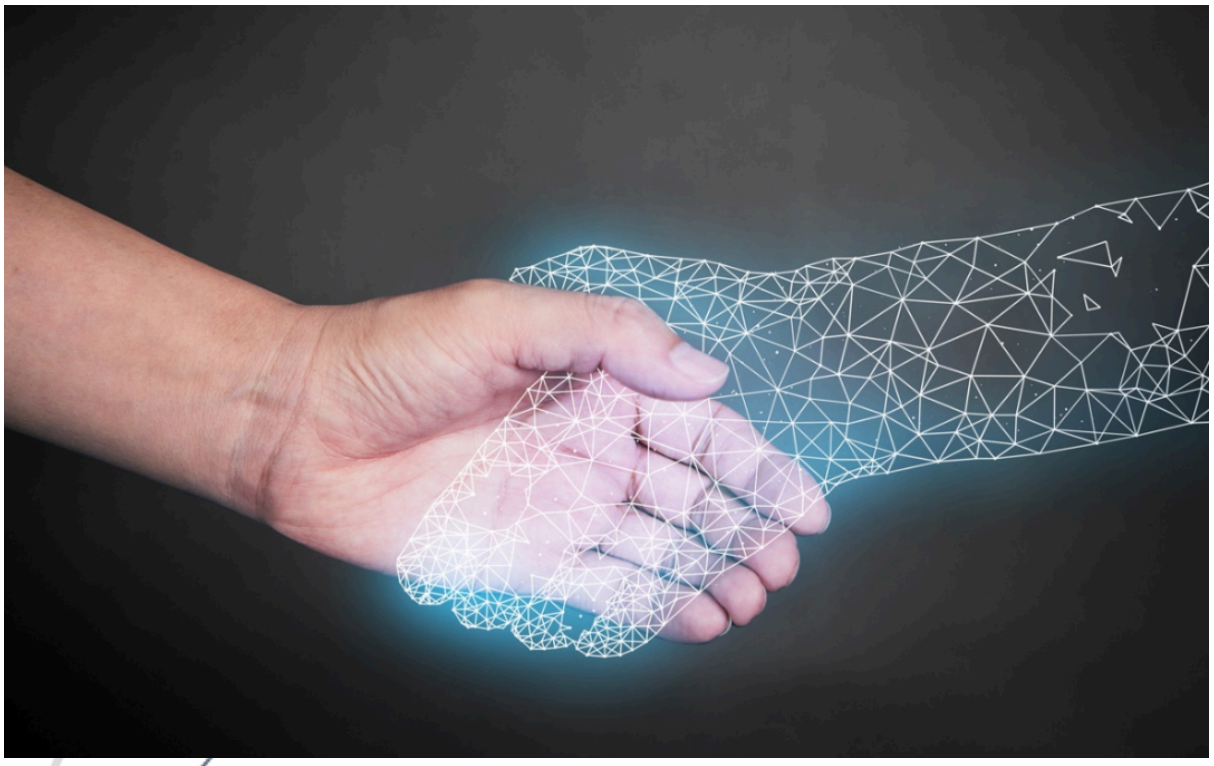
User Behaviour Cyber Risk & Training & Awareness Programme

Zero Day Security, Ltd.



Colin Cooper
R00240295
Emerging Cyber Trends (COMP 8063) 2022/23 - Assignment 1

1. Executive Summary

Zero Day Security (ZDS) is a cybersecurity company that provides threat detection and remediation services to its customers. This makes it both a potential valuable target for malicious actors as well as making the financial and reputational cost of a breach extremely high.

ZDS has invested heavily in technological solutions that minimise the risk of a successful attack. However, two recent breaches that used social engineering as the attack entry point to compromise employee credentials have caused concern among executives that the largest weakness in the company's security posture is in its human resources. In both cases, common psychological techniques were used by hackers to bypass the best judgement of employees and in one of the instances, suppliers' information was accessed through compromised employee credentials. Although no major financial damage was caused, these incidents serve as a warning that investment in the company's non-technological security posture is badly needed.

A post-incident review revealed critical weakness in the human element of security, including lack of clear documented security policies; poor awareness of how to report security incidents; poor password management practices; and a lack of general knowledge about psychological tactics used by social engineering hackers and how to recognise these techniques and respond appropriately.

Using the Security Behaviour Intentions Scale (SeBIS) framework, this report recommends a formalised security awareness training programme that combines both general security (passwords, device security, systems updates, and proactive awareness) and role-specific policy and security training for all new and untrained employees; as well as a programme of periodic refresh training and regular reinforcement throughout every employee's tenure with the company. These programmes are designed to support and prepare employees to appropriately recognise and react to suspicious activities and ensure they know how to report them, while avoiding desensitising employees to security messaging.

Table of Contents

1. Executive Summary 1
2. Introduction 3
2.1. Background 3
2.2. Recent Social Engineering Breaches 3
2.3. Purpose 4
3. Evaluation of user behaviour on the company's cyber risk profile 4
3.1. Overview 4
3.2. General impacts of user behaviour on cyber security risk profile 5
3.3. Specific impacts of user behaviour on cyber security risk profile at ZDS 7
4. Security Awareness Training (SAT) Programme 8
4.1. SAT Development Process 8
4.2. Principles of Programme Design 8
4.3. Material Development: General Security In-Class Training Modules 10
4.4. Reinforcement Training Modules 11
4.5. Post Implementation Review 11
5. Overall Conclusions 11
6. Bibliography 12

2. Introduction

2.1. Background

Zero Day Security ("ZDS") is a Managed Detection and Response (MDR) provider specialising in outsourced cybersecurity monitoring, threat detection and remediation services to its customers. ZDS's typical customers are small enterprises with between 50 and 250 employees for whom a dedicated in-house Security Operations Centre (SOC) would not be financially feasible. Through a shared service model, ZDS is able to dilute SOC operational costs - such as the physical secure SOC environments, hardware, networking, threat analyst staff costs, and threat detection and forensics software licensing costs - among its customer base to offer a service that scales to the needs and budgets of small organisations.

ZDS had gross revenues of €15.2m in 2021 from 350 customers mainly based in the UK, Ireland, and Sweden from which it made an operating profit of €3.6m in the same period. The company has three centres of operation: in Cork (Ireland), Reading (UK) and Stockholm (Sweden). All three sites have fully operational interconnected Security Operations Centres.

ZDS also has its own internal operational functions and systems including HR, payroll, finance, sales, marketing, and procurement departments. Each department uses a variety of applications to perform its day-to-day functions, some of which are cloud-based, and others hosted in a small on-premises data centre that is physically located in Cork.

As a security vendor, ZDS is extremely sensitive to any breach of its information system environments and has invested heavily in threat prevention and detection technologies that include secure service edge (web gateway, CASB and Zero Trust Network Access) to facilitate remote working, internal firewalls, network segmentation, advanced anti-malware, honeypots and threat detection technologies. ZDS recognises the potential reputational damage of a breach, and that the nature of its business makes it a significant target for attackers.

2.2. Recent Social Engineering Breaches

During the Q4 2022 Quarterly Business Review (QBR), the company's CISO disclosed that several threats had been detected and successfully mitigated. When questioned on how these threats successfully bypassed the technological defences, the CISO revealed that the primary entry point of the attacks was through social engineering where employees had been contacted by phone or email and induced to disclose their login credentials or install malware.

In the first case, a senior sales manager was contacted by someone claiming to be from the IT department and needing the employee's credentials to urgently apply critical patches to the employee's laptop. When the employee hesitated to give the credentials, the attacker held the prospect of disciplinary action and named the CISO and the employee's direct reporting manager. Although the employee gave his credentials to the attacker and allowed him to install an application on his laptop, he realised shortly afterwards that the nature of the call was suspicious and contacted the IT department who quickly locked his account and

quarantined his laptop. Attempted use of the compromised credentials was detected shortly afterwards by the Security Operations Centre.

In the second case, a junior Accounts Payable employee who had recently joined the company was sent an email requiring them to update their password for a SaaS payments service. The email contained a link to a realistic, but fake, login page where the employee provided their existing password and an MFA token. Once provided, the attackers were able to use this information to log in to the SaaS service. The compromised credentials were only discovered during an investigation into login activity from a suspicious IP address detected by the Security Operations Centre.

While both threats were ultimately quickly detected and mitigated without significant loss, these incidents have raised concerns about the quality of the company's defence against social engineering and threats caused by poor employee security behaviours.

2.3. Purpose

The purpose of this report is to:

- Critically evaluate the impact of poor user behaviour on the cyber risk profile of the company.
- Propose a security training and awareness programme tailored to the needs and unique challenges of ZDS.

3. Evaluation of user behaviour on the company's cyber risk profile

3.1. Overview

The critical role of technological solutions such as firewalls, intrusion detection and prevention products, endpoint protection applications and threat detection products in improving an organisation's cyber security posture is well understood. To protect their critical assets, organisations will work with their IT departments and third-party providers to implement solutions and architectures that reduce the likelihood and impact of a security breach.

However technological solutions do not provide sufficient levels of security and cannot protect information assets from a breach that is caused by an employee performing an action that they are permitted to do but shouldn't. For example, it may be reasonable for an Accounts Payable team member to update the payment details for a supplier, but if that change is initiated from a fraudulent phone call, the last line of defence may be that team member themselves. So-called "social hackers" are also adept at psychological manipulation, using techniques that abuse deep-seated human instincts, such as:

- **Baiting:** Appealing to a person's greed (e.g. Nigerian Prince), vanity (romance scams) or curiosity (clickbait headlines and secret admirer scams) to get them to act.
- **Inducing Panic:** Deceiving someone into believing that something bad will happen imminently if they don't act immediately. Creating a sense of panic often causes humans to override their better judgement. For example, financial scammers have used such tactics to convince individuals to move

money out of their bank accounts in the belief that if they don't, the money would be at risk.

- **Fake Authority:** Using a false position of trust (such as a boss, a senior company employee, a bank official or tax authority) to induce a person to perform an action such as divulging sensitive information, moving money, or purchasing gift cards. This is a modern-day equivalent of an old confidence trick that exploited the tendency of humans to obey commands that come from people in recognised uniforms of authority [1].
- **Empathy:** Abusing natural human instincts to help someone in trouble. For example, social engineering hackers have used fake crying baby background noises [2] and "hard-case" backstories to induce others to bypass normal authentication protocols.

These psychological manipulation techniques are often point-in-time attempts to cause an employee to engage in poor security behaviour. However poor user security behaviour can manifest in more passive ways that lower the security posture of the organisation that can be difficult to detect.

For example, an employee may use a common password for work and personal devices or have poor patch management on a personal device that is used to access company services. A recent example of this was at LastPass [3] in early 2023 where a threat actor stole customer and corporate data by installing keylogger software on a LastPass employee's personal device through an unpatched media player application. This keylogger recorded the employee using a master password and MFA token and this allowed the attacker to access the company's source code and customers' password vaults stored in the cloud. In this case, the employee was never directly contacted by the attacker but was subject to a targeted reconnaissance that eventually exploited poor patch management and poor threat protection practices on a personal device.

This example provides a salient warning for ZDS which has supported remote working through use of business and personal devices for accessing internal and cloud services from outside the corporate network. Like LastPass, ZDS is an attractive cybersecurity industry target for threat actors looking to blackmail the company, disrupt operations or as a jump point for targeting its customers.

3.2. General impacts of user behaviour on cyber security risk profile

The Security Behaviour Intentions Scale (SeBIS) [4], describes user attitudes to security across four sub-domains:

- Password Generation
- Updating (keep software up to date)
- Device Securement (locking devices)
- Proactive Awareness (considering security alerts and acting upon them)

These subdomains serve as a good framework to define types of user behaviour and what impacts these may have on the company's cyber security risk profile.

Sub-domain & associated positive behaviours	Impact of poor behaviours
Password Generation	
• Regular password change • Different passwords for different identities • Complex passwords	• Increased exposure time if a password is unknowingly compromised • Corporate user account compromise if any personal user account is compromised • Easily brute-forced password cracking
System Updates	
• Prompt install of OS updates • Use latest versions of software • Anti-virus update	• Exploitation of known OS & application vulnerabilities • Failure of anti-virus software to detect new threats
Device Security	
• Automatic screen locking when not in use • Password or passcode on laptops and tablets • Manually lock screen when stepping away • PIN / passcode for mobile phones	• Physical compromise of device • Hijacking of authenticated active sessions by a third party
Proactive Awareness	

• Verify before clicking a link • Recognition of legitimate websites • Use of https / SSL before submitting data to a website • Mouse-over before click • Report a suspected security issue quickly • Recognise suspicious request over email, phone, or other communication medium[1]	• Malware download • Phishing • Disclosure of sensitive information through unencrypted transit • Delayed reaction from Computer Emergency Response Team (CERT) or Security Operations Centre (SOC) to a triggered threat resulting in further system and data compromise • Fund redirection • Credential theft

3.3. Specific impacts of user behaviour on cyber security risk profile at ZDS

The two incidents in the CISO's Q4 2022 QBR report highlight that employees can and will be targeted by malicious actors and that technological solutions on their own are insufficient to provide adequate security of the organisation's information assets. In both cases, attackers successfully compromised the Identify and Authentication Management controls which included Multi-Factor Authentication and strong password complexity and expiry policies that were in force through Group Policies. The potential for poor user behaviour to significantly undermine the investments made in technology and policy solutions can no longer be considered theoretical for ZDS. Investments that improve user behaviour before, during, and after an attack are required to minimise this potential.

While post-incident reviews did highlight the need to tighten some of the Zero Trust Network Access policies, these cannot be considered as having completely mitigated similar future attacks.

[1] This is not actually part of the SeBIS questionnaire, but in my view should be.

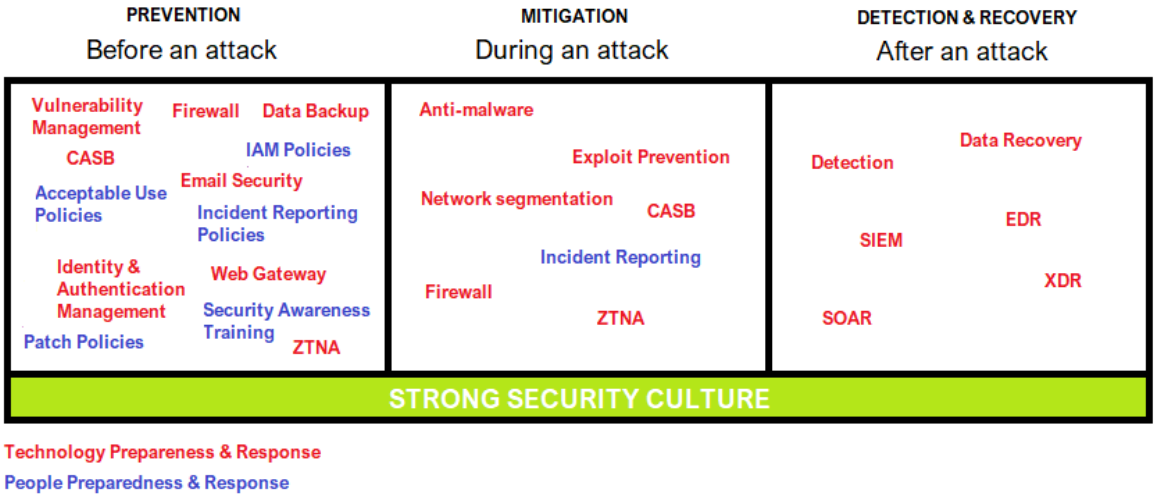


Figure 1 - End-user readiness for a cyber-attack is a significant factor in attack prevention and early mitigation

Specifically, deficiencies were discovered in the following areas:

- A lack of clarity of policies around acceptable use of user-owned devices to access company resources. The usage of such devices had grown significantly due to the rise in remote working, without formal written guidance for employees on anti-malware protection and patch management.
- While an Incident Reporting policy was documented, it was not part of all employees' onboarding training, and it was not easy to find in the company's intranet portal.
- Password policies were enforced through group policy and active directory management, but these did not prevent users from using the same passwords across company and personal accounts. It was also found that password expiry policies that required employees to change passwords every 90 days were being subverted through trivial and predictable alterations to expiring passwords. Worryingly, the frequent password expiry was causing some employees to store passwords in physical notebooks and unencrypted documents. No formal training had been provided to employees on best password practice, nor on the potential consequences for poor password management.
- Lastly, no formal training has been provided to employees to develop a security culture within the company that encourages healthy questioning of authority, recognition of unusual instructions and common social engineering tactics, or rewards for contributing to a positive security culture.

A Security Awareness Training (SAT) programme could significantly improve the security posture of the company by address the above areas through focus on:

- Providing awareness, accessibility, and clarity to employees around acceptable use policies for personal devices and accounts
- Detection and avoidance of common social engineering attacks such as phishing, smishing, vishing, tailgating, water holing and baiting.

- Providing awareness of when, clarity on how, and a safe environment for reporting security incidents and concerns.

A key challenge of any SAT programme will be achieving the right balance between the frequency of security messaging reinforcement and creating a habituation problem where the desired response is decreased due to "*repeated exposure to the same stimulus over time*" [5]. For example, GDPR-driven cookie notifications are now routinely accepted and dismissed by website users due to "consent fatigue" [6] which undermines their very purpose under GDPR to give those users information and choice.

4. Security Awareness Training (SAT) Programme

4.1. SAT Development Process

NIST [7] recommends the development of a Security Awareness Training programme in a number of phases:

- Programme Design
- Material Development
- Programme Implementation
- Post Implementation

4.2. Principles of Programme Design

To develop an effective Security Awareness Training programme, the following principles will apply:

- **Timeliness.** All new employees will be required to partake in the programme as part of their initial induction through an on-site in-personal training event. Refresh training should be triggered by a change in role, promotion or on a minimum frequency of 18 months.
- **General and job specific.** As well as covering general topics such as secure password management and device security, the SAT for each department needs to be tailored to the job role being done by the employee. For example, all Accounts Payable employees should be trained on the protocols for changing payment details for suppliers, while IT personnel should be trained around policies for creating and securing new cloud virtual machines and services.
- **Real-world examples of the consequences of insecure behaviour.** By providing employees with real examples of poor user behaviours such as clicking on phishing links, the risk of those employees engaging in the same behaviour is reduced. [7]
- **Regularly refreshed.** Where new forms of threat become more common, the training material should be refreshed regularly to ensure it does not become out of date and that employees are aware of the latest trends in social engineering and user behaviour driven breaches. This helps to ensure that the impact of the training – particularly where it is being retaken by an employee – is retained and not diluted by habituation and desensitisation.

- **Supported by regular positive and negative reinforcement outside of the training room.** All too often, security behaviour reinforcement is only done through avoidance of negative consequences. If an employee does not click on a phishing link, there is usually no reward for reinforcing the learned behaviour except for the avoidance of a reprimand. Using a reward system for exhibition of positive security behaviour should increase adherence to security behaviours [5].
- **Use simulated experience to reinforce learning.** Users who have a practiced response to threats such as phishing demonstrate increased compliance with security policies [7]. Simulated threats such as phishing / smishing can both reinforce learning while also providing the CISO with real data about the state of readiness of different employee groups for a threat that uses poor user experience as an attack vector, allowing the SAT programme to be adjusted in terms of its content and frequency.

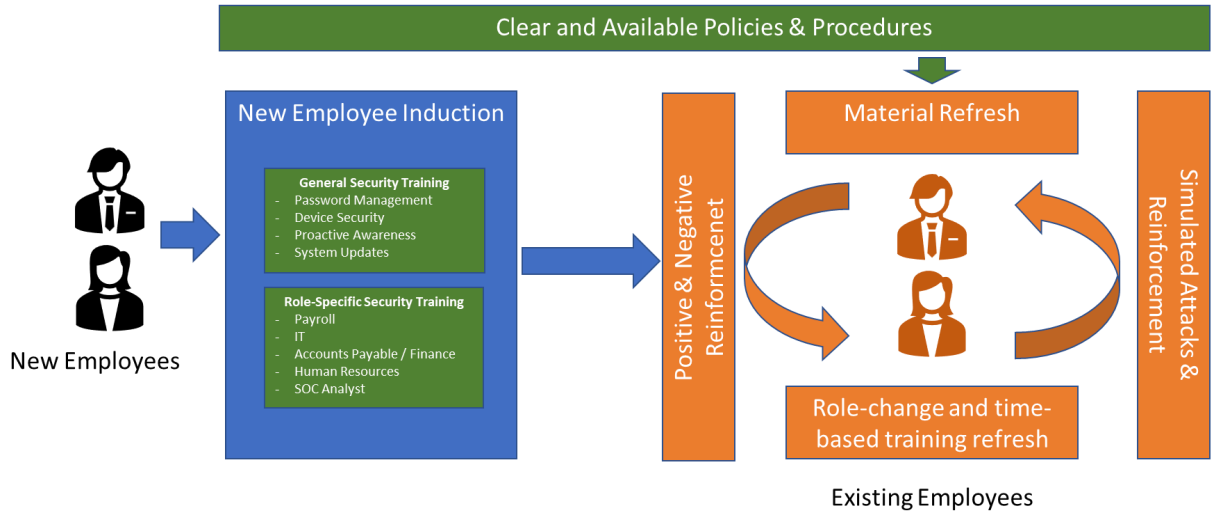


Figure 2 A model for initial and continued security awareness learning for employees is one that is timely and appropriate for the employee's role and tenure in the company and is reinforced through simulated events.

4.3. Material Development: General Security In-Class Training Modules

Password Management Module	**Device Security Module**
• Company password policies covering expected password behaviours such as no password sharing; no disclosure; no recording of passwords in insecure formats; limits on use of password manager software; password re-use. • Real world attack simulations such as fake IT engineer calling to request credentials and MFA.	• Company device security policies for both personal and company-issued devices such as not sharing PINs or passcodes; screen locking best practices. • Requirements for personal devices such as device encryption; anti-malware and firewall; VPN. • Best practices for configuration of different classes of personal devices and use on insecure public Wi-Fi hotspots. • Awareness of processes for reporting lost or compromised devices. • Real world examples of shoulder-surfing and free Wi-Fi honeypot compromises.
Systems Updates Module	**Proactive Awareness Module**
• Company patch management policies for personal and company-issued devices • Real world examples of how out of date software on personal devices can compromise organisational security (e.g., LastPass hack / Plex Media Player)	• Role-play based training covering common scenarios and tactics used by social engineering hackers. • Understand the psychological weaknesses that are exploited by these hackers, how to recognise them. • How to react to and report a suspected social engineering attack. • Company policies and best practices on social media such as LinkedIn and Facebook.

4.4. Reinforcement Training Modules

Phishing / Smishing Simulations	**Publish Success Stories**
• Regular testing of employee awareness and alertness to potential phishing attacks. • Positive reinforcement for successfully recognising an attack through a redeemable reward points programme. It's important that "false positive" reports are taken seriously and that employees feel that they will be supported if they report a suspicion – even if that suspicion turns out to be a false alarm. • Additional support for employees failing to recognise an attack. It's important than employees don't feel punished if they fail a phishing test in case this leads to a reluctance to report real security failures in the future.	• Where employees successfully recognise a real-world attack, provide public recognition and company e-newsletter mentions to help retain a strong culture of security, provide positive reinforcement to those employees, and provide ongoing examples to all employees of the kinds of suspicious behaviour that should be reported.

4.5. Post Implementation Review

The SAT should be considered a living programme that is regularly reviewed and updated to reflect technology advances, trends in human-vector attacks, as well as internal organisational and role changes. Measurements from simulated attacks and reviews of real-world attacks should be considered when assessing the effectiveness of the training and related materials.

While occasional employee surveys may be useful to assess the effectiveness of the SAT programme, care should be taken in interpreting results that are self-assessed and which employees may feel that they need to give the "right" answer rather than an accurate one.

5. Overall Conclusions

Due to its position in the cybersecurity industry, ZDS is particularly strongly motivated to protect its information systems assets across cloud services, on-premises data centres and end-user devices. Its investments in technological solutions such as malware protection, firewalls and secure service edge solutions, the company has experienced breaches that exploited common social engineer tactics that caused employees to unintentionally disclose their credentials.

It's clear that the company's security investments are undermined by poor user security behaviour and that investment in the human dimension of its security infrastructure is undertaken. A Security Awareness Training programme should be developed to ensure that:

- Security-related policies are developed, documented, made very clear and accessible for employees.
- The policies form the basis for general security and role-specific training modules.
- The general security covers the four SeBIS sub-domains of Password Generation, Updating, Device Securement and Proactive Awareness.
- All employees take this training programme during their employee onboarding, role-changes and at a minimum of 18 months intervals to reinforce and update the security learning objectives of the modules.
- Training programmes are not abstract or theoretical but use a combination of information exchange, real-world examples of the consequences of poor security behaviour and role-playing of social engineering attacks.
- The training is reinforced through regular simulated attacks such as phishing emails that allow employees to practise their learned skills and provide management with visibility of any potential weak spots to be addressed.
- A positive security culture is created whereby reporting of suspicious behaviour is encouraged, recognised, and rewarded; and where employees feel empowered to report security mistakes early and are not motivated to hide or ignore them.

6. Bibliography

[1] L. Bickman, "The Social Power of a Uniform," *Journal of Applied Social Psychology,* vol. 4, no. 1, pp. 47-61, 1974.

[2] "The Art of Social Engineering: A Crying Baby and a Phone Call," Cybrary, 27 12 2017. [Online]. Available: https://www.cybrary.it/blog/2017/12/art-social-engineering-crying-baby-phone-call/. [Accessed 14 03 2023].

[3] J. Weatherbed, "LastPass reveals attackers stole password vault data by hacking an employee's home computer," The Verge, 28 02 2023. [Online]. Available: https://www.theverge.com/2023/2/28/23618353/lastpass-security-breach-disclosure-password-vault-encryption-update. [Accessed 14 03 2023].

[4] S. Egelman. and E. Peer, "Evaluation of user behaviour on the company's cyber risk profile," in *Security Feedback & Warnings CHI*, Seoul, 2015.

[5] A. Maurushat, "The Role of User Behaviour in Improving Cyber Security Management," *Frontiers in Psychology,* 18 6 2021.

[6] “Your users are suffering from consent fatigue and here’s why,” Aceptio, 19 01 2023. [Online]. Available: https://www.axeptio.eu/en/blog/meet-a-cookie/your-users-are-suffering-from-consent-fatigue-and-heres. [Accessed 15 03 2023].

[7] M. Wilson and J. Hash, “Building an Information Technology Security Awareness Program,” National Institute of Standards and Technology, 2003.

[8] A. Baillon, J. d. Bruin, A. Emirmahmutoglu, E. v. d. Veer and B. v. Dijk, “Informing, simulating experience, or both: A field experiment on phishing risks,” *PLoS ONE,* 2019.