BSBXCS402 Promote workplace cyber security awareness

Develop cyber security awareness in the work place

CyberSecurity

Objectives

- Establish current level of CyberSecurity awareness
- Create and maintain CyberSecurity awareness program
- Contribute to policy and procedures

Awareness

Awareness – the ability to directly know and perceive, to feel, or be conscious of events

Cyber Security awareness refers to how much end users know about the threats their networks face, and the risks they introduce.

Awareness

Organisations allocate funds to protect their networks from outside threats and reduce vulnerabilities.

End users are a major vulnerability – so spending on technical security is not enough.

Organisations need to educate their staff on current threats and how to avoid them

Awareness

Discuss : ***its easier to steal a password than to hack one***

Discuss: ***without an embedded culture of cybersecurity awareness and enforcement, expensive security systems won't work***

Social Engineering

The psychological manipulation of a user

- Phishing
- Watering hole – compromised websites
- Pretexting – fake identities
- Baiting / quid pro quo
- Scareware
- Tailgating

Components of cyber trainnig

Employees are first line of defence – awareness training can equip them with the knowledge and skills needed to help defend against cyber threats

Awareness training can increase the chance of detecting a threat, reduce damage in the event of a threat, and reduce the cost of recovery

Create a training program

- Employees must understand their security responsibilities
- Some personnel have non-standard roles and their training must be tailored to meet their needs
- Security awareness training will depend on the objectives of the organisation

Cyber Security Awareness Training

DCENCOMPASS

Educating staff on the importance of Cyber Security Awareness

The staff induction process is an ideal time to train new employees about the importance of cyber security.

Why is it so important?

Under the Notifiable Data Breaches (NDB) scheme, Australian organisations are required to report data breaches

The OAIC has the power to fine organisations up to $1.8 million.

The Ponemon Institute puts the average cost of a data breach in Australia at $2.13 million*

What's involved?

An effective cyber security awareness training course should be practical and inclusive (all staff should be able to understand the material).
The following topics are usually covered during a session:-

- The Privacy Act (outline responsibilities)
- Document handling and classification policies
- Types of threats
- Phishing attacks
- The dangers of downloading "unofficial" files
- Social engineering
- The dangers of installing "unofficial" apps and programmes
- Best practice password management
- Public Wi-Fi hotspots (the need for VPN software)
- Avoiding insecure or unverified websites
- Social media posts (do's and don'ts)
- Ongoing vigilance

Ways to create cyber training

1. Focus on ‘must see’ policies : focus on issues most likely to happen and/or those with the greatest risk. Staff need deep understand of ‘key’ policies, not ‘all’ policies
2. Connect with staff. Staff have unique understanding of the security issues and behaviours in their areas of work.

Ways to create cyber training

3. Use targeting. Target messages to different audiences depending on the security issues they face.

4. Repeat key messages in multiple channels. Repetition drives recall. Reinforce messages through bite-sized pieces using multiple channels.

Ways to create cyber training

5. Enlist decision makers. If senior staff are not on board, program won't be adopted. Senior staff model and reinforce behaviours.

6. Challenge beliefs of safety. Most people underestimate cyber threat. Awareness of extent and cost of cyber threat will strengthen any training program.

Ways to create cyber training

7. Visual cues. Distinct colours linked to security messages can help employees immediately identify the nature of a message and act accordingly (eg red = urgent)

8. Gamify. Eg KnowBe4 Keep the energy up and interest levels high.

Ways to create cyber training

9. Define behaviour changes and measure the impact. Staff need to clearly understand the desired changes, and changes in the desired behaviours need to be surveyed, monitored and reported.

Ways to create cyber training

Discuss: ***how would you raise awareness and promote key messages in your workplace?***

Cyber security policy/procedures

Policies and procedures help employees understand their role

Cyber policies outline the organisation's:

- ***Assets that need to be protected***
- ***Threats to those assets***
- ***Rules and controls for protecting the assets***

Cyber security policy/procedures

Policies and procedures ought guide staff on:

- ***The type of business information that can be shared and where***
- ***Acceptable use of devices and online materials***
- ***Handling and storage of sensitive material***

Password policy

Cyber Security policy ought explain:

- ***How to store passwords correctly***
- ***Password complexity/history***
- ***The importance of unique passwords for different logins (Password Managers!!)***

Email policy

Cyber Security policy ought explain:

- ***Opening email attachments from trusted contacts and businesses***
- ***Blocking junk, spam and scam emails***
- ***Deleting and reporting suspicious looking emails***

Sensitive Data

Cyber Security policy ought explain:

- ***When staff may share sensitive data with others***
- ***Ways to store physical files (secured cabinets)***
- ***Ways to properly identify sensitive data***
- ***Ways to destroy sensitive data***

Handling technology

Cyber Security policy ought explain:

- ***Where staff can access their devices/data***
- ***How to store devices when not in use***
- ***How to report theft or loss of device***
- ***How patches/updates will be rolled out***
- ***Screen lockouts/logouts***
- ***Restrictions on use of removable devices***

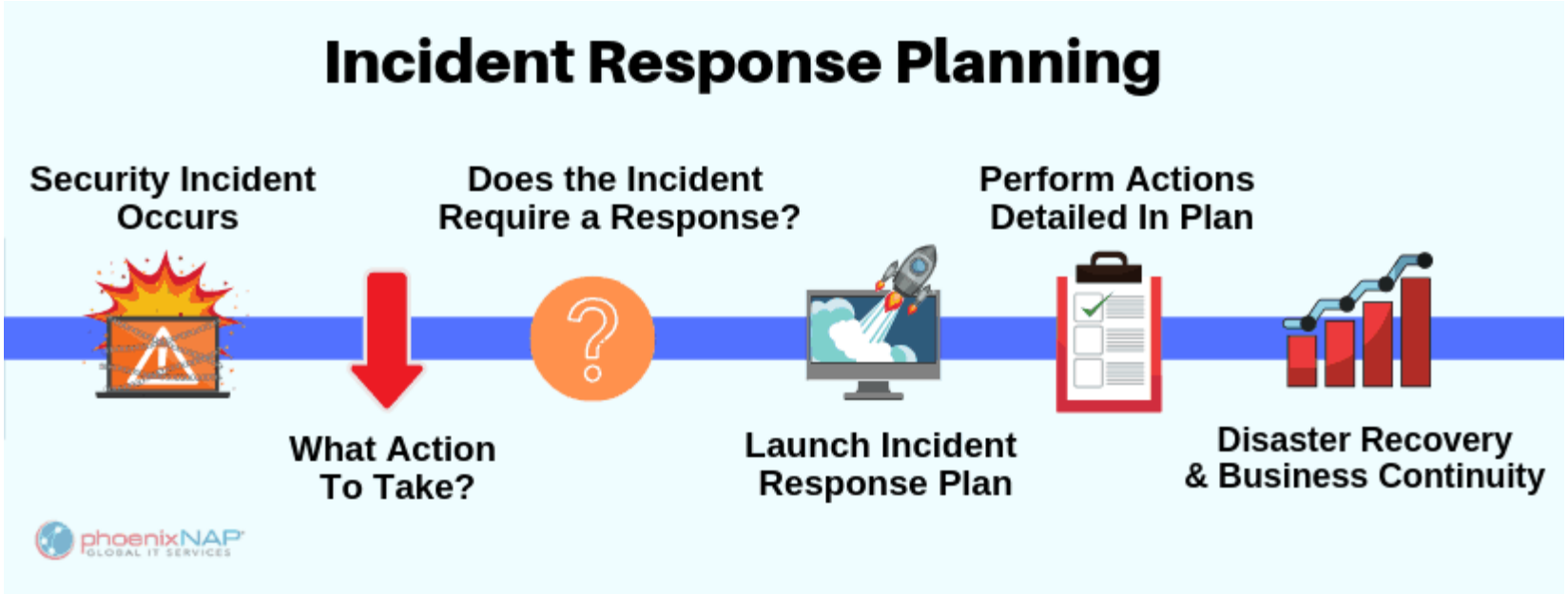
Eg USB

Social media and internet

Cyber Security policy ought explain:

- ***What is appropriate to share on social media channels***
- ***What is appropriate for work email accounts***
- ***Guidelines are appropriate access***

Prepare for an incident



Prepare and prevent

An incident response plan helps to prepare for, and respond to a cyber incident

Develop policies and procedures that help staff :

- Understand how to prevent an attack
- Identify an incident
- Respond in the event of an incident

Incident plan

- Prepare and prevent
- Check and detect
- Identify and assess
- Respond
- Review

Prepare and prevent

Prepare inventory of assets – financial, information and technology assets

Create roles and responsibilities so everyone knows who to report to if an incident occurs eg Microsoft SOC

Check and detect

Unusual activities include:

Accounts/network not accessible

Passwords locked out

Data is missing or altered

Hard drive space is full

Computer crashes

Others report your business email sending spam

Web page pop-ups

Identify and assess

Identify the cause of the incident

Determine the impact of the incident

Determine the impact if the incident is not immediately contained

Respond

Limit further damage by isolating the affected systems.

Eliminate the problem by removal of threat, or control the vulnerability

Recover from the incident by repairing to pre-incident status – business as usual

Review

Identify if systems/processes need improving – and initiate the necessary changes

Evaluate the incident before/ after/ lessons learnt

Update the Cyber Security incident response plan based on the lessons learnt

Develop, review and maintain Cyber Security policy regularly

Communicate

When communicating Cyber Security incidents to senior management, avoid technical language and focus on business objectives.

To be successful, your suggested changes must be aligned with the vision and priorities of management.

Questions

1. How can you establish awareness of cyber security in an organisation?

2. What is a cyber security awareness program?