Dc, use this appropriately.identifies who gets access

Business, Accounting

DC, JP, RL What is a security policy and why does an organisation need a security policy? A security policy identifies the rules and procedures for all individuals accessing and using an organisations IT assets and resources. 1 The objectives of an IT security policy is preservation of Confidentiality, Integrity and Availability. Also known as (CIA). Confidentiality can be broken down into two main factors: data confidentiality and privacy.

Data confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals. Privacy ensures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Integrity consists of two key areas : data integrity and system integrity. Data integrity ensures that information and programs are changed only in a specified and authorized manner. System integrity ensures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. Availability ensures that systems work promptly and service is not denied to authorized users. There are many reasons why an organisation may need a security policy, these include: They address threats, for example the global exposure to ransomware, which can be devastating and costly to companies.

Identifies who does what, when, and why, ie: The administrator has to ensure that each user has secure login credentials to a site for example: the password has to follow a particular format and it’s up to them to use this appropriately. Identifies who gets access to what, for instance certain teams in large corporations will sign an NDA with a client. It is important that other

teams in the company do not have access to these documents on the company’s file server. Outlines what the penalty is such as : Queen’s University’s penalty of pen testing the server will result in academic discipline. 2.

DC Come up with an example of your own of an issue, which could be caused by missing security policies? A common, but often overlooked example of a missing security policy issue is the encryption of USB flash drives. Many companies have very sensitive information on their servers, whether it be client confidential documents or financial reports yet to be released. These are easily downloaded onto the employee’s (encrypted and secure) laptop/local machine. But sometimes the scenario where the employee copies the documents to their flash drive to take home and review/work on hasn’t been considered. The issue with this is that the USB Flash drive often is not encrypted because the company hasn’t considered this as a potential threat. All it takes is for the USB drive to be misplaced and the security of the data has been compromised, resulting in a loss of client confidence and the dismissal of the employee. This could all be prevented if only encrypted USB drives are allowed to be plugged into a work machine and the data is encrypted upon being copied to said machine. A famous example of a failure in this policy is when Edward Snowden was able to walk out of the NSA with top secret documents on his USB flash drive 2 and then shared them with Glenn Greenwald, a reporter at the Guardian, which resulted in the documents being released for public scrutiny.

3. DC, JP, RL What are the basic things that need to be explained to every employee about a security policy? At what point in their employment? Why? (List at least 4 things). (For example, how to handle delicate information)There are a number of things which need to be explained to each employee about a company's security policy which are outlined below: How sensitive information must be handled: Sensitive information such as employees details must be handled correctly and those only with correct permissions would only be able to gain access to this information.

3 How to properly maintain your password, as well as any other accounting data: Passwords for example should be maintained regularly and updated correctly using the correct requirements for example: passwords should contain a certain number of characters. How to respond to a potential security incident, intrusion attempt, etc: This would include emails with malicious attachments and employees being made aware of any disaster recovery plans which maybe in place. How to use workstations and Internet connectivity in a secure manner: At workstations ensure you're securely logged in and out ensuring that no sensitive data is on display.

When connecting to the company's network memorise sensitive information such as passwords and avoid writing them down anywhere where they are visible to intruders. Don't ever connect to a non secure network ensuring that the " https" logo is displayed on any visited webpages. If working from home, ensure that you are connected to the company's VPN. Confidential data should be locked away and out of sight: Confidential data stored on external hard-drives/ USB flash drives for example, should be encrypted and

stored in a safe and secure manner. The above examples should be introduced at the very start of an employee's employment as they could never have come into contact with a security policy before and security policies often differ across various companies. You cannot assume knowledge of security policies, otherwise you are opening yourself up to a major potential breach.

This should often be revisited. For most organisations there are different annual retraining events and sign-offs that need to be completed when an employee is handed a security policy. Reinforcement is a key factor in such security policies. They can be reinforced by internal newsletters that allow employees to stay aware of vulnerabilities and also by ' Did you Know' internal company emails which can be circulated around weekly. 4. DC, JP, RL Your organisation has an e-mail server that processes sensitive emails from senior management and important clients. What should be included in the security policy for the email server? Having a detailed security policy for the email server is key in ensuring in the confidentiality of the data on the server. Some of the points that need to be considered when designing the security include: The prevention of email spoofing, where an attacker can mask their email address and replace it with the email address of an employee.

This can lead to a breach, if, for example, the attacker emailed another employee asking for certain data/files. Since the owner of the email that is being spoofed would normally have the permission to access these files, the victim of the attack will most likely send the data to the attacker. Banned

attachment types, certain file types, for example . exe files, are commonly used to transfer ‘ malware’ such as viruses, spyware etc through an email server.

For security purposes an organisation would not want them to pass through any servers incase this leaked sensitive data to an unauthorised user. If an employee needed to send or receive file types it should be archived first using a file type such as ZIP. No spamming – one of the most important aspects of a email server is that it should be available and running all the time.

A lot of companies work across continents and timezones and therefore if the server goes down, communication can be disrupted and this can lead to a loss of productivity/revenue. One way the server can be taken down is through repeated spamming of emails/requests, which is a form of DDoS attack. A good email server policy should be well equipped to deal with such attacks (i. e.

a strong firewall to prevent a SYN flooding attack) and have a contingency plan in place if one of the servers is taken down. Spot check emails – In a secure email server, there will be a filter which ensures that emails are genuine. There are also a number of tell tale signs which can be flagged up if an issue arises.

The email could have a mismatched url which can be spotted by hovering over the attached link. The message might ask for personal information such as credit card details. In order to overcome this, emails can be filtered and

quarantined in order for them to be reviewed for their authenticity. This is usually done by one of the IT Systems Administrators. Furthermore, any emails that are leaving the server that are directed to an outside organisation should usually be spot checked to ensure that a rogue employee is not breaching company security policy. 5.

DC, JP, RL Read the UCL and Harvard university security policies 1, 2. Compare and critique the policies suggesting improvements/updates, as appropriateJP, RL UCL and Harvard university both have security policies in place ensuring that both staff and students follow specific guidelines when connecting to each of their own networks. The UCL security policy provides a general insight into how the users should adhere to the information security policy.

When comparing this to the Harvard University's Policy statements, the university provides an in depth analysis of how each user, device and server should adhere to the rules and procedures covered in the security policy. An improvement for the UCL would be to cover the elements of devices and servers similar to that of the Harvard University policy alongside the users aspect. JP, RL Concerning the user's own personal responsibility, users are asked to act in a " responsible and professional way" through the UCL security policy. This policy does not state of what this requirement entails for the user's behaviours.

The Harvard University provides real life examples of how the user should behave when connected to the university network such as protecting your

own devices and what to do whilst using them/ information on what happens if you lose these. An improvement on this would be for the UCL to have a specific list of user's " professional" manners whilst using the network. JP, RL Through both policies there is a clear section on who is responsible for each security policy within the university. UCL users report to the UCL Information Security Group and Harvard University report to Chief Information Security Officer Christian Hamer. An improvement to both these methods would be to include contact information if any user needs any training or consultancy for example feel amendments to the policy are required. DC Also, it is clear from looking at the policies that it is easier to find the information that is relevant in the Harvard page compared to the UCL page.

The Harvard policy is broken into different sections/hyperlinks whereas the UCL policy is in a massive . pdf document. An upside to the Harvard policy will be that the right information will get across to the user quickly and they won't have to scan through a large document to find what they need. It is worth noting, however, that UCL provide a handy 2 page infographic that summarises their policy for the user. Also, the Harvard policy, whilst getting the right information across, can require more clicks than the UCL one. For me to get to the user policies, it required 2 clicks from the home page, compared to one click on the homepage for the UCL page. An improvement to the harvard policy would be to have an infographic that summarises the policy for a basic user to get the information quickly without dropping off. DC, JP, RL In the Harvard policy, it is not explicitly clear who is authorised to access each level of data, for example in the Harvard policy they mention

handling credit card transactions 4 but don’t state what level of user will be able to access this information.

This is bad practice as it doesn’t identify who does what and why, which is a key element of a Security policy (Integrity). This is also apparent in the UCL Security policy, it mentions different people such as “ Heads of Department” 5 but doesn’t explicitly state what their level of access is. If you were to implement this Security policy you would need to know who gets access to what, otherwise it is not effective at limiting the data to the correct users. Finally, in the UCL policy, there is specific reference to availability (i. e.

“ authorized users always have access to information when they need it” 5) whereas in the Harvard policy there is no explicit reference to availability that is readily available. An improvement to Harvard’s policy would be to have explicit reference to availability. Overall, you can see that both policies have their positives and negatives. The UCL policy has a handy user guide leaflet which is good to key the key information across to the user without them dropping off. The Harvard policy has a lot of more in-depth information available, but at an inconvenience to the user with many button clicks required. Both policies had reference to who is responsible for the security policy which was encouraging.

Electronic Documents: General Internet Site1CyberPedia, “ What is an IT Security Policy”, Paloalto Networks, para. 1, 2017. Online, Available: https://www. paloaltonetworks. com/cyberpedia/what-is-an-it-security-policy

Accessed Jan 23rd, 2018. 3Adi “ At what point in their employment should security policies be explained to an employee?”, StackExchange, para.

1, Jun. 18, 2015. Online, Available: https://security. stackexchange. com/questions/94231/at-what-point-in-their-employment-should-security-policies-be-explained-to-an-em Accessed Jan 23rd, 2018Newspaper Article From the Internet2Shaun Waterman, “ NSA Leaker Ed Snowden used banned thumb-drive, exceeded access”, The Washington Times, para.

1, June 14, 2003. Online, Available: https://www. washingtontimes. com/news/2013/jun/14/nsa-leaker-ed-snowden-used-banned-thumb-drive-exce/ Accessed Jan 23rd, 2018. Professional Internet Site4Harvard University, “ Information Security Policy”, Harvard University, 2017.

Online, Available: https://policy. security. harvard. edu/level-3#widget-0 Accessed Jan 23rd, 20185 UCL, “ Information Security Policy”, UCL, section 1. 2 – 2. 3, 6 Sept, 2016.

Online, Available: https://www. ucl. ac. uk/informationsecurity/policy/public-policy/information-security-policy. pdf Accessed Jan 23rd, 2018