attacks in a rapidly evolving cyber threat landscape. The authors gave an example where one of the most common manifestations of complacency is the neglect of regular software updates and security patches. In that sense, individuals or organisations might feel that since they have not been attacked yet, their systems are secure enough, leading them to postpone critical updates. This leaves systems vulnerable to known exploits that attackers actively seek out. Additionally, simple, easily

guessable passwords or reusing the same password across multiple accounts is a typical result of complacency (Nobles, 2022). As a result, it will make it easier for attackers to gain unauthorised access through credential stuffing or brute force attacks. Similarly, feeling overly secure in current measures can also lead to neglect in preparing for potential data loss scenarios (Nobles, 2022). Therefore, Nobles (2022) and Nwankpa and Datta (2023) suggested that regular backups and a clear disaster recovery plan are essential for minimising damage and restoring operations quickly after an incident. They stated that complacency in these areas could exacerbate the impact of ransomware attacks and data breaches.

3.3 Lack of Knowledge

Meanwhile, a significant risk factor for cybersecurity incidents is a need for more knowledge among employees, management, and IT staff regarding cybersecurity best practices, emerging threats, and security policies (Zwilling et al., 2020). According to Zwilling et al. (2020), this knowledge gap can lead to unintentional insider threats, where well-meaning individuals make mistakes that compromise their organisation's security. Moreover, individuals who do not understand the significance of strong, unique passwords and the use of password managers may reuse passwords across multiple accounts or choose easily guessable passwords, making it more straightforward for attackers to gain unauthorised access (Al-Alawi & Al-Bassam, 2020). Without awareness of how sophisticated phishing attacks have become, employees might not recognise the signs of a phishing email, such as subtle misspellings, unusual sender addresses, or urgent requests for information, leading them to inadvertently disclose login credentials or sensitive information. Similarly, a lack of knowledge about data protection policies and practices can result in mishandling sensitive data, such as storing it on unsecured devices, sharing it via unencrypted e-mails, or adequately disposing of sensitive information documents (Al-Alawi & Al-Bassam, 2020).

3.4 Distractions

Another common category of human error which can cause cybersecurity incidents is distractions. As stated by Maalem Lahcen et al. (2020), distractions in the workplace can significantly increase the risk of cybersecurity incidents by diverting attention away from critical security practices and protocols. This is further complicated because, in today’s fast-paced work environments, where multitasking is common and constant interruptions are the norm, the likelihood of making mistakes that could lead to security breaches rises (Maalem Lahcen et al., 2020). Maalem Lahcen et al. (2020) showed how distractions can lead to failure in recognising potential phishing attacks. Maalem Lahcen et al. (2020) argued that phishing attacks rely on deception to trick individuals into revealing sensitive information, downloading malware, or initiating unauthorised transactions. Coupled with distractions, it can impair an individual's ability to scrutinise e-mails or messages, making them more likely to fall for phishing scams (Maalem Lahcen et al., 2020). Another example is that distractions can cause a momentary lapse in judgment or a rushed decision, potentially leading to individuals clicking on a malicious link or attachment (Triplett, 2022). In an organisation, handling sensitive data often requires concentration and adherence to strict protocols. However, distractions can lead to mistakes such as sending e-mails with sensitive information to the wrong recipients, misconfiguring privacy settings, or failing to encrypt data before transmission securely (Triplett, 2022). Such errors can result in data breaches, exposing sensitive information to unauthorised parties. Additionally, regular security practices, such as locking computers when stepping away, using two-factor authentication, and regularly updating passwords, can also be overlooked or deemed too burdensome by employees when distracted or overwhelmed with other tasks (Triplett, 2022). This neglectful behaviour creates opportunities for attackers to exploit the cybersecurity system and practices.

3.5 Lack of Teamwork

In an ideal situation, the organisation should rely on solid employee teamwork to ensure the security protocols are intact (Sinlapanuntakul et al., 2022). Therefore, a lack of teamwork in cybersecurity can significantly elevate the risk of incidents within an organisation. It should be noted that cybersecurity is inherently a team effort, requiring coordination, communication, and collaboration among various stakeholders to safeguard information assets (Sinlapanuntakul et al., 2022) effectively. Without teamwork, Sinlapanuntakul et al. (2022) hypothesised that the action could lead to multiple vulnerabilities and gaps in an organisation's security posture. For example, when teams operate in silos without effective communication, the critical security information may not be shared across the organisation. This lack of information sharing can prevent teams from completely understanding the organisation's threat landscape, making it difficult to defend against attacks that require coordinated responses (Simonson et al., 2020). Moreover, without teamwork and coordination, different departments or units may implement security practices inconsistently. This inconsistency can lead to gaps in the organisation's security defences, where attackers can exploit the weakest link to gain unauthorised access to sensitive information (Simonson et al., 2020). Thus, Simonson et al. (2020) recommend that a coordinated effort should be one of the pillars of an organisation's effort to protect itself from potential cybersecurity incidents. Simonson et al. (2020) further elaborated that with solid teamwork, organisations should be able to form a barrier as an 'organisational' rather than as an 'individual', in which case the organisation may become vulnerable if the individuals do not possess the required skills to defend themselves against the cyber attacks.

3.6 Fatigue

Hakimi et al. (2024) describe fatigue as mental or physical exhaustion that impairs cognitive function and decision-making, significantly increasing the risk of cybersecurity incidents. This is because its impact on individuals working in cybersecurity and IT and general employees can lead to various vulnerabilities and errors. Elaborating further, the authors stated that fatigue affects concentration, memory, and attention to detail, leading to mistakes such as misconfiguration of security settings, improper handling of sensitive data, or overlooking signs of a security breach. In addition, even simple errors which can be avoided when well-rested can become significant security vulnerabilities when individuals are fatigued. Another reason that fatigue can cause cybersecurity incidents is that individuals are more likely to make poor decisions due to decreased cognitive function (Nifakos et al., 2021). This might involve skipping necessary security steps for convenience, using weak passwords, or deciding against updating systems or software because it feels like too much effort at the time. Another reason is that fatigue diminishes an individual's ability to stay alert, potentially leading to a delayed or missed detection of unusual activities indicating a cybersecurity threat, such as phishing e-mails, malware infections, or unauthorised access attempts (Nifakos et al., 2021).

3.7 Lack of Resources

Lack of resources, including insufficient funding, staffing shortages, outdated technology, and limited cybersecurity training, can impact an organisation's ability to protect itself against cybersecurity threats and respond to cybersecurity incidents (Safitra et al., 2023). This is because organisations may rely on outdated, less secure technology without sufficient investment in security infrastructure, lack critical security tools like firewalls and intrusion detection systems, or fail to implement strong encryption practices (Safitra et al., 2023). Consequently, this leaves systems more vulnerable to attacks. One illustration of such a problem is a need for more skilled cybersecurity professionals, leading to gaps in an organisation's security posture. As a result, essential tasks such as monitoring for threats,

conducting regular security assessments, and responding to incidents can be delayed or overlooked entirely due to understaffing. Meanwhile, Uchendu et al. (2021) stated that when cybersecurity resources are limited, an organisation's ability to quickly identify and respond to security incidents is compromised. Uchendu et al. (2021) gave an example where delays in response times can allow attackers more time to extract sensitive information, cause damage, or spread to other parts of the network. It is known that keeping software up to date is critical for security, but it requires resources to manage effectively. Organisations with limited IT staff may need help to keep up with patches and updates, exposing systems to known vulnerabilities that have been fixed in newer software versions.

3.8 Pressure

Pressure from workloads, deadlines, performance expectations, or other sources can significantly impact organisational and individual behaviour, potentially leading to cybersecurity incidents (Chowdhury et al., 2020). This pressure can manifest in various forms, affecting decision-making processes, attention to detail, and adherence to security protocols. One such scenario is when, under tight deadlines, employees may rush through tasks that require careful attention, such as configuring security settings, reviewing code for vulnerabilities, or ensuring that data is transmitted securely. This hurried approach increases the likelihood of mistakes leading to security breaches (Chowdhury et al., 2020). Cybersecurity professionals frequently advocated that keeping software and systems up to date is crucial for security, as updates often include patches for known vulnerabilities. However, under pressure to maintain productivity or uptime, individuals and organisations might need to pay more attention to these updates, leaving systems vulnerable to attack (Ogbanufe et al., 2021). In such events, pressure to quickly access systems and information can lead to poor password practices, such as using simple, easily remembered (and easily guessed) passwords or sharing passwords to expedite collaborative work, compromising security.

3.9 Lack of Assertiveness

Lack of assertiveness in cybersecurity contexts can lead to incidents and vulnerabilities by preventing individuals from taking necessary actions or speaking up about potential or actual security threats (McAlaney & Benson, 2020). Assertiveness in this context refers to the confidence and self-assurance with which individuals communicate their concerns, enforce policies, or adhere to best practices in the face of convenience or pressure to do otherwise (McAlaney & Benson, 2020). In environments where employees or management could be more assertive, there might be a reluctance to enforce security policies strictly. For example, an employee might notice a coworker violating security protocols (like sharing passwords or bypassing two-factor authentication) but feel too uncomfortable to address the issue or report it to their superiors (Schoenherr & Thomson, 2021). Similarly, individuals who lack assertiveness might notice suspicious activity or red flags indicating a potential security threat but hesitate to report them due to fear of being wrong, causing inconvenience, or stepping beyond the perceived boundaries of their authority (Schoenherr & Thomson, 2021). All these factors can cause delay, giving cyber attackers more time to inflict damage.

3.10 Stress

Stress plays a significant role in cybersecurity incidents, influencing individual behaviours and organisational vulnerabilities (Ambrozaitytė et al., 2021). The authors further stated that focusing on immediate tasks and pressures in high-stress environments can lead to oversights and lapses in cybersecurity practices. Ambrozaitytė et al. (2021) implies stress impairs cognitive function, making individuals more prone to mistakes. This can include falling for phishing scams, misconfiguring systems, sending sensitive information to the wrong recipient,

or inadvertently deleting essential data. This argument is also supported by Nobles (2022), who stated that errors under stress are among the leading causes of cybersecurity breaches. The authors gave an example where employees may take shortcuts that compromise security under pressure to meet deadlines or manage high workloads. This might involve using unsecured networks to save time, sharing passwords for ease of access, or bypassing multi-factor authentication or other security protocols. Stress and time constraints can also lead to procrastination or outright neglect of routine but critical security practices, such as applying software updates and patches (Nobles, 2022). According to Nobles (2022), these updates often contain fixes for vulnerabilities that, if left unpatched, can be exploited by cyber attackers. Another reason, according to the same author, is that continuous stress can lead to burnout, reducing an individual's vigilance and attentiveness to potential cybersecurity threats. In such a scenario, when employees are overwhelmed, they are less likely to scrutinise e-mails for signs of phishing or to recognise unusual activity that could indicate a security breach.

3.11 Lack of Awareness

Lack of awareness about potential cybersecurity threats or best cybersecurity practices and knowing the potential consequences of security breaches is also a factor that can lead to cybersecurity incidents (Triplett, 2022). This lack of awareness can manifest across individuals and organisations, contributing to vulnerabilities and increasing the risk of cyber attacks (Triplett, 2022). Triplett (2022) further elaborated that individuals are more likely to fall victim to these schemes without awareness of common tactics used by cybercriminals, such as phishing e-mails or social engineering. In addition, many users need to know the importance of strong, unique passwords for securing their accounts (Zwilling et al., 2020). This lack of awareness can lead to stronger passwords and password reuse, making it easier for attackers to gain unauthorised access. Similarly, a lack of awareness about the importance of software updates can lead individuals and organisations to delay or ignore them, exposing systems to exploitation by cybercriminals who quickly take advantage of known vulnerabilities (Zwilling et al., 2020).

3.12 Norms

Finally, workplace and individual norms can affect cybersecurity posture and lead or contribute to cybersecurity incidents in various ways (Goyal et al., 2019). These norms encompass the behaviours, practices, and attitudes towards cybersecurity that are considered acceptable or standard among individuals and within organisational cultures (Goyal et al., 2019). In organisations where security is not prioritised and emphasises speed or convenience over security, employees are more likely to take shortcuts that compromise cybersecurity (Wylde, 2022). This includes sharing passwords, using unsecured networks, or bypassing security protocols. Suppose the norm is to provide minimal or no cybersecurity training. In that case, employees might not recognise security threats (like phishing attempts) or know how to handle them, increasing the risk of incidents. In the same manner, if the norm is to ignore or delay software updates and patches, security vulnerabilities can remain unaddressed, leaving systems open to exploitation (Wylde, 2022), while a norm of hastily clicking on links without verifying their legitimacy can lead to malware infections or phishing (Goyal et al., 2019). This behaviour is hazardous when individuals carry it into their workplace, exposing organisational networks to threats.

4. Future Research Opportunities

The application of DuPont's Dirty Dozen framework to cybersecurity offers several opportunities for future research, given the framework's focus on human factors and their

previous contribution to safety incidents. This is particularly significant as translating this into the cybersecurity context can uncover insights into how human errors contribute to security breaches and how organisations can better prepare to mitigate these risks. Moreover, investigating how the framework manifests in different industries can reveal sector-specific vulnerabilities and strengths. For instance, comparing the prevalence and impact of these factors in healthcare, finance, and manufacturing could provide targeted recommendations for improving cybersecurity postures in these specific sectors. Additionally, exploring how organisational culture influences the occurrence and impact of the framework can yield insights into effective cultural and organisational change strategies for enhancing cybersecurity. Thus, this potential area of research could examine how leadership practices, communication norms, and employee engagement relate to cybersecurity vulnerabilities. Another research avenue is to assess the effectiveness of training programs designed to address the elements of DuPont's Dirty Dozens in cybersecurity defences. The findings from such a study can later be applied to help refine cybersecurity education and awareness initiatives, or the research could focus on identifying which training approaches are most successful in mitigating specific human errors, such as complacency or lack of awareness. Next, future research could investigate the role of technology in mitigating the risks associated with DuPont's Dirty Dozen. This could involve examining how advanced technologies like artificial intelligence (AI) and machine learning can be leveraged to compensate for human errors or enhance decision-making in cybersecurity. Future studies could also include conducting longitudinal studies to track how DuPont's Dirty Dozen elements contribute to cybersecurity incidents over time, which can offer insights into trends and the evolving nature of cyber risks. Findings from such research could help identify whether certain factors become more or less significant as technology and organisational practices evolve. Finally, future studies could delve deeper into the psychological and behavioural aspects that underlie DuPont's Dirty Dozen elements in cybersecurity incidents, as its findings could lead to more effective interventions. Understanding the cognitive biases, stressors, and motivational factors contributing to errors can inform the development of targeted measures to reduce their occurrence. By exploring these areas, researchers can contribute to a deeper understanding of the human factors in cybersecurity, leading to more robust defences against cyber threats. Based on the above suggestions, applying DuPont's Dirty Dozen framework in cybersecurity research should offer a structured approach to investigating and addressing the human elements that significantly influence an organisation's cyber resilience.

5. Conclusion

This paper shows that DuPont's Dirty Dozen framework can be valuable for organisations seeking to identify and mitigate human-centred vulnerabilities within their cyber defences. It is important to note that cybersecurity is not just a technical issue, as human factors play a critical role in organisations' security posture. The framework highlights how human behaviours and organisational culture can significantly impact cybersecurity effectiveness. Addressing the human elements of cybersecurity requires proactive measures, including conducting regular training across all levels of employees, enhancing a culture of security awareness, and putting in place policies that reduce risks associated with the Dirty Dozen factors. Therefore, effective cybersecurity defence requires a comprehensive approach that includes technical controls and addresses human factors. In that sense, organisations must strive for a balanced strategy that incorporates the principles outlined in DuPont's Dirty Dozen framework to mitigate risks. Additionally, the dynamic nature of cyber threats and the evolving landscape of technology mean that organisations must commit to continuous improvement. For that reason, the framework can help regularly assess and refine strategies to address human and

technical vulnerabilities. As illustrated earlier, leadership commitment and effective communication across all levels of an organisation are indispensable if an organisation wants to mitigate the risks associated with the twelve elements of DuPont's Dirty Dozen. This can be achieved by establishing a culture of shared responsibility for cybersecurity and empowering employees to contribute to cyber resilience. In conclusion, DuPont's Dirty Dozen framework highlights the importance of addressing human factors in cybersecurity. Organisations can significantly enhance their cyber defences by recognising and mitigating the risks associated with these factors. It underscores the need for a holistic approach to cybersecurity that integrates technical measures with efforts to improve human behaviour and organisational culture. As cyber threats evolve, understanding and addressing the human element becomes more critical in safeguarding information assets and maintaining operational integrity.

Acknowledgement
The author would like to thank the School of Graduate Studies, Asia e University (AeU), for supporting the publication of this paper.

References

Al-Alawi, A. I., & Al-Bassam, S. A. (2020). The significance of cybersecurity systems in helping manage risk in the banking and financial sector. *Journal of Xidian University*, *14*(7), 1523–1536. https://doi.org/10.37896/jxu14.7/174

Ambrozaitytė, L., Brilingaitė, A., Bukauskas, L., Domarkienė, I., & Rančelis, T. (2021). Human Characteristics and Genomic Factors as Behavioural Aspects for Cybersecurity. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Bioinformatics)*, *12776 LNAI*. https://doi.org/10.1007/978-3-030-78114-9_23

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PLOS ONE*, *14*(12). https://doi.org/10.1371/journal.pone.0224216

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, *2022*, 1–10. https://doi.org/10.1155/2022/2693080

Center for Strategic and International Studies. (2024, March). *Significant cyber incidents: Strategic technologies program*. Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chatzi, A. V., & Malliarou, M. (2023). The need for a nursing-specific patient safety definition, a viewpoint paper. *International Journal of Health Governance*, *28*(2), 108–116. https://doi.org/10.1108/ijhg-12-2022-0110

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behaviour: Theoretical Framework and countermeasures. *Computers & Security*, *97*, 101963. https://doi.org/10.1016/j.cose.2020.101963

De Silva, B. (2023). Exploring the relationship between cybersecurity culture and cyber-crime prevention: A systematic review. *International Journal of Information Security and Cybercrime*, *12*(1), 23–29. https://doi.org/10.19107/ijisc.2023.01.03

El-Bably, A. Y. (2021). Overview of the impact of human error on cybersecurity based on ISO/IEC 27001 information security management. *Journal of Information Security and Cybercrimes Research*, *4*(1), 95–102. https://doi.org/10.26735/wlpw6121

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6–12. https://doi.org/10.1016/s1361-3723(20)30127-5

Goyal, S., Ajmeri, N., & Singh, M. P. (2019). Applying norms and sanctions to promote cybersecurity hygiene. *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS*. https://doi.org/10.1773/aamas 47361.2019.9212872

Hakimi, M., Quchi, M. M., & Fazil, A. W. (2024). Human factors in cybersecurity: An in-depth analysis of User Centric Studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, *3*(01), 20–33. https://doi.org/10.58471/esaprom.v3i01.3832

Jurgens, J., & Dal Cin, P. (2024, January). *Global cybersecurity outlook 2023*. World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity. *Security Science Journal*, *2*(2), 51–64. https://doi.org/10.37458/ssj.2.2.3

Kalhoro, S., Ayyasamy, R. K., Jebna, A. K., Kalhoro, A., Krishnan, K., & Nodeson, S. (2022). How personality traits impact cyber security behaviours of SME employees. *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. https://doi.org/10.1109/3ict56508.2022.9990621

Kuraku, S., Kalla, D., Smith, N., & Samaah, F. (2023). Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks. *International Journal of Computer Trends and Technology*, *71*(11), 74–79. https://doi.org/https://doi.org/10.14445/22312803/IJCTT-V71I11P111

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioural aspects of cybersecurity. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00050-w

Makkar, A., Ghosh, U., Sharma, P. K., & Javed, A. (2023). A fuzzy-based approach to enhance cyber defence security for next-generation IoT. *IEEE Internet of Things Journal*, *10*(3), 2079–2086. https://doi.org/10.1109/jiot.2021.3053326

Mazzolin, R., & Samueli, A. M. (2020). A survey of contemporary cyber security vulnerabilities and potential approaches to Automated Defence. *2020 IEEE International Systems Conference (SysCon)*. https://doi.org/10.1109/syscon47679.2020.9275828

McAlaney, J., & Benson, V. (2020). Cybersecurity as a social phenomenon. *Cyber Influence and Cognitive Threats*, 1–8. https://doi.org/10.1016/b978-0-12-819204-7.00001-4

Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). *Rising cyber threats pose serious concerns for financial stability*. International Monetary Fund. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119

Nobles, C. (2022). Stress, Burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA – Journal of Business and Public Administration*, *13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of Cyber Awareness and cybersecurity policies among remote workers. *Computers & Security*, *130*, 103266. https://doi.org/10.1016/j.cose.2023.103266

Office of the Australian Information Commissioner. (2024, February 21). Data breach report highlights supply chain risks. *Newsroom.* https://www.oaic.gov.au/newsroom/data-breach-report-highlights-supply-chain-risks

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management*, *58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*. https://doi.org/10.1016/j.cose.2023.103309

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. *The 12th International Conference on Advances in Information Technology*. https://doi.org/10.1145/3468784.3468789

Sabillon, R. (2021). Delivering effective cybersecurity awareness training to support the organisational information security function. *Research Anthology on Privatizing and Securing Data*, 629–650. https://doi.org/10.4018/978-1-7998-8954-0.ch029

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

Sarno, D. M., & Neider, M. B. (2021). So many phish, so little time: Exploring email task factors and phishing susceptibility. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *64*(8), 1379–1403. https://doi.org/10.1177/0018720821999174

Satyanarayana P., & Veluchamy, R. (2023). Post-mortem analysis of Dirty Dozen companies referred by Reserve Bank of India to insolvency and bankruptcy code. *SN Business & Economics*, *3*(4). https://doi.org/10.1007/s43546-023-00462-z

Schoenherr, J. R., & Thomson, R. (2021). The cybersecurity (CSEC) questionnaire: Individual differences in unintentional insider threat behaviours. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. https://doi.org/10.1109/cybersa52016.2021.9478213

Simonson, R. J., Keebler, J. R., Lessmiller, M., Richards, T., & Lee, J. C. (2020). Cybersecurity teamwork: A review of current practices and suggested improvements. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *64*(1), 451–455. https://doi.org/10.1177/1071181320641101

Sinlapanuntakul, P., Fausett, C. M., & Keebler, J. R. (2022). Exploring team competencies in Cybersecurity. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *66*(1), 1110–1114. https://doi.org/10.1177/1071181322661496

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586. https://doi.org/10.3390/jcp2030029

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Wylde, A. (2022). Cyber security norms: Trust and cooperation. *European Conference on Cyber Warfare and Security*, *21*(1), 328–335. https://doi.org/10.34190/eccws.21.1.498

Yeoh, A. (2023, October 25). *Cybersecurity Malaysia Report: Government Sectors suffered the most data breaches, while Telcos spilled over 400GB of data in H1 2023*. The Star. https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023

Zafar, M.F. (2024). Safety Management - Human Factor. In: Khan, A.A., Hossain, M.S., Fotouhi, M., Steuwer, A., Khan, A., Kurtulus, D.F. (eds) *Proceedings of the First International Conference on Aeronautical Sciences, Engineering and Technology*. ICASET 2023. Springer, Singapore. https://doi.org/10.1007/978-981-99-7775-8_42

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, knowledge and behaviour: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269