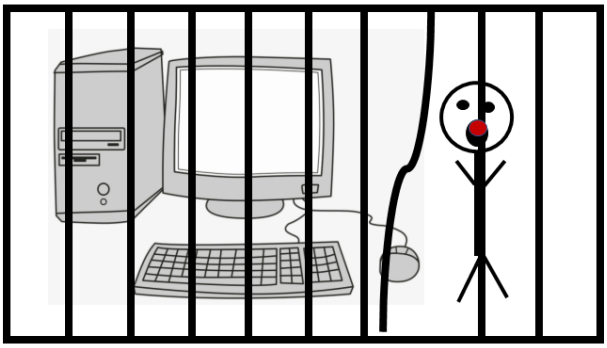
Slide 1

Security Breaches

- A security breech can be likened to a break in on a house. In terms of security breeches in term of computing may occur if an unauthorized person gets hold of sensitive data belonging to your organization. If a security breech does occur it can damage the organizations reputation and could result in financial loss.

Types of security breeches
Viruses
Spyware
Malware

Real life examples
Equifax security breach
Facebook security breach
Yahoo security breech



What is a system breech?

It is an incident that results in unauthorised access of data, applications, services, devices. Hackers do this by bypassing the underlying security measures that an organisation have in place. It is also sometimes referred to as a security violation. If a security breech does occur within an organisation it can result in the reputation of that organisation and could ultimately result in financial loss.

Types of security breeches

There are 3 main types of security breeches and these are;

Viruses are a piece or sequence of computer code that is capable of multiplying itself so it spreads across your whole computer network. Hackers can use different types of viruses depending on what they are tying to achieve. The most common ones used by hackers are;

Direct action, Browser highjack, Overwrite

Spyware is unwanted software the infiltrates your computing device. It's classed as a type of malware that is capable of gaining access to your internet usage data and much more. It monitors your internet activity without you knowing, remembers things like your password and billing details.

A total of 978 million people in 20 countries were affected by cybercrime in 2017, according to Norton Cyber Security Insights Report Global Results.

Victims of cybercrime globally lost $172 billion.

Jake Leonard

Slide 2

Firewall

- Having a firewall installed can help to minimise security breeches into a system, it can filter information that enters the system and block unauthorised access with the use of a whitelist (list of authorised access) and backlist (list of unauthorised access) it also prevents against malware attacks.

A firewall can help to minimise security breeches from viruses, malware and spyware attacks. The firewall can block unwanted traffic form the internet, this includes blocking malware, spyware and viruses as it acts like a filter between the network and the internet allowing authorised data to pass through, while blocking malicious programs. One of the ways it can filter is with the use of a whitelist, the firewall can be configured to block all traffic from the internet except the traffic from the white list (a list of authorised IP addresses to accept data from).

Charlotte Peachey

Slide 3 (My work)

System Software update and business

Software, whether high level or low level, should be updated regularly.

There are a few benefits to keeping software up to date, not limited to feature updates. These benefits often revolve around security.

- Low level security patches – exploits and issues that allow for attacks. Example of this would be Heartbleed or ZombieLoad.
- Higher level security – Issues with software like Word or Chrome that result in system instability or security risks.

Software should be updated regularly. Updates are important as they help prevent against security risks.

Problems with low level software are risky as they often go unnoticed and often can result in the biggest issues. Heartbleed is a bug in OpenSSL that allows for an attacker to gain any information stored in the memory of the target server. As well as this, ZombieLoad is an issue in Intel CPUs that allows for a program to access sensitive data that the CPU is accessing, like passwords and files. These are both issues that can be fixed through updating software.

High level software can have issues that result in similar problems, although the impacts are usually less severe. Passwords and data are still at risk, however, and keeping software updated can solve these issues.

Charlotte Ward

Slide 4

Anti-Virus Software

- Purpose?
  is to detect neutralize or eradicate malware
- How does it work?
- 1st scan the computers files to seek out any viruses that fit the description in the virus dictionary
- Using a method called heuristic analysis, it will also try to detect suspicious activity from any program or software that may be affected

The software will not only identify and destroy the computer virus, but its also designed to fight off other kinds of threats such as phishing attacks, worms, torajan horse rootkits and more.

Fairly recently (first quarter of 2013) was a time that was the most active, ever, for the entire gamut of malicious software generation.

More than 14 million new samples were identified by McAfee.

Malware is evolving, becoming savvier. An example is the Zeus malware that gets spread when the user unintentionally downloads it (from being tricked into doing so), or, when the user opens an attachment in an e-mail, not knowing it's poised to infect his computer. This malware is smart because it evades anti-spam software by presenting as graphics instead of text in the e-mails.

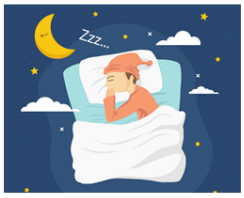
Every month means about six million new botnet infections.

Between the first and second halves of 2013, new phishing websites doubled in number.

Sixty percent of the leading Google search terms returned malicious sites just in the first 100 search results alone.

Jake Leonard

Slide 5



System Downtime

- System down time is the span of time where the system is unavailable. This occurs when a system fails or shuts down for example when a power surge/shortage occurs rendering the system unable to carry out its functions and as a result needs recovering in order for the company to operate at its full capacity.
- System downtime can be minimised with the use of a good recovery plan. Having a recovery plan in place means that if that system goes down there is a procedure in place to get the system functioning as soon as possible minimising the downtime of the system.

System down time

System down time is the span of time where the system is offline. This needs to be minimised for a number of reasons, including to ensure the company can continue to function as it normally would for as long as possible. There are multiple different ways to reduce system down time, the first is:

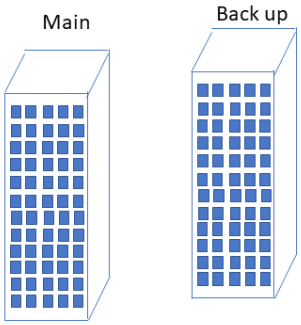
Charlotte Peachey

Slide 6

Recovery plan : Server Redundancy

- Server redundancy is when a replica server is created that is identical to the main server the company uses. This server is then used to store a complete back up of the main server.

New York stock exchange



Redundancy

A recovery plan is infrastructure that can be put into place in order to minimise the downtime experienced by a system. One of the recovery plans that can be used to minimise system downtime is redundancy. Redundancy is when a full backup and identical copy is made of the system, this will include all the infrastructure e.g. servers and data copies stored on them. Toy story 2 example, when working on toy story 2 a command was mistakenly executed that deleted all of the data for the film, the backups had not been working for weeks however as one employee had been working from home a lot ,due to having a baby, she had all of the data saved onto her home computer which acted as an unexpected backup of the animation for the film. The New York stock exchange has identical backups of all of its data as part of its recovery plan, there is a fully redundant backup site for the NYSE.

Redundancy useful to minimise the system downtime as when the main server goes down the company can transfer to using the back up server system meaning the system is only down for a short amount of time. The main system can then be recovered with the use of the back up system resulting in minimal downtime and data loss. Ideally this back up server will be updated with the data from the main system once per 24/48 hours the more frequently the system is updated (when the company is not using the system) the less data will be lost.

Charlotte Peachey

Slide 7

Recovery plan : backup generator/extra power source (Uninterrupted power supply)

- **Overview**
- This is a power supply that is usually placed on a site separate to where the computer network
- **Benefits**
- Emergency power supply
- Maintains battery life
- Huge power back up in the industries

The direct alternative current is conditioned and supplemented by external power supply known as the Uninterrupted Power Supply (UPS) System. Previously, it was used for computer systems but when its valuable benefits were observed, it found its use in various areas such as factories, cordless phones, motor etc. It can be used for getting long power back up as an inverter. You can choose the size and functions of the UPS depending upon the demand and supply. Critical load shedding and uncertain disruption of power supply can be sorted with good quality UPS.

Whenever there is a power spike or a blackout, UPS stands as the reliable alternate power source. You can resume your work by using UPS in case of long power cuts.

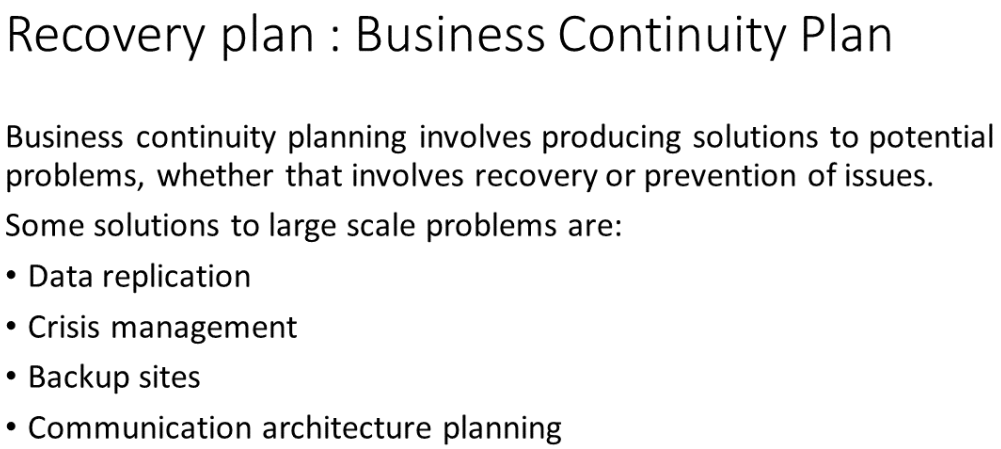
You can keep working on the operational mode even when there is a power cut as it maintains constant charging once you connect a UPS to a battery.

Various firms rely on UPS and connect it with their gadgets and machines. It can hugely affect their work output if there is a power disruption and therefore UPS is the essential need when it comes to smooth operation at work.

UPS is a major need in both household and commercial organizations. It is one of the best forms of temporary power and should be only used which comes with good quality. If you are a resident of UK and you are looking for UPS, then Temporary Power Solutions stands as the perfect destination for you. Here you will be guided by expert professionals so that you get the best power solution at the best budget.

Jake Leonard

Slide 8 – My Work

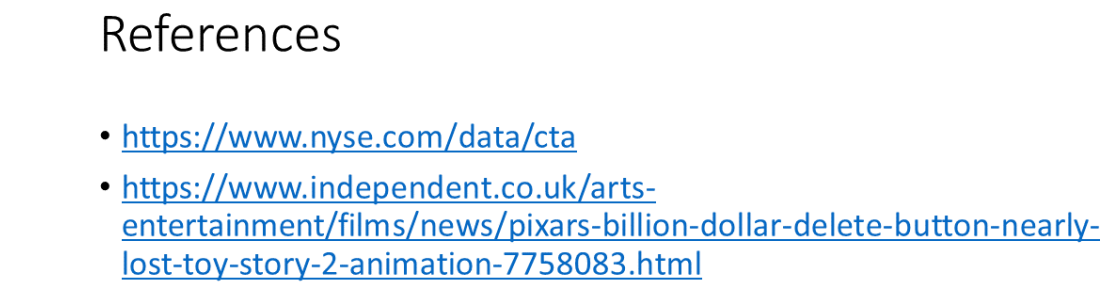


Business continuity plans involve producing solutions and preventative measures for problems that a company could face. Planning and thinking about recovery methods helps lower system downtime, resulting in faster and more structured recovery. As well as this, preventative measures attempt to stop a problem from happening in the first place, identifying potential risks and mitigating them before they evolve.

Some common solutions to large scale problems are data replication, crisis management, backup sites and communication architecture planning. These all help resolve issues that could come up, like loss of communication, or data loss.

Charlotte Ward

Slide 9 - References



Nyse.com. (n.d.). *Consolidated Tape Association*. [online] Available at: https://www.nyse.com/data/cta [Accessed 15 Jan. 2020].

Orr, G. (2012). *Pixar's billion-dollar delete button nearly lost Toy Story 2 animation*. [online] The Independent. Available at: https://www.independent.co.uk/arts-entertainment/films/news/pixars-billion-dollar-delete-button-nearly-lost-toy-story-2-animation-7758083.html [Accessed 15 Jan. 2020].