

Part 2. Human-Centred Security



1. Authentication design

Passwords have historically been considered the de facto authentication mechanism for granting access to systems that have access control requirements. They were implemented largely due to the ease with which they could be administered by technical staff and utilised by end users. Unfortunately, this mechanism now proves to be easy to compromise, particularly when not implemented with any minimum password complexity requirements (Ometov et al, 2018), with users frequently selecting inherently weak passwords where no password strength criteria are enforced (Hall, Hoppa and Hu, 2023).

1.1 Reported weaknesses in password authentication mechanisms

A survey conducted by the Department for Science, Innovation & Technology (DSIT) found that almost a third of businesses surveyed did not implement a company policy that enforced the use of strong passwords (DSIT, 2024). This survey further found that this proportion has been gradually increasing over the course of the last four years, as demonstrated in Figure 1.

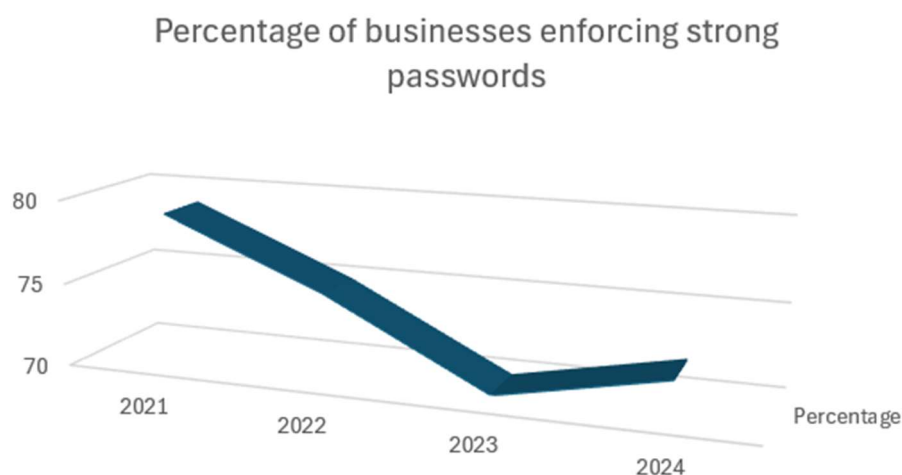


Figure 1: line graph showing the decline of strong password policies in business (DSIT, 2024).

Password complexity policies (usually mandating a password contain a minimum number of characters, as well as a combination of upper- and lower-case letters, numbers and symbols) are intended to act as a technical control that forces users to select passwords that cannot be guessed easily by attackers, thereby mitigating the risks posed by brute force attacks, such as those described in Table 1. If successful, these attacks can result in credential theft, data breaches, and privilege escalation, which could further result in website defacement or take-over, or the deployment of malware or ransomware within a corporate network.

Table 1: types of brute force attack.

Attack type	Description
Simple brute force	An attacker uses a small list of common passwords against a user account. A successful login indicates that a genuine credential pair has been discovered.
Dictionary	An attacker uses a large “dictionary” of common words, phrases, and character combinations against a user account. A successful login indicates that a genuine credential pair has been discovered. The dictionary in use can be one obtained or created by the attacker, allowing for custom word lists to be used that include details specific to the user (e.g. date or place of birth).
Password spraying	A single password is used against many user accounts. A successful login indicates that a genuine credential pair has been discovered.
Credential stuffing	A credential pair (username and password) are entered against many different services. A successful login indicates that a genuine credential pair has been discovered.
Rainbow table	An attacker uses a very large table of encoded common words, phrases, and character combinations, trying each in turn against a user account. A successful login indicates that a genuine credential pair has been discovered.

In practice, the enforcement of password complexity policies can actually increase the risk of falling foul of one of these attacks, as users will continue to choose dictionary words, or words that could be associated with their account, supplemented with numbers and special characters, to fit the requirements of the policy (Habib et al., 2018). Furthermore, the use of a password expiration element to a complexity policy has been found to compound this problem, with users reusing old passwords with minor alterations when forced to update their password (Shay et al., 2016). It is for these reasons that the current password guidance from the National Cyber Security Centre (NCSC) specifically advocates against the use of password complexity policies for systems where users create their own passwords (NCSC, 2018).

1.2 Authentication recommendation

Multi-factor authentication (MFA) is the main technical control recommended by the NCSC in its guidance for identity and access management (NCSC, 2021). MFA takes advantage of the premise that authentication methods can take the form of one of several factors, of which the three most common are:

- Something you know (e.g. a password or PIN).
- Something you have (e.g. a hardware/software token, or an authentication app).
- Something you are (e.g. a fingerprint or iris recognition).

MFA is a single authentication method that implements more than one factor as part of its authentication process. A user must provide the correct values for each factor involved in the process or the request for authentication will fail, severely hampering the effectiveness of the brute force attacks discussed previously. MFA can also be effective in mitigating the risk from some social engineering attacks, specifically those designed to ascertain username and password combinations from unsuspecting users (usually delivered by phishing e-mails or malicious websites), as the passwords themselves are useless without the secondary authentication information (Momoh, Adelaja and Ejiwumi, 2023).

Ometov et al (2018) described the evolution of MFA as originating from single-factor authentication (SFA) through to two-factor authentication (2FA), before emerging as MFA as it is currently perceived. This evolution can be seen, as described by Ometov et al (2018), in Figure 2:

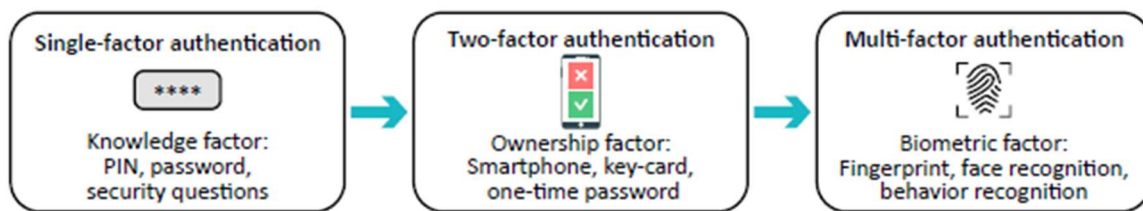


Figure 2: evolution of authentication methods from SFA to MFA (Ometov et al., 2018).

It is the recommendation of this report that ScottishGlen look to enhance their existing password-only authentication architecture with 2FA as the first step of a long-term project to implement MFA. It is further recommended that ScottishGlen consider the use of a smartphone app as the provider of the secondary factor - this is based on the following reasoning:

- Most (if not all) of their employees will already have a smartphone available to them (personal or corporate).
- There are a number of existing cloud suppliers that can provide the service, so additional infrastructure will not be required.
- Existing suppliers have already developed the apps required to support the functionality, so app development will not be required.
- Existing suppliers have developed their systems with built-in security measures, so can be considered as secure (subject to corporate review of third-party practices).
- Many existing solutions have the ability to implement a third biometric factor as part of the authentication process, enabling the extension into MFA seamlessly and with minimal additional technical work.

The introduction of a second factor would greatly mitigate the risks posed by the current SFA design ScottishGlen has in place, particularly with regards to social engineering attacks aimed at unsuspecting users. Whilst the threat posed by non-malicious/unintentional insiders could be considered similarly mitigated in this way, it should be noted that an SFA (and any resultant MFA) implementation would be ineffective against malicious/intentional insider threats.

2. Insider threats

A 2024 report by Gurukul found that nearly half of the organisations they surveyed saw an increase in insider attacks over the twelve months prior to the survey being conducted (Gurukul, 2024), as demonstrated in Figure 3:



Figure 3: changes to insider threat attack occurrences (Gurukul, 2024).

The survey further found that the financial consequences of a successful insider threat attack can be significant, with the most common response from organisations suggesting such an attack typically costs up to half a million dollars (US), with some reporting losses of over two million dollars (Gurukul, 2024). Recovery is also reported to be slow, with almost half of organisations reporting that it takes a week or longer to recover to business-as-usual following an insider attack (Gurukul, 2024). With these factors in mind, attacks from insiders have been recognised as one of the most serious threats posed to all organisations (Georgiadou, Mouzakitis and Askounis, 2022).

2.1 Scope of potential insider threats

Despite the significant threat that insider threats pose to organisations, it has been claimed that there is still much work to be done in understanding the human factors that drive these threats (Prabhu and Thompson, 2022). Many attempts have been made to develop frameworks and taxonomies that will enable further understanding (Renaud et al., 2024). Prabhu and Thompson (2021) posit that whilst further classification of insider threats should be based upon the threat types demonstrated in Figure 4, simple categorisation of the intent of an attacker is not sufficient. They further argue that in order for organisations to gain better understanding of insider threats (and therefore how to mitigate against them), consideration should be given to factors that contribute to the motive of an attacker.

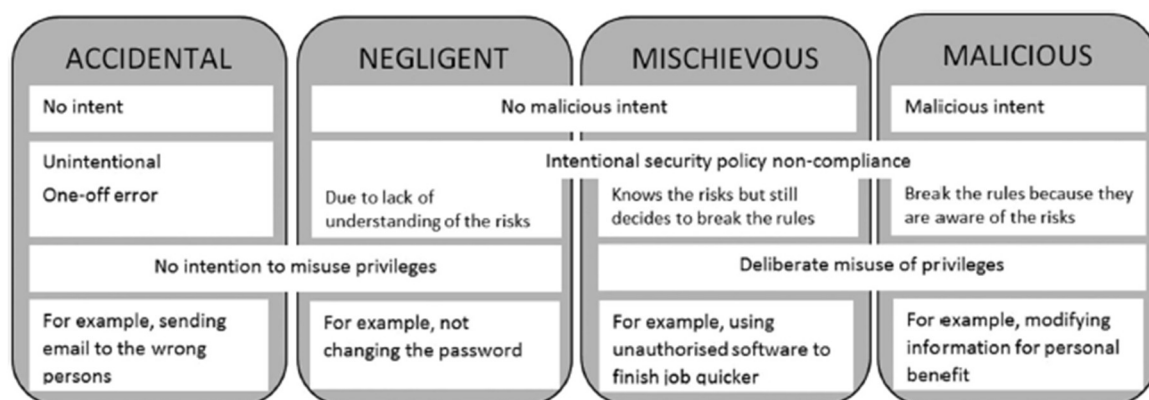


Figure 4: insider threat classifications (Prabhu and Thompson, 2021).

The need to consider the motivations (intentional or otherwise) of an attacker is given further consideration by Georgiadou, Mouzakitis, and Askounis (2022). Their work presents the argument that insider threat motivations can be driven by the inherent cyber security culture within the organisation that they may present a threat to, as well as considering external environmental factors (Georgiadou, Mouzakitis, and Askounis, 2022). The resulting model proposed can be seen in Figure 5. It posits that insider threats cannot simply be addressed by technical controls, and that addressing the risks posed should be an organisation-wide issue.

Level	Dimension	Domain	Insider Threat Factor
Individual	Attitude	Employee Satisfaction Employee Profiling	1 – Dissatisfaction 3 – Enterprise role 5 – Employee profile
	Awareness	Policies and Procedures Awareness Roles and Responsibilities Awareness	10 – Policies and roles awareness 10 – Policies and roles awareness
	Behavior	Policies and Procedures Compliance Security Agent Persona	8 – Policy violation 2 – Personality predispositions 7 – Sense of entitlement
	Competency	Security Behavior Security Skills Evaluation Training Completion and Scoring	4 – Concerning behavior 11 – Situation awareness 11 – Situation awareness
Organizational	Assets	Personnel Security	6 – Access Controls
	Access & Trust	Access Management	6 – Access Controls
	Defense	Information Security Policy & Compliance	9 – Auditing
	Security Governance	Audit Logs Management Incident Response & Management	9 – Auditing 9 – Auditing

Figure 5: cyber security culture model and insider factors (Georgiadou, Mouzakitis and Askounis, 2022).

Though the work conducted in both of these studies provides valuable insight into developing affective countermeasures against insider threats, Renaud et al (2024) argue that further categorisation is needed to ensure that the entire range of insider threats is considered. Their taxonomy expands upon existing research and includes consideration for remote work environments and emerging technologies. The resulting grouping can be seen in Figure 6:

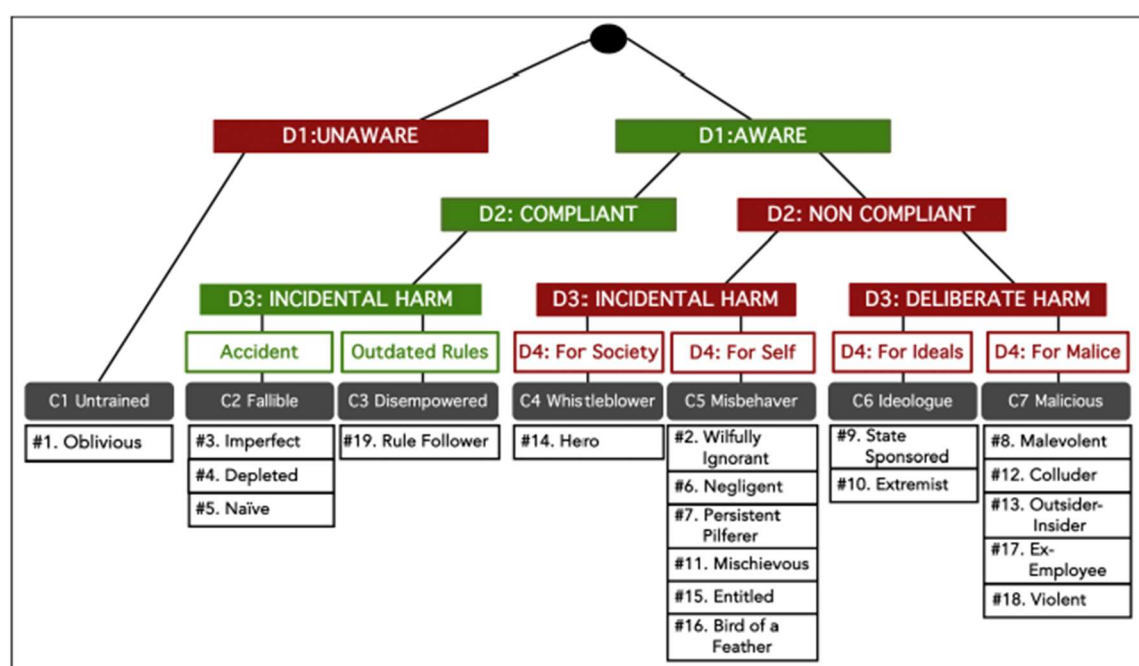


Figure 6: insider threat groupings (Renaud et al., 2024).

When examining the taxonomy presented by Renaud et al (2024), the examples of what can be considered an insider threat demonstrate a vast scope of behaviours that need to be addressed in order to consider the risk mitigated. It also becomes clear that there is a far greater range of risk from aware insiders than from non-aware. Furthermore, it can be seen that the scope of threats presented by non-compliant insiders is larger than that of those from compliant insiders. This variety poses a particular challenge for organisations as no mitigation will be successful against all types of insider threats (Renaud et al., 2024), and as such, it can be observed that a range of countermeasures should be implemented, both technical and behavioural in nature (Georgiadou, Mouzakitis and Askounis, 2021; Prabhu and Thompson, 2022; Renaud et al., 2024).

2.2 Recommendations

Based on the existing research and the particular circumstances surrounding the data breach at ScottishGlen, it is recommended that the organisation implement the following:

Technical controls

- Device access control.
- Data loss prevention (DLP).

Behavioural practices

- Security education and training awareness program (SETA).
- Whistleblowing policy.
- Pre-employment screening.

It is acknowledged that it is infeasible to completely mitigate the risks posed by all categories of insider threat (Renaud et al., 2024), and it is for this reason that the two technical controls have been included in this report. It is important that organisations are able to prevent the actions of an insider being successful in the event that they have been unsuccessful in identifying the risk proactively (Alsowail and Al-Shehari, 2022). Device access control, which can block the use of unauthorised devices on corporately owned endpoints, could prove effective against unintentional insider threats (e.g. a user plugs a USB device containing malware into a company laptop) and act as a hindrance to intentional insider threats attempting to exfiltrate data from corporate infrastructure. The implementation of data loss prevention, which can detect the exfiltration of sensitive data, could provide additional assurances on this latter example.

The Insider Threat report identified that almost a third of organisations surveyed considered the lack of training and awareness as a key driver behind the rise in insider attacks (Gurukul, 2024). Furthermore, a nuanced and adaptable training program that runs regularly and is audited for relevance is recognised as an important countermeasure against both non-aware and aware insider threat types (Renaud et al., 2024). A SETA that includes both employee training for recognising threats and managerial training for recognising the signs of potential malicious insiders would assist in the mitigation of threats from both aware and non-aware insider types. This latter point could be enhanced with the implementation of a whistleblowing policy (i.e. a policy empowering staff to report evidence of wrongdoing by other staff members without fear of reprimand) for all employees at the company.

Pre-employment screening is an effective preventative measure that could prevent a malicious insider ever gaining access to corporate assets (Renaud et al., 2024). The implementation of this countermeasure would mitigate against several of the intentional insider threat types. The introduction of this countermeasure would also demonstrate that improving the cyber security posture of the organisation is a responsibility that does not fall solely within the remit of the technical or security teams, potentially driving improvements to ScottishGlen's over-arching cyber security culture (Georgiadou, Mouzakitis and Askounis, 2021).

3. Challenges

There are three types of challenges facing the team tasked with adopting the recommendations in this report:

- Technical implementation.
- User acceptance.
- Business requirements.

The technical requirements can be partially mitigated with the use of established third-party applications - there are numerous vendors available that provide solutions for the implementation of MFA, device access control and DLP, as well as those that offer comprehensive and adaptable training programs for staff. The use of a “ready-made” package to administer these countermeasures would greatly reduce the resources required to implement them, though resource would be required to customise and maintain them to the needs of the organisation.

User acceptance of new technologies can be difficult to address, particularly if users perceive the newcomer as too restrictive or obstructive to their normal workload (Ometov et al., 2018). This challenge would be particularly applicable to the introduction of MFA and a SETA program, though could extend to the implementation of device access control and a whistleblowing policy. It is important for ScottishGlen to adopt a “no-blame” organisational policy to garner user support in communications around the latter three of these countermeasures, empowering users to understand that mistakes should be seen as opportunities for learning development (Renaud et al., 2024). User resistance to the introduction of MFA may be more challenging to counter, and ScottishGlen should look to consider usability and user preferences when implementing this (Ometov et al., 2018).

Finally, business requirements at ScottishGlen could introduce conflicting priorities with regards to financial and other workload-specific needs. In this instance, time and resource should be allocated to conduct the appropriate risk assessments and business cases, which will allow the organisation to evaluate its priorities in an informed and security-conscious manner.

References

- Alsowail, R.A. and Al-Shehari, T. (2022) 'Techniques and countermeasures for preventing insider threats', *PeerJ. Computer Science*, 8, pp. 938- Available at: <https://doi.org/10.7717/peerj-cs.938>.
- Department for Science, Innovation & Technology. (2024) *Cyber security breaches survey 2024*. Available at: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024> (Accessed: 2 March 2025).
- Georgiadou, A., Mouzakitis, S. and Askounis, D. (2022) 'Detecting Insider Threat via a Cyber-Security Culture Framework', *The Journal of Computer Information Systems*, 62(4), pp. 706–716 Available at: <https://doi.org/10.1080/08874417.2021.1903367>.
- Gurucul (2024) *Insider Threat Report*. Available at: <https://go1.gurucul.com/2024-insider-threat-report> (Accessed: 14 March 2025).
- Habib, H., Emami-Naeini, P., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N. and Cranor, L.F. (2018) *User Behaviors and Attitudes Under Password Expiration Policies. Fourteenth Symposium on Usable Privacy and Security*, Baltimore, MD, USA, 12-14 August, 2018.
- Hall, R.C., Hoppa, M.A. and Hu, Y. (2023) 'An Empirical Study of Password Policy Compliance', *Journal of The Colloquium for Information Systems Security Education*, 10(1) Available at: <https://cisse.info/journal/index.php/cisse/article/download/156/156>.
- Momoh, I., Adelaja, G. and Ejiwumi, G. (2023) *Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution* Piscataway, NJ, USA: IEEE.
- NCSC (2021) *Identity and access management*. Available at: <https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management> (Accessed: 9 May 2025).
- NCSC (2018) *Password policy: updating your approach*. Available at: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach> (Accessed: 12 March 2025).
- Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y. (2018) 'Multi-Factor Authentication: A Survey', *Cryptography*, 2(1) Available at: <https://doi.org/10.3390/cryptography2010001>.
- Prabhu, S. and Thompson, N. (2021) 'A primer on insider threats in cybersecurity', *Information Security Journal*, 31(5), pp. 602–611 Available at: <https://doi.org/10.1080/19393555.2021.1971802>.
- Renaud, K., Warkentin, M., Pogrebna, G. and Van Der Schyff, K. (2024) 'VISTA: An inclusive insider threat taxonomy, with mitigation strategies', *Information & Management*, 61(1) Available at: <https://doi.org/10.1016/j.im.2023.103877>.
- Shay, R., Komanduri, S., Durity, A.L., Huh, P., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F. (2016) 'Designing Password Policies for Strength and Usability', *ACM Transactions on Information and System Security*, 18(4), pp. 1–34 Available at: <https://doi.org/10.1145/2891411>.