Universal Barriers

TIME

to complete tasks and processes at a reasonable pace

People need enough time to complete tasks and processes at a reasonable and comfortable pace for them.

TIME

TIME

People need enough time to complete tasks and processes at a reasonable and comfortable pace for them. The length of time people need will vary according to their circumstances and the task requirements. Being time-pressured can significantly affect people's concentration and attention. Being short of time, either due to the circumstances or the complexity of the task, can make people anxious or frustrated.

Being time-pressured or short of time, can result in delays, mistakes, bad decisions, or actions that bypass security systems and features. Some people may find it challenging to manage tasks that time out or Multi Factor Authentication (MFA) features with short time limits.

Universal Barriers

FINANCE

to afford secure devices, products, and services

The financial costs associated with cyber security can pose a significant barrier to compliance and secure behaviours.

FINANCE

Financial costs associated with cyber security can pose a significant barrier to compliance and secure behaviours. This can include limited access to secure personal devices, as well as to up-to-date and compliant hardware and software. For individual employees, the costs of broadband and mobile data allowances to enable working from home or offsite, and/or the need to own a secure smartphone for MFA, can be prohibitive.

Additionally, there is the cost of commuting into an office or main site to comply with security rules (e.g., password updating). Larger departments may have financial leverage in procuring commercial cyber security contracts, but smaller government organisations and arms-length bodies may only be able to afford the most basic/minimal viable products and services.

Universal Barriers

ACCESS

to secure devices, software, infrastructure, and connections

Access to secure devices and to a strong and reliable internet connection are essential to working securely.

ACCESS

ACCESS

Access is a broad and cross-cutting barrier that is likely to impact cyber security particularly where off-site and remote working is part of normal service delivery. To work securely, people will need access to a smartphone, more than one device (for MFA), and strong reliable internet connection. In smaller government departments and arms-length bodies, employees may only have access to basic phones or refurbished laptops with limited functionality.

Local council employees in rural areas may have unreliable Wi-Fi and mobile coverage. Government employees who regularly work off-site may only be able to update passwords from a secure on-site device and, therefore, may seek non-secure workarounds. People need barrier-free access not only to buildings, to technology, and to infrastructure, but also to appropriate support (including troubleshooting).

Universal Barriers

INTERACTION

to communicate with cyber security systems and professionals

Barriers to effective interaction in cyber security include physical usability as well as basic communication issues.

INTERACTION

Barriers to effective interaction in cyber security contexts include physical usability as well as basic communication issues. People may not fully understand technical language or jargon. People may struggle to understand written or verbal instructions. Poor Wi-Fi or mobile connections can also hinder communication. Reading text on a small phone screen can be difficult. People can struggle to create and remember secure passwords.

People can lack the physical dexterity needed to interact with the required equipment to access security systems (e.g. with some keyboards and screens). Effective and secure interaction is about both accessibility and usability – ensuring that people of all abilities and capabilities can use essential security controls, including through robust assistive technology.

Universal Barriers

SELF-CONFIDENCE

to try new ways of working and to ask for help or advice

Navigating complex tasks, understanding processes and instructions, setting up and using new systems and software, all require confidence to complete successfully.

SELF-CONFIDENCE

Individuals' confidence in their own abilities and skills can affect their use and full engagement with cyber security measures. Navigating complex tasks, understanding processes and instructions, and setting up and using new systems and software all require confidence to complete successfully. People lacking in confidence, whether in general or about specific skills in themselves or their teams, may avoid tasks they perceive as difficult.

They are more likely to find new equipment, systems, and processes a challenge and prefer the familiar – including older legacy systems, services, and components. When an incident occurs, they may be reluctant to seek external expert help. Over-confidence may also present a barrier where an individual or a team considers its security to be invulnerable or unlikely to be targeted.

Universal Barriers

AWARENESS

to know what to do, who to talk to, and where to go for help

People need to know what they need to do to keep their part of the business secure, and where to go if they encounter a problem.

AWARENESS

People need to be aware of the latest cyber security guidelines and to understand how these directly relate to them and their role within the organisation. People don't always know how to keep their part of the business secure or what to do if they encounter a problem. People aren’t always aware of what security classifications mean and how these relate to forwarding emails, or to document storage, etc.

Lack of awareness of available support is a fundamental barrier to people seeking help in a timely way, especially if they don’t know it exists in the first place. Lack of awareness of the alternative options (e.g., alternative MFA, cloud services, Microsoft products, NCSC toolkits) can also pose barriers to effective security.

Universal Barriers

COMPREHENSION

to comprehend the basics of cyber security culture, risks, and resilience

People need to understand the risks of clicking on a suspicious link or sharing passwords, and why they need backups and business continuity plans.

COMPREHENSION

People may not always fully understand what is expected of them, or how they can help keep their part of the business secure. They may not understand the risks or consequences of clicking on a suspicious link or of sharing passwords. They may not appreciate the importance of backups and business continuity plans. Limited understanding of cyber security terminology and jargon can also be a barrier to secure behaviours, and can affect anyone at any level.

Being able to process information can be compromised because of health conditions and special circumstances, including stress. People may also struggle to comprehend information when they are required to concentrate for long periods, to multitask, or to hear several important points at the same time.

Universal Barriers

EMOTIONAL STATE

to feel positive about and take an active part in security culture

People who are under stress, tired, overwhelmed, anxious, or angry, will find complex security tasks cognitively challenging.

EMOTIONAL STATE

EMOTIONAL STATE

People need the cognitive and emotional capacity to focus on cyber security. Designs and systems that assume everyone can give security their full attention may ask too much of people. Where cyber security measures create friction or require additional effort, they can trigger negative emotions. People experiencing stress, fatigue, anxiety, or anger may find any complex task cognitively challenging.

We also know that emotional triggers are cleverly manipulated in most phishing attacks and scams. A cyber incident at any scale will have an emotional impact on those involved, posing a potential barrier to their full engagement with recovery and resilience processes. Individuals' emotional states can vary across people and over time.

Universal Barriers

TRUST

to rely on the right people, systems, devices, and services

Too much trust in familiar security tools can pose risks, but lack of trust is also a barrier to secure behaviour.

TRUST

TRUST

Lack of trust is a barrier to cyber security in many contexts. People must be able to trust guidance, products, intelligence, and alerts. Government organisations must demonstrate to their employees that they are trustworthy and that security goals benefit employees as well as the organisation's mission. Data and automated systems must be trustworthy. Lack of trust in cloud computing or AI tools may prevent organisations from taking advantage of secure innovations.

Over-confidence in familiar security tools can also pose risks. People may not trust that reporting systems are designed to help them, and fear blame or punishment if they report clicking a malicious link, a data leak, or breach. Likewise, people may not trust the agencies deployed to offer crucial support and guidance enough to report their concerns.

Universal Barriers

EVIDENCE

to authenticate identities and access secure services

People need to be able to provide the right evidence and authentications to work securely when in the field or off site.

EVIDENCE

EVIDENCE

Good evidence and data sit at the heart of good cyber security, but evidence can become a barrier in some contexts and circumstances. For example, every individual within an organisation is typically required to provide evidence to authenticate their identity several times during a workday. Providing the evidence necessary to authenticate when working in the field or at another site can be a barrier to access.

Like access, evidence is a wide-ranging and cross-cutting barrier which is likely to impact cyber security in organisations particularly where out-of-office and remote working is essential and part of normal service delivery.

Universal Barriers

ENTHUSIASM

to adopt and maintain good cyber hygiene

Lack of enthusiasm and motivation can cause people to disengage from good security practice and risks insecure behaviours.

ENTHUSIASM

ENTHUSIASM

Lack of enthusiasm or motivation can hinder individuals and organisations from fully engaging with all kinds of new security initiatives, products, and services. It can prevent them from staying informed about the latest policies, guidelines, and strategies. This is one of the most difficult barriers to address and it can critically undermine security culture.

People may lack the motivation to follow the basics of good cyber hygiene or the will to follow complicated instructions or adopt new behaviours. Even minor friction points presented by cyber security measures may be enough for people to disengage and adopt insecure behaviours.