GOVERNMENT OF
WESTERN AUSTRALIA

TAFE WA North Metropolitan

BSBXCS402 Promote workplace cyber security awareness

Support effective cyber security practices in work place

CyberSecurity

This session will investigate:

- Reviewing Cyber Security practices according to organisational policies and procedures
- Updating training, information and records as required
- Reporting review and updates to required personnel, and potential impacts on workplace

Review

A review is an evaluation of :

- A publication eg a book
- A service eg a business transaction
- A piece of hardware eg a TV screen
- An event eg a concert

Review

A review of cyber security practices is an evaluation of how well an organisation manages their cyber security

(policy and guidelines, information security, personnel security and physical security)

Best Practices

General best practices:

- Safe online behaviour
- Compliance with company policies
- Procedures for preventing, detecting , responding and recovering from security incidents

Safe Online behaviour

Organisations need to protect their company data (eg intellectual property, private staff and client information, sensitive business data)

Safe Online behaviour

Workplace security and safety depend as much on human behaviour (wetware) as the physical and technological systems

Safe online behaviour

An organisation can address:

- Governance – policies and procedures
- Information security
- Personnel security
- Physical security

Governance

Policies should be developed, and understood by all staff.

Password policy – complexity rules, history etc

Disposal of data policy– shredding, sanitizing of obsolete equipment

Acceptable use policy – rules on what can be accessed and shared on line

Backup policy – where, when and what ought be backed up

Policies for 3rd party suppliers – do 3rd party suppliers have cyber security practices in place?

Governance

Discussion questions:

Should staff internet use and emails be monitored?

How should old computers be disposed of?

Should staff be able to use public wifi?

Should staff be able to use their own devices?

Who is responsible for writing/enforcing policies?

Information Security

The goals of information security:

Confidentiality, integrity and availability

CIA needs to be applied to 3 states of data:

Data at rest, data in transit and data in process

Information Security

Technology to assist in information security:

Firewalls, antivirus and anti-malware software, patching of operating systems and applications, VPNs for external workers, encrypted and hidden office wifi, backup procedures and backup devices

Personnel security

Cyber Security needs to be considered when:

- Bringing new staff into the organisation
- Training/educating/monitoring exisiting staff
- Staff leaving (eg disgruntled ex employees)

Personnel security

New staff:

Processes for selecting staff (eg merit select)

HR policies (eg check references, police check etc)

Personnel security

Existing staff:

Smart companies train their staff

Staff must be informed of the company's Cyber Security policy, and managers must implement it.

Staff must be invested in 'the culture of security' in an organisation

Personnel security

Discusssion questions:

How can we protect against phishing emails?

Complete the phishing quiz https://phishingquiz.withgoogle.com

What is the greatest security weakness – software , hardware or wetware (humans)?

Physical security

Physical cyber security includes:

Lock out /time outs on computers

Physical security on doors etc.

Restricted access to secure areas

Best Practices

Protect your data (don't allow sensitive data to be leaked)	Avoid pop-ups, unknown emails, unsecured websites and links	Use strong password protection and authentication (eg MFA)
Connect to secure wifi (avoid public wifi and poorly security hotspots)	Enable firewall protection at home and at work	Invest in security technology (antivirus, VPNs, firewall devices, SIEMs)
Install patches and updates on operating systems and applications	Have policies that cover security such as: • 3rd party suppliers • Onboarding and offboarding staff	Promote a culture of security in a workplace through staff training and education
Have processes to prevent, detect, respond and recover from security incidents eg disaster recovery plan	Regularly review and update the cybersecurity plan to deal with new and evolving threats	Have physical security controls in place

How to Protect Your Business from Cyber Attacks | NIST

Protect your business from cyber threats | business.gov.au

How

How do cyber security policies and procedures protect against cyber attacks?

A company's cyber security policy helps clearly outline the guidelines for transferring company data, accessing private systems, and using company-issued devices.

How

Cyber security policies inform each staff member of their responsibilities for protecting IT systems and data

Cyber security procedures set the standards of behaviour for work (eg email encryption, social media use, handling of data/media)

How

Cyber security policies help to protect against the risk of costly cyber attacks and data breaches.

43% of data loss is due to internal users

Cyber security policies protect regulated organisations (healthcare, finance, insurance) from penalties if their security procedures fail compliance.

About the Notifiable Data Breaches scheme — OAIC

Training

Goal : Arrange training and information updates as required, and maintain related records

Training

Training /educating staff can assist in early identification of security threats.

Employees , not hackers, are the most common entry points for many attacks eg phishing

Training

Human problem:

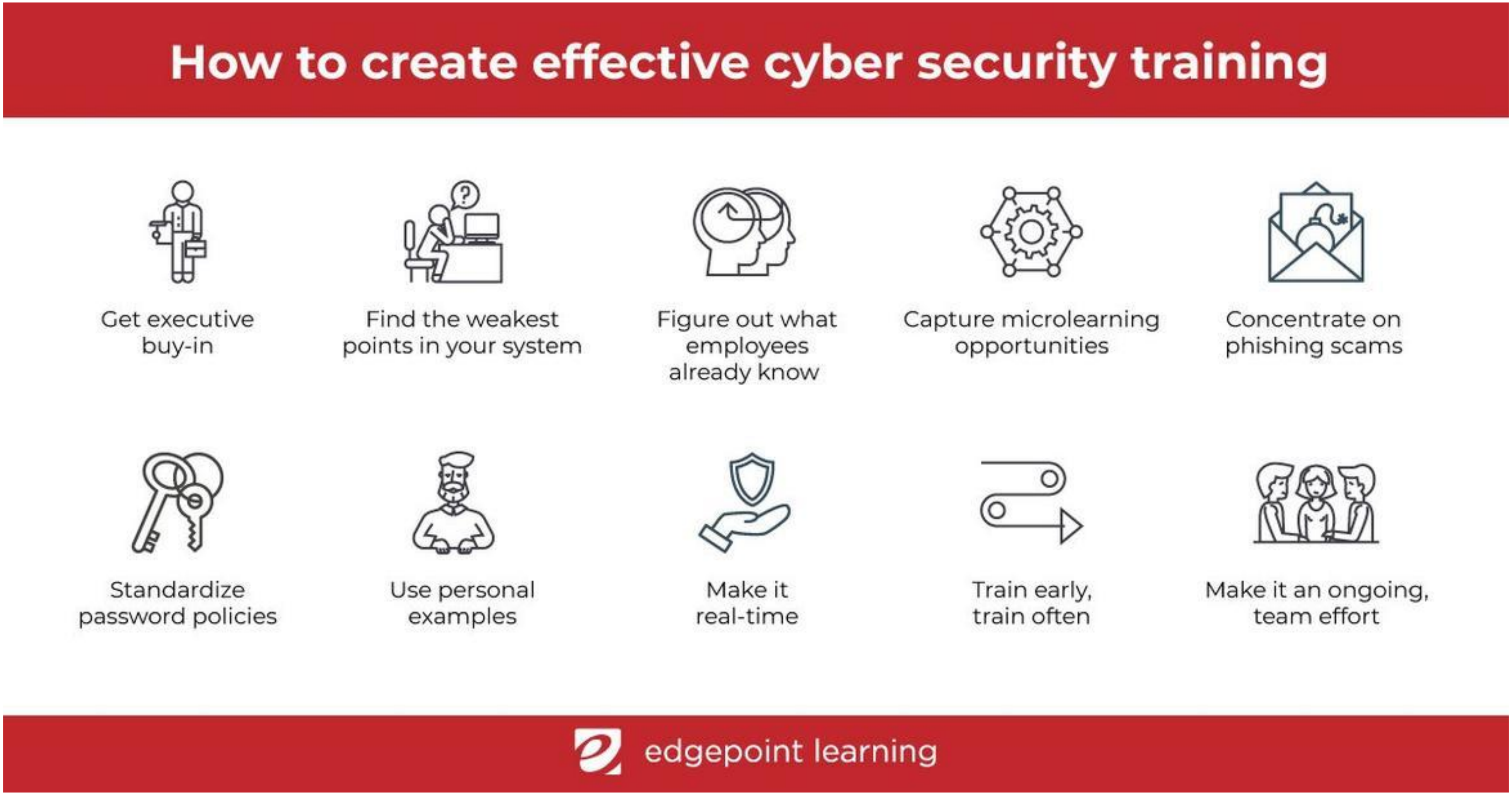
People are trusting

People are 'conditioned' to respond to authority (even hackers pretending to authority)

People make mistakes

People can be tempted and persuaded

Training



How to create effective cyber security training

- Get executive buy-in
- Find the weakest points in your system
- Figure out what employees already know
- Capture microlearning opportunities
- Concentrate on phishing scams
- Standardize password policies
- Use personal examples
- Make it real-time
- Train early, train often
- Make it an ongoing, team effort

edgepoint learning

Training

1. Get executive buy-in

Cyber security awareness training is worth the ROI. The cost of training is less than the cost of a breach when it comes to protecting your customers, their data, and your company's proprietary information.

It may be as simple as pulling together the statistics on the costs of cyber security training versus the **costs of rebuilding your reputation and customer base** after an attack. Focus on hard numbers and tailor your pitch to leadership knowing your company's needs.

Training

2. Take a broad view, and then evaluate your company's weak points

When designing cyber security training courses for your company, look at the overall security already in place, and then consider the weakest points in your system.

Are there gaps in security when it comes to payment processing? Inter-office emails? Uploading to DropBox or another file storage program? Attachments and document security? Figure out the weakest link and focus the start of your course design there.

Training

3. Figure out what employees already know

Don’t waste employees’ time (and your own) teaching them what they already know.

Work with your cyber security training developers to evaluate employee awareness before sending everyone to the same training.

Training

4. Use microlearning and at-hand resources

Chances are good that your company already has training resources at hand. Don’t re-invent the wheel. If your employees respond best to online training, don’t shuffle them into a room and make them stare at a four-hour presentation.

Utilize the principles of **microlearning** to deliver essential small bites of information that address the most vital cyber security tips for employees.

Training

5. Train employees about email and phone phishing scams

Get specific when it comes to current phishing scams via phone and email.

Even the most well-informed employees may not be completely up-to-date on every scam that comes down the pike. Microlearning can come in handy here, too. Nearly **91% of cyber attacks start with an email**. Teach employees how to protect themselves (and the company!).

Training

6. Standardize a company-wide process for updating passwords

Do you want employees to change passwords every 30 days? Should each password have a capital letter, a special character, and eight or more characters total? What about **two factor authentication** (2FA)?

Set the standard, and make sure the entire company knows what it is, and create automatic processes that force them to update their passwords.

Training

7. Use personal examples

In a company of any size, chances are good that one or more employees have been the victim of some form of identity theft or cyber attack.

Make your cyber security training personal by having willing employees share their experiences, tying them back into protecting the company, too. From **Uber** to **Equifax**, everyone is vulnerable.

Training

8. Make it real-time

Your company can also create simulated cyber attacks for each department of your company. These “live-fire” training exercises can sharpen cyber security awareness and get everyone ready if the time comes when it’s not just a drill.

Evaluate employee response to the drill and adjust your training accordingly.

Training

9. Train early, train often

Start cyber security training for employees during the onboarding process as an integral part of joining the company.

This can help you identify new employees’ level of awareness and tailor training to their needs. Check in as they integrate into the workforce.

Training

10. Make it an ongoing, team effort

“Most organizations roll out an annual training and think it’s one and done. That’s not enough.”

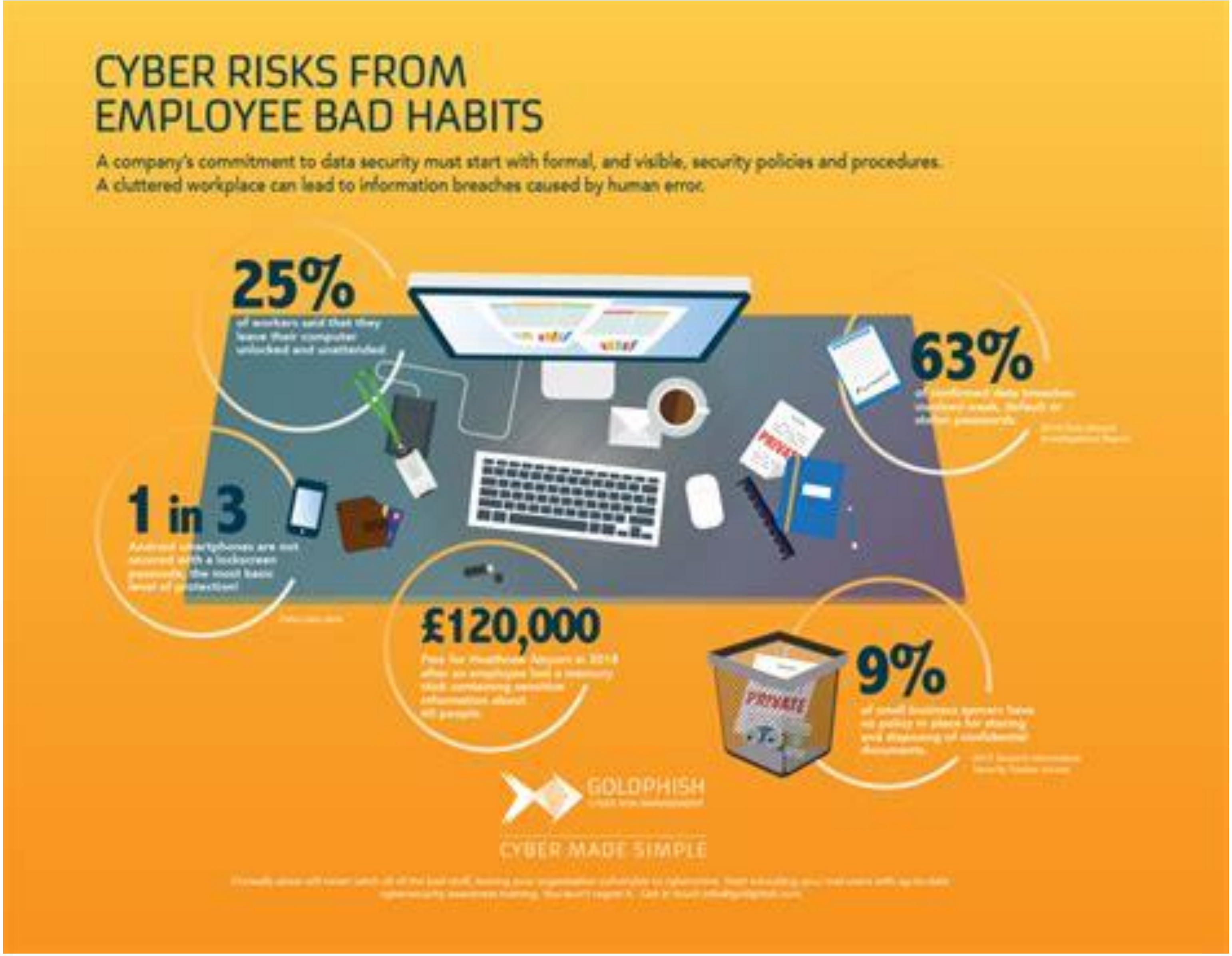
“People Patching.” : Similar to regular software upgrade, cyber security training should be an ongoing, team effort that takes into account changes in the industry, the world, and the ever-evolving tools of the hackers.

“Your people are your assets, and you need to invest in them continually. If you don’t get your people patched continually, you’re always going to have vulnerabilities.”

Maintaining records

Physical documents ought be secured: lock the drawers, lock the room, keep the desk clear

Maintaining records



CYBER RISKS FROM EMPLOYEE BAD HABITS

A company's commitment to data security must start with formal, and visible, security policies and procedures. A cluttered workplace can lead to information breaches caused by human error.

25% of workers said that they leave their computer unlocked and unattended

1 in 3 Android smartphones are not secured with a lockscreen password, the most basic level of protection!

£120,000 Fine for [illegible] in 2014 after an employee lost a memory stick containing sensitive information about [illegible] people

63% of confirmed data breaches involved weak, default or stolen passwords

2016 Data Breach Investigations Report

9% of small business owners have no policy in place for storing and disposing of confidential documents.

[illegible]

[illegible]

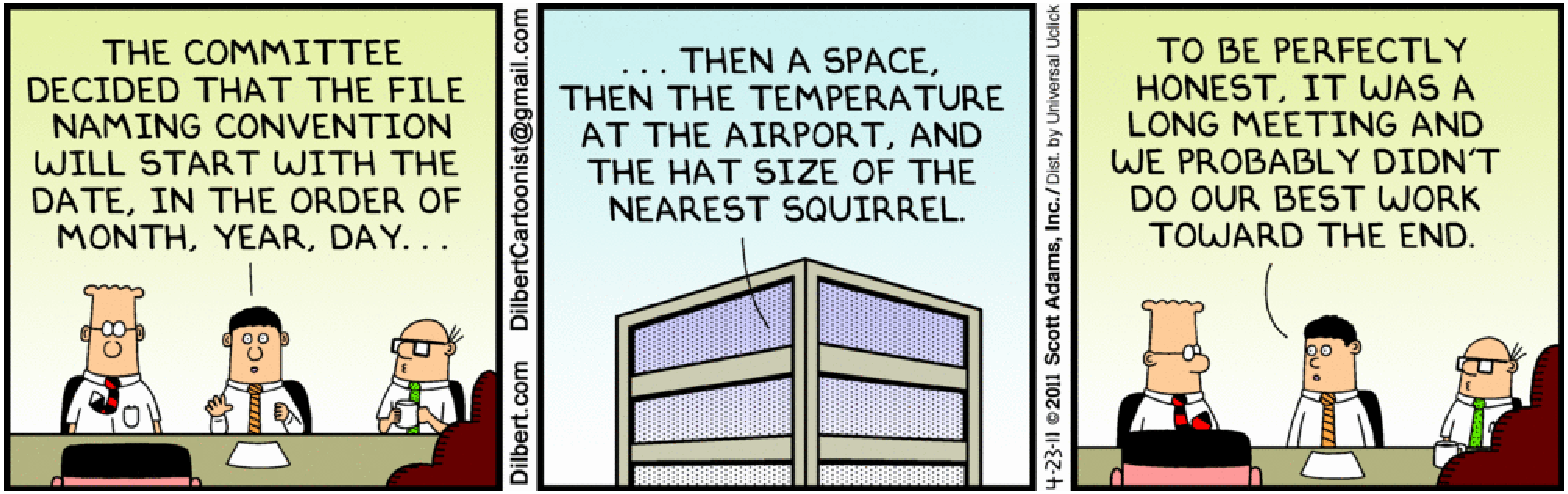
Maintaining records

Limit access to company files – employ the Principle of Least Privilege

Limiting who can access, copy, delete or modify records can reduce the risk of human error as well as reduce the risk of deliberate compromise of company data

Maintaining records

Naming conventions – files and records ought to be systematically labelled and stored to reduce the risk of error


THE COMMITTEE DECIDED THAT THE FILE NAMING CONVENTION WILL START WITH THE DATE, IN THE ORDER OF MONTH, YEAR, DAY. . .
. . . THEN A SPACE, THEN THE TEMPERATURE AT THE AIRPORT, AND THE HAT SIZE OF THE NEAREST SQUIRREL.
TO BE PERFECTLY HONEST, IT WAS A LONG MEETING AND WE PROBABLY DIDN'T DO OUR BEST WORK TOWARD THE END.
Dilbert.com DilbertCartoonist@gmail.com
4-23-11 ©2011 Scott Adams, Inc./Dist. by Universal Uclick

Maintaining records

Backup, backup and backup – backups ought be secured, offsite, and checked/restored regularly to confirm that valuable data is being protected

Disaster plans – fire, security alarms, water, pests all need to be considered and prepared for.

Maintaining records

Files and digital media need to be disposed/destroyed in a systematic way

Some data needs to be retained for a certain period of time (legislative requirements).

Destroying data when it is no longer needed, reduces the companies attack surface, and reduces its liability (legal and risk)

Maintaining records

Record management systems need to be regularly audited to confirm that they are addressing the risks .

Audits provide feedback to improve systems and respond to changing threat environments

Benefits to regular training

Security awareness training helps in influencing the behaviour of employees, reducing cyber risks, and ensuring compliance within the organization.

Benefits to regular training

Employees are a great source of information in early detection of cyber attacks

Employees that are trained, will be more confident and capable in using the IT systems

Training forms the first step in building a better and sustainable culture of security

Benefits to regular training

Achieve better uptime – the fewer data breaches and downtime the better	Reduce costs and overhead – cheaper to prevent a data breach than have to recover from one	Control and protect the company's data – data is an important and valuable asset
Adhere to internal policies – training informs staff of expected behaviour and helps to monitor/manage it	Comply with relevant laws and regulations – companys must comply with data privacy laws and staff need to be trained in ways to protect data	Contain threats – trained staff can assist in identifying threats early, avoiding threats, and containing threats so that the company doesn't suffer extensive damage

Questions

What are cyber security practices?

How can you secure related records?

What is the Essential Eight?