BSBXCS402 Promote workplace cyber security awareness

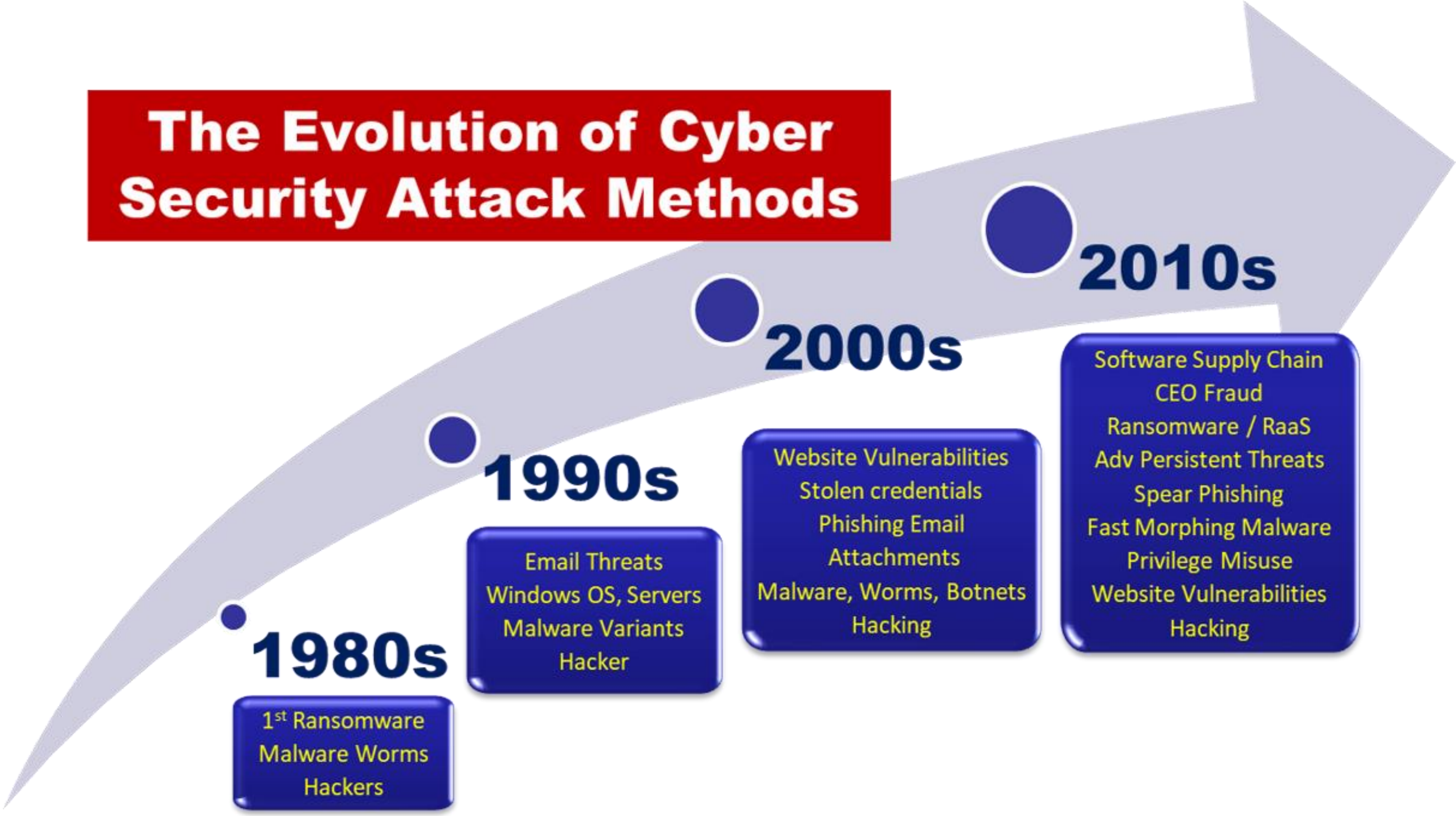
Review cyber security awareness in work place

CyberSecurity

This session will investigate:

- Reviewing Cyber Security threats and trends
- Document outcomes of review and suggested improvements
- Communicate review and suggestions according to organisation policies and procedures

Latest cyber threats and trends



The Evolution of Cyber Security Attack Methods

1980s

1st Ransomware
Malware Worms
Hackers

1990s

Email Threats
Windows OS, Servers
Malware Variants
Hacker

2000s

Website Vulnerabilities
Stolen credentials
Phishing Email Attachments
Malware, Worms, Botnets
Hacking

2010s

Software Supply Chain
CEO Fraud
Ransomware / RaaS
Adv Persistent Threats
Spear Phishing
Fast Morphing Malware
Privilege Misuse
Website Vulnerabilities
Hacking

Trends

The risk and severity of cyber attacks continues to grow

Global cybercrime costs are expected to grow to $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

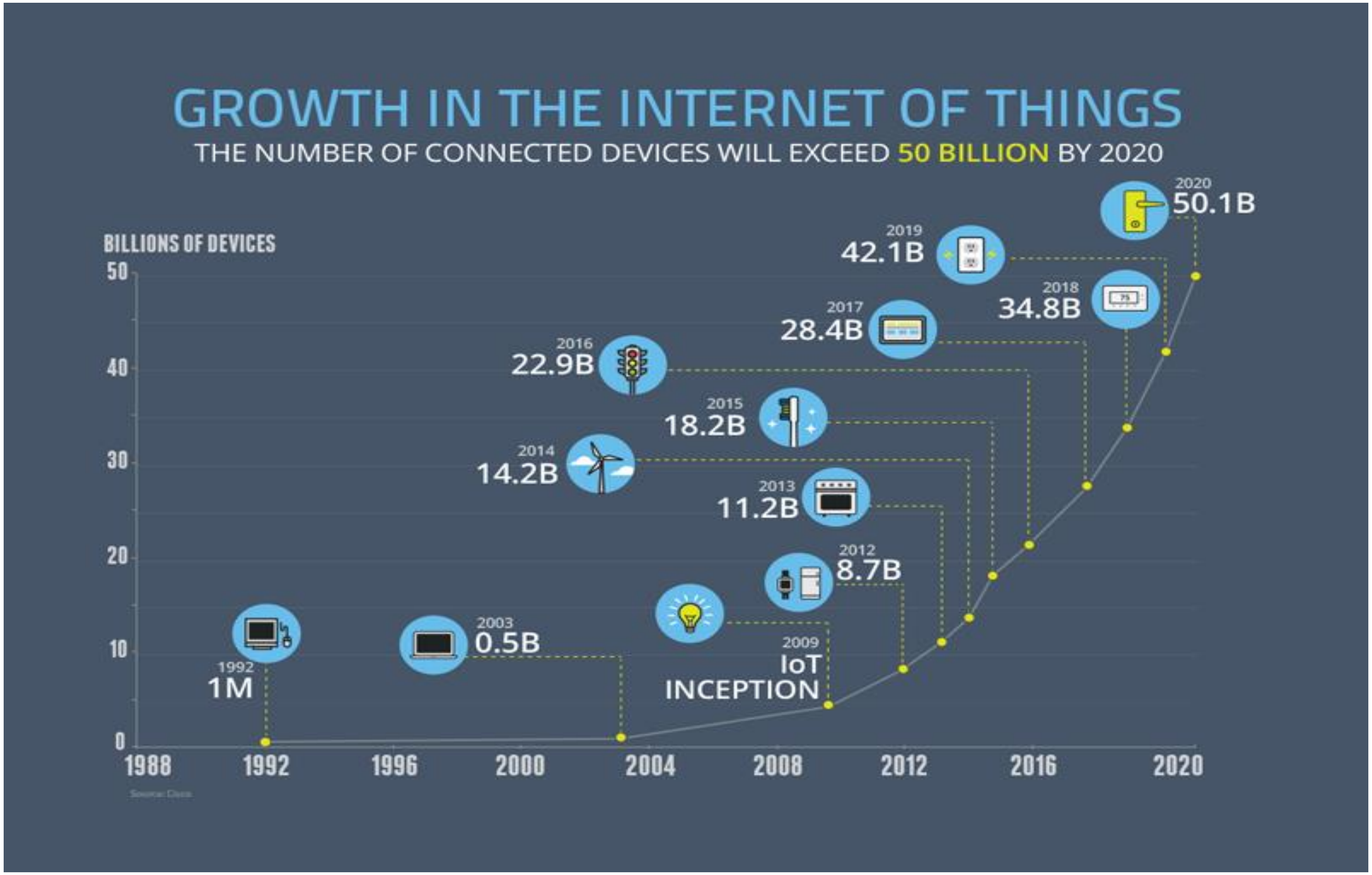
This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Trends

Nov. 13, 2020

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world’s third-largest economy after the U.S. and China.

Trends in technology



Behind The Numbers: Growth in the Internet of Things | NCTA — The Internet & Television Association

Trends

The world is shifting to IOT and cloud devices.

Both technologies introduce new cyber security risks to an organisation

IOT

Businesses are quickly adopting IoT devices due to high potential for savings. For example, after Harley-Davidson turned their Pennsylvania plant to a ‘smart factory’ using IoT devices in every step of the production process, they reduced costs by 7% and increased net margin by 19%.

IOT

Since IoT devices are connected to the internet, they can be hacked just like any other internet-enabled device.

One of the key IoT security issues is the expansion of attack surfaces due to an increased number of endpoints.

IOT

Since IoT devices are connected to the internet, they can be hacked just like any other internet-enabled device.

One of the key IoT security issues is the expansion of attack surfaces due to an increased number of endpoints.

Cloud

Cloud computing has a number of advantages

- Cost Savings.
- Back-up and restore data. ...
- Automatic Software Integration. ...
- Reliability. ...
- Mobility. ...
- Unlimited storage capacity. ...
- Collaboration. ...
- Quick Deployment.

Cloud

Cloud computing has a number of security risks:

- User Account Hijacking –. Account Hijacking is the most serious security issue in Cloud Computing. ...
- Changing Service Provider –. Vendor lock In is an important Security issue in Cloud Computing. ...
- Denial of Service (DoS) attack –. This type of attack occurs when the system receives too much traffic. ..

New cyber threats

Artificial Intelligence and machine learning have led to :

AI fuzzing : uses artifical intelligence to create a tool for detecting system vulnerabilities (useful for defenders as well as attackers)

Blockchain: businesses are increasingly using blockchain technologies for digital asset exchange. The relative 'newness' of this technology makes it vulnerable to cyber criminals

New cyber threats

Social engineering attacks like phishing are effective, high reward and low risk for hackers.

Phishing remains the number one cause of data breaches globally

New cyber threats

Deepfake – AI technology allows for increasingly convincing images and videos

Business impacts

Top 5 business impacts of cyber threats:

(note different industry's are impacted differently depending on their product, attack surface, reliance on reputation etc.)

Business impacts

Reputation damage – loss of customer confidence equates to share price loss, loss of revenue, loss of ability to attract best talent, suppliers and investors.

Some businesses eg Ashley Madison Online dating site, were completely destroyed after a data breach

Business impacts

Theft – Stolen data can be a considerable motivation for hackers, and lead to considerable monetary loss for a business.

*2020 Cybercrime costs the world more than **$1 trillion**, a 50% increase from 2018 Cybercrime costs the world economy more than $1 trillion, or just more than one percent of global GDP, which is up more than 50 percent from a 2018 study that put global losses at close to $600 billion, McAfee reveals.*

Business impacts

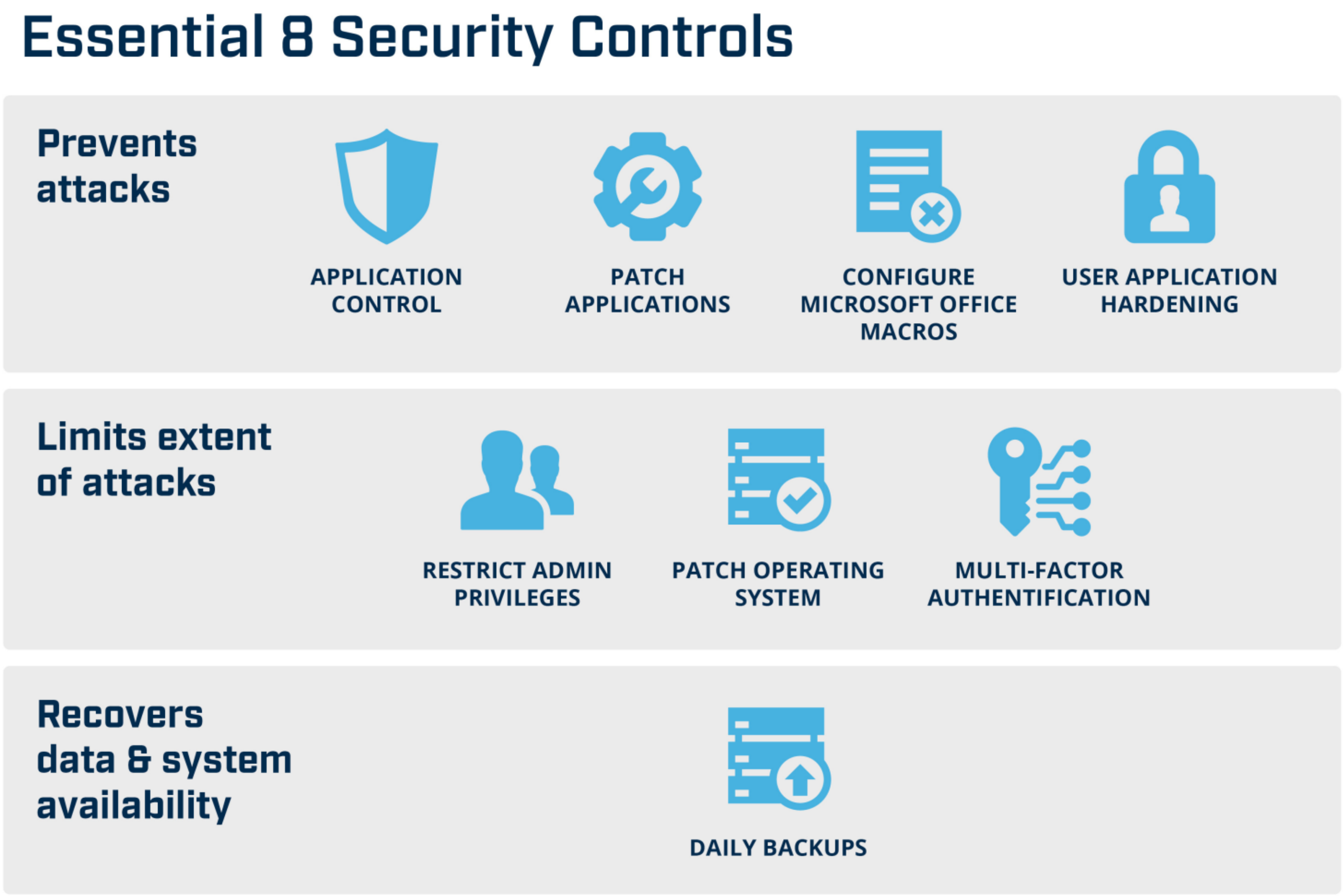
Fines: The European Union has introduced the GDPR which can fine a company up to 4 % of global revenue if a European citizen's personal information is breached.

Recommended improvements

The Australian Cyber Security Centre recommends the Essential 8

https://www.cyber.gov.au/

Recommendations



Essential 8 Security Controls

Prevents attacks

- APPLICATION CONTROL
- PATCH APPLICATIONS
- CONFIGURE MICROSOFT OFFICE MACROS
- USER APPLICATION HARDENING

Limits extent of attacks

- RESTRICT ADMIN PRIVILEGES
- PATCH OPERATING SYSTEM
- MULTI-FACTOR AUTHENTIFICATION

Recovers data & system availability

- DAILY BACKUPS

Communicating

We need to be able to communicate the results of our cyber security reviews, and make suggestions for improvement to the organisation's security (eg Essential 8).

Communicating

4 main types of communication:

Verbal

Non verbal

Written

Visual

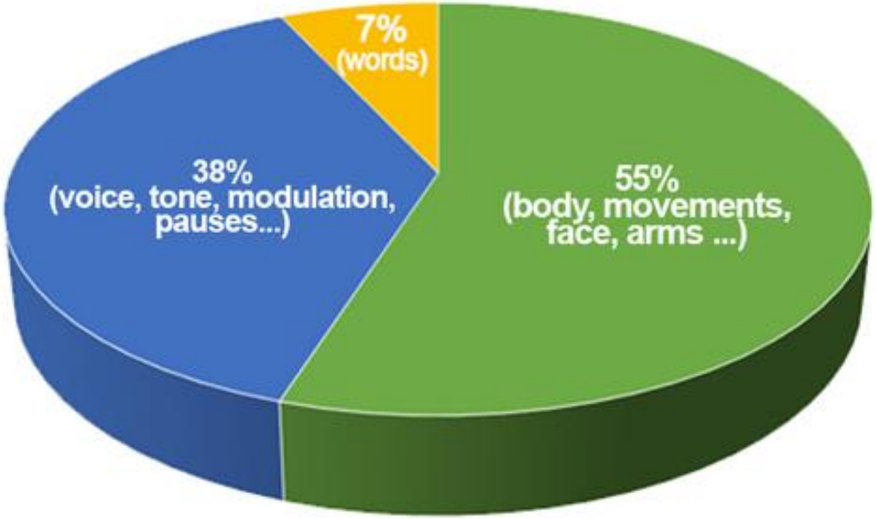
Verbal

You can improve your verbal communication by:

- Using a strong and confident speaking voice
- Using active listening – avoid interrupting, summarize and repeat back
- Avoid filler words – um, like, yeah, nah
- Avoid technical language with a non-tehnical audience

Non- Verbal

Non verbal communication is the use of body language, gestures and facial expressions to convey information



Non- Verbal

You can improve your non-verbal communication by:

- Displaying positive body language
- Use non-verbal communication like nodding to communicate approval and positive feedback

Written

In the workplace we use written communication in the form of emails, reports, letters, memos, books, documents and web sites. Written communication provides a record of information for reference.

Written

You can improve your written communication by:

- Striving for simplicity and using clear and appropriate language
- Avoid tone. When verbally communicating we can indicate a joke, sarcasm etc with our tone of voice. When writing we should keep to plain and simple.
- Proof-read written communication to identify mistakes or opportunities to say something different

Visual

Visual communication is the act of using photographs, art, drawings, sketches, charts and graphs to convey information.

Because people have different learning styles, visual communication can be very helpful to communicate ideas and information. Especially in conjunction with written communication.

Visual

NO RUNNING
Slow Down!

Visual

You can improve your visual communication by:

Selecting your visuals carefully (some might offend or confuse)

Consider your audience. Overly complicated visuals (eg charts) might distract from your message.

Corporate communication

Ways to communicate your cyber security review outcomes and improvements need to align with the corporate practices of your workplace.

Corporate communication

Encourage open discussion

When staff are encouraged to communicate openly, they feel valued and are more likely to give feedback and express opinions.

Corporate communication

Face to face

Whilst email is convenient, large volumes of emails can lead to a reduction in effectiveness of communication

It can be simpler and quicker to talk directly to a colleague via face-to-face conversation

Corporate communication

Be careful when wording emails

It's difficult to intepret 'tone' when reading an email eg sarcasm.

Brief emails can be ambiguous and confusing

Emails require proper spelling, punctuation and grammar (and they are a lasting digital record)

Corporate communication

Body language

You ought be aware of your body language and how people may react to it

You ought endeavour to communicate with a positive physical presence eg smiling, eye contact, uncrossed arms

Corporate communication

Meetings

Meetings should be held when necessary, not for the sake of it

Meetings should have an agenda, a time limit and a clear purpose

Corporate communication

Visuals

Relevant graphics can help to reinforce your messaging

Questions

What are the latest cyber security threats and trends?

What are the recommendations to prevent cyber attacks?