



uniac
assurance for universities

IT Risk Management
Briefing – Cyber
Security and Digital
Disruption



- Over 25 years in HE
- Specialist Internal Audit and Assurance
- Largest single team of higher education specialists
- Mature experience auditors
- We work with 15 Higher Education Institutions

2018 *This Is What Happens In An Internet Minute*



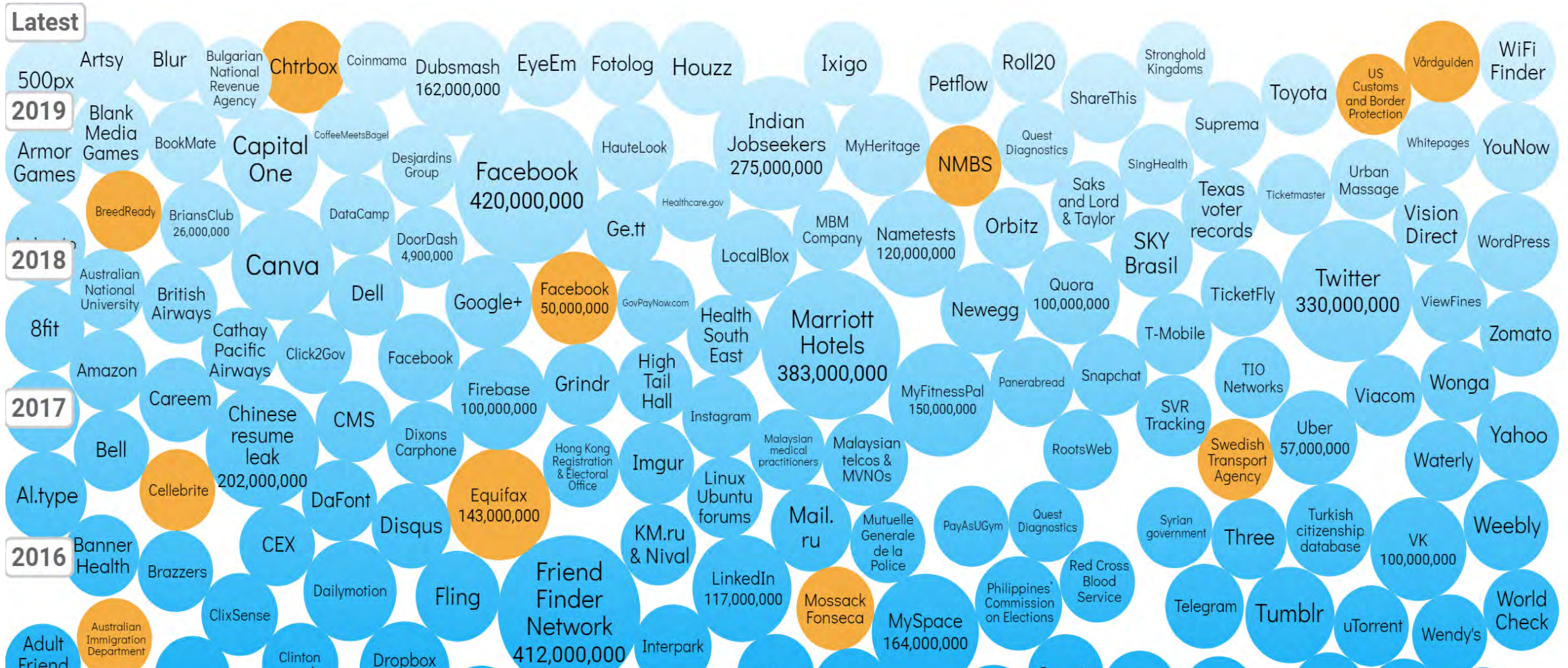
Created By:
[@LoriLewis](#)
[@OfficiallyChadd](#)

2019 *This Is What Happens In An Internet Minute*



Created By:
[@LoriLewis](#)
[@OfficiallyChadd](#)

World's biggest Data Breaches and Hacks



What are the top five risks to your organisation?

Cybersecurity & data privacy: rising expectations of internal audit



The increasing regulatory burden



Digitalisation & business model disruption



Looking beyond third parties



Business resilience, brand value & reputation



Financial risks: from low returns to rising debt



Geopolitical instability & the macroeconomy



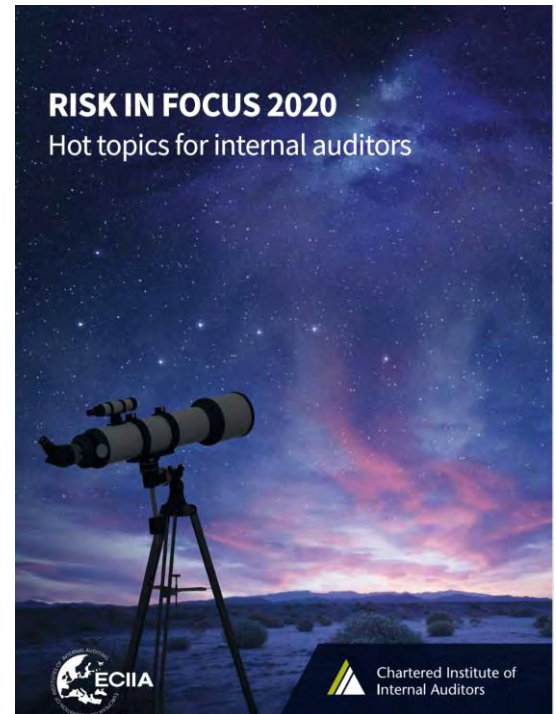
Human capital: the organisation of the future



Governance, ethics & culture: the exemplary organisation



Climate change: risk vs opportunity







uniac
assurance for universities

Cyber Security – 10 Things Your SMT should know

Ian Musgrave

Head of IT and Cyber Assurance

What I will cover ...

- Summary of major cyber security issues
- Based on work in the higher education sector over past 2-3 years
- NCSC control framework
-  Key risks and  best practice for the key issues

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.



User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.



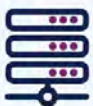
Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.



Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.



Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Managing user privileges



Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management



Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring



Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working



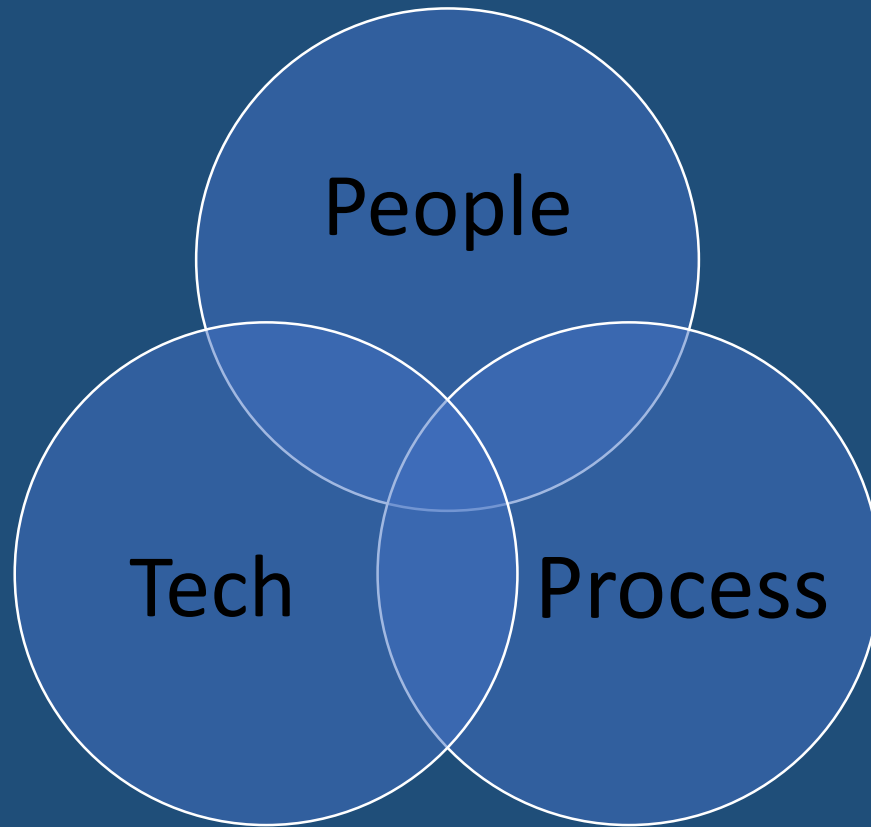
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

#1- Cyber Attacks continue to grow



- Cyber Incidents continue to grow
- Increase of 24% (2018 City of London police)
- 43% of businesses have experienced a cyber attack in past 2 years (UK Government - DCMS)
- 49% in education sector – the least prepared industry globally (Source: Harvey Nash)

#2 - Technology is only one part



#2 - Technology is only one part

'PEOPLE' includes

- Behaviour
- Ethics
- Attitudes
- Culture
- Internal comms
- Tone from the top
- Training and awareness
- Specialist skills and qualifications

'PROCESS' includes

- Governance and security frameworks
- IT Security policies
- Password procedures
- Patching methods and systems
- IT risk management and audit

#3 - Cyber needs to be owned by the whole organisation

- Treating it as a specialist 'IT' subject is a surefire way to avoid buy-in and commitment
- Must be regularly on Executive and Board agenda
- IT is a key corporate enabler (not just 'keeping the lights on')

#3- Cyber needs to be owned by the whole organisation



Common Problems

- IT too operational
- No visibility of IT risks / No IT risk register
- Lack of engagement with wider business –Security is left to the CIO
- No formal SIRO role



Best Practice

- IT is key strategic business partner
- Cyber is seen as a BUSINESS RISK
- Regular IT risk reporting to SMT
- All sources of assurance are mapped
- CIO part of top management team

#4 - Boards and Governing Bodies are accountable ...but frequently not responsible

Board members must:

- Ensure that a sound framework exists to provide strategic guidance for the enterprise
- Monitor management
- Oversee the integrity of the enterprise's systems and information

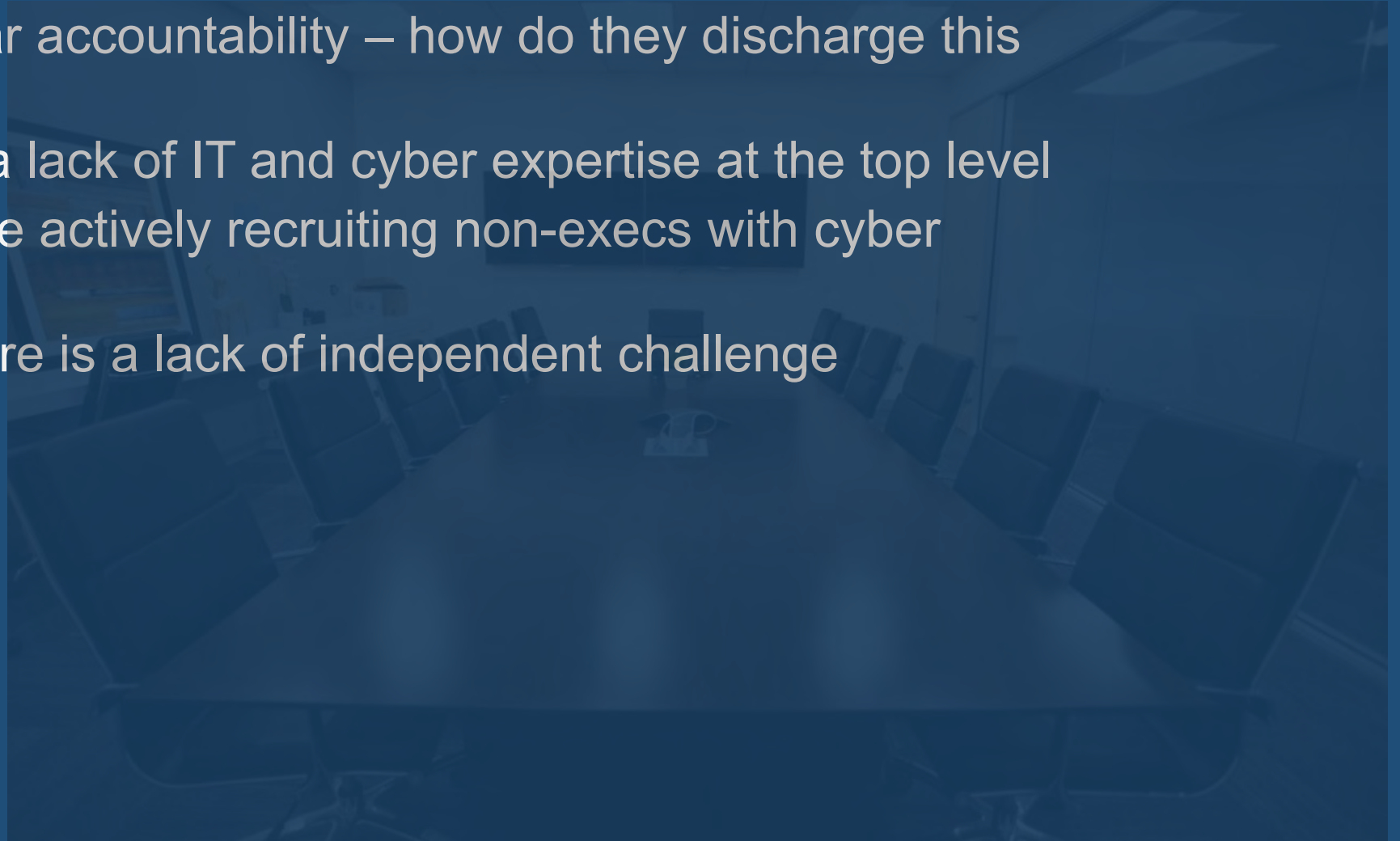
(Principles of Corporate Governance, OECD 1998)

THEREFORE BOARD MEMBERS:

- are **accountable** for the performance of IT
- Should address IT like **any other strategic board agenda item**

#4 - Boards and Governing Bodies are accountable ...but frequently not responsible

- So Boards have clear accountability – how do they discharge this role?
- We continue to see a lack of IT and cyber expertise at the top level
- Many Universities are actively recruiting non-exec's with cyber background
- In the meantime, there is a lack of independent challenge



#4 - Boards and Governing Bodies are accountable ... but frequently not responsible



Common Problems

- Lack of IT expertise at Board level
- Insufficient independent challenge and scrutiny
- No Board input into cyber strategy



Best Practice

- IT/cyber skills/background is a key criteria for Board appointments
- Dedicated IT risk register
- Board demands regular assurance on cyber including independent audit, accreditation
- Move towards annual reporting

#5 - People are not always 'Our Greatest Asset'

Despite the cliché, people can also be the greatest threat due to

- Insider malicious activity
- user error
- 'social engineering' attacks

These are all major risks



#5 - People are not always 'Our Greatest Asset'



Common Problems

- Human nature
- People are the weakest link
- Culture is difficult to manage



Best Practice

- Emphasise:
People-People-People
- Training needs to address the main risks
- Strong policies and disciplinary procedures

#6 - Mandatory user training is easier said than done

- User Training and Education is a fundamental control
- One of the main areas of management concern and audit activity
- Most Universities have moved to mandatory user training- but are struggling with enforcing it
- How is it managed and refreshed? Is it effective – and how do you know?

#6 - Mandatory user training is easier said than done



Common Problems

- Training take-up is not monitored
- Difficult to enforce sanctions on staff who don't engage
- Remote sites hard to reach
- Effectiveness is not assessed



Best Practice

- Online training with test scores and automated results
- Clear disciplinary policies
- Refresher training annually
- Different methods used – face to face, workshops, poster campaigns

#7 - User privileges are excessive and unmanaged

- Access controls to main network, Active Directory
- Privileges within the main business applications (the 'Crown Jewels')
- Essential these are managed on a 'need to know' basis
- Communication between departments and systems

#7 - User privileges are excessive and unmanaged



Common Problems

- Lack of monitoring and housekeeping
- Excessive users/privileges
- Accumulation of rights over time
- Shared /generic accounts
- Uncontrolled super users



Best Practice

- Centralised identity management
- Close liaison between IT and application owners
- Systematic reporting and checking
- Admins use non-privileged accounts for regular activity

#8 - Passwords are a key source of compromise

- We are still reliant on password security, despite the growth of multi-factor authentication, biometrics;
- Links to user behaviour, training and education
- What's your password?

<https://www.google.com/search?q=what%27s+your+password&oq=what%27s&aqs=chrome.1.69i57j69i59j0l4.3582j0j7&sourceid=chrome&ie=UTF-8>

- Debate over optimum password length, complexity, change frequency;

<https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere>

Password Policy

Advice for system owners

The NCSC is working to reduce organisations' reliance on users having to recall large numbers of complex passwords. The advice below advocates a greater reliance on technical defences and organisational processes, with passwords forming just one part of your wider access control and identity management approach.

How passwords are discovered...

Interception

Passwords can be intercepted as they travel over a network.



Brute force

Automated guessing of billions of passwords until the correct one is found.



Manual guessing

Details such as dates of birth or pet names can be used to guess passwords.

Key logging

Installing a keylogger to intercept passwords when they are entered.



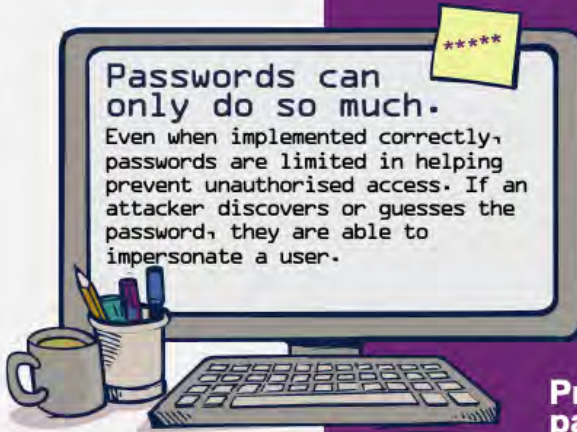
Shoulder surfing

Observing someone typing in their password.



Stealing passwords

Insecurely stored passwords can be stolen, such as ones written on sticky notes and kept near (or on) devices.



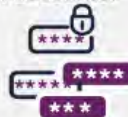
Stealing hashes

Stolen hash files can be broken to recover the original passwords.



Password spraying

Trying a small number of commonly-used passwords to access a large number of accounts.



Phishing & coercion

Using social engineering techniques to trick people into revealing passwords.



Data breaches

Using the passwords leaked from data breaches to attack other systems.

...and how to improve system security.

Reduce your reliance on passwords



1. Only use passwords where they are needed and appropriate.
2. Consider alternatives to passwords such as SSO, hardware tokens and biometric solutions.
3. Use MFA for all important accounts and internet-facing systems.

Implement technical solutions



1. Throttling or account lockout can defend against brute force attacks.
2. For lockout, allow between 5-10 login attempts before locking out.
3. Consider using security monitoring to defend against brute force attacks.
4. Password blacklisting prevents common passwords being used.

Protect all passwords



1. Ensure corporate web apps requiring authentication use HTTPS.
2. Protect any access management systems you manage.
3. Choose services and products that protect passwords using standards such as SHA-256.
4. Protect access to user databases.
5. Prioritise administrators, cloud accounts and remote users.

Help users generate better passwords



1. Be aware of different password generation methods.
2. Use built-in password generators when using password managers.
3. Don't use complexity requirements.
4. Avoid the creation of passwords that are too short.
5. Don't impose artificial capping on password length.

Key messages for staff training



1. Emphasise the risks of re-using passwords across work and home accounts.
2. Help users to choose passwords that are difficult to guess.
3. Help users to prioritise their high value accounts.
4. Consider making your training applicable to users' personal lives.

Help users cope with password overload



1. Allow users to securely store their passwords, including the use of password managers.
2. Don't automatically expire passwords. Only ask users to change their passwords on indication or suspicion of compromise.
3. Use delegation tools instead of password sharing. If there's a pressing business requirement for password sharing, use additional controls to provide the required oversight.

#8 - Passwords are a key source of compromise



Common Problems

- Lack of clear and consistent password policies
- Over-emphasis on forced regular change rather than complexity
- Passwords still being written down!
- Insecure password allocation (e.g. user home postcode!)

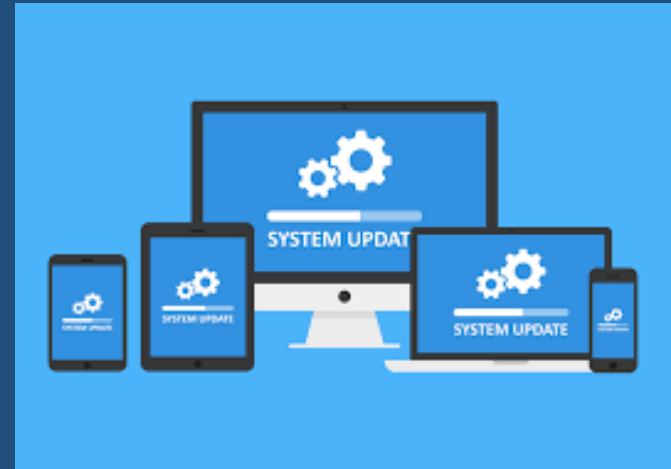


Best Practice

- Multi-factor authentication
- Forced change on first use
- Move towards pass-phrases
- Consistency across systems

#9 - Software patching is not being done consistently

- Out of date operating systems and applications remain a proven source of cyber attacks
- Removing unnecessary functionality
- Legacy systems which are no longer supported
- Shadow IT
- Fixing known vulnerabilities
- Systematic and regular updates



#9 - Software patching is not being done consistently



Common Problems

- Shadow IT
- Informal policies leading to infrequent patching regimes
- Manual processes with risk of error
- Ad hoc approach due to unacceptability of downtime



Best Practice

- Formal patching regime with clear responsibilities for implementation and sign off
- Response to emerging threats and security events

#10 - Incidents are not being managed proactively

- Proactive or reactive approach
- All users and managers need to be aware of the correct procedures for breach reporting
- Supportive culture which encourages openness
- Root causes may not be addressed and are therefore more likely to happen again



#10 - Incidents – Cultural Factors

- Encouraging employees to report incidents
- ‘No blame’ culture
- Emphasis on security being everyone’s responsibility

#10 - Incidents are not being managed proactively



Common Problems

- Reactive approach which only seeks to contain the incident
- Cyber events not properly identified
- Events not being consistently followed-up
- Lack of specialist incident response staff



Best Practice

- Clear definitions of what constitutes a cyber incident and how to respond
- Systematic documentation of events, type, cause, how resolved
- Liaison with other relevant parts of the business
- Security Operations Centre (SOC)

Ten Things Management Need to Know

- 1 Cyber threats continue to grow
- 2 Technology is only part of the problem
- 3 Needs to be owned by the whole organization
- 4 Boards are accountable but not always fully responsible
- 5 People are not always our greatest asset
- 6 Mandatory user training is easier said than done
- 7 Excessive user privileges
- 8 Passwords are key source of compromise
- 9 Patching not being done consistently
- 10 Incidents not being proactively managed

Summary

- Communication and clarity
- Cyber Security is an ongoing undertaking
- Understanding the scale of the problem
- Wide organisational ownership, governance and management
- Recognition of the main threats and what good looks like
- Auditors role is crucial – not just via formal reporting, also informal meetings, presentations
- Need top management buy-in