WebF1 Literature Review
Mitigating corporate information exposure on the web.

There are many ways that data exposure can damage a company today and mitigating the effects is important in helping to reduce the loss that the company makes when data is leaked. states that data leakage is becoming more and more of a risk “because more forms of communication are being utilized within organisations, such as instant messaging; VOIP; etc.” *Gordon (2007, P6)*

One way to mitigate this kind of data loss is by creating a mitigation plan that’s based on the the risk tolerance of each important data asset. Each piece of data a business stores has varying levels of importance and how damaging it is to the business if leaked. The plan should contain findings of the exposure risks of internally and externally and an estimate of the business impact exposing this data would have. They can also assess the security measures they have in place for different data and compare the importance of the data to how restricted the access should be and the level of security in place to protect it.

Another way of reducing internal exposure is by limiting employees access to data and what they are allowed to do with it for instance only allowing employees to use their internal email account and having that account be unable to send messages to people outside of that email like students only being able to email people with myport.ac.uk addresses. Another way to reduce the vulnerability of having employees is by either ruling out or monitoring the Bring Your Own Device business practice. While cheaper, companies underestimate the internal threat of data leakage over the seemingly more threatening external leakage, having personal devices at work means employees can store corporate data and take it off property where the business has no control over what is done with it. I *(Etsebeth, 2011, p.6).* Employees can also maliciously leak data through File Transfer Protocols to deposit them on remote servers. Instant messaging like emails and social media are more likely methods of internal exposure and businesses need to regulate the use of this as the threat of it is just as dangerous as external exposure. “The information age, and more specifically the use of the internet by most companies, make corporate and industrial espionage faster, easier and more anonymous” *(Etsebeth, 2011, p.3)*

Another method of preventing external exposure is through an application proxy firewall,”Stateful Inspection firewalls will examine traffic at the Transport or Network layer and either allow it to pass through, or block it based on its rule set.” *Gordon (2007, P40)* A compromised website could easily have malware that can automatically downloaded to a vulnerable device. An application proxy firewall would analyse the behaviour of the malware and at the application layer and then detect it’s malicious intent. Another method in safeguarding employees on the web is through Cloud Web Security.”keeps malware off the network and helps organizations of all sizes more effectively control and secure web usage.” *(Cisco 2016, P4)*. By removing the malware from the web it mitigates the chances of company computers being breached through malicious websites.

There are other less technical ways to mitigate the data. The structure of the building a company operates in can also have vulnerabilities such as ensuring that security on the site is secure by using key cards with different levels of access depending on the employee to prevent people getting unauthorized access to the building or certain computer rooms.

There are still ways to mitigate cooperate damage after a third party has gained unauthorized access to the system, one way is by encrypting data stored on a server to prevent the malicious attack from gaining any valuable information, a company can use 2 types of encryption, symmetric encryption involves a key that the company keeps secured that can be used to both encrypt and decrypt the data, this means hackers will not only need to acquire the data but will also need the key that encrypts the data, mitigating the risk of damage to the company once breached. The other method is through asymmetric encryption, this is where 2 keys are used, the public and private key, the public key is used by the senders to encrypt their data and a private hidden key is used to decrypt the data on the receiving end. This eliminates the possibility of the data being hijacked while being transferred as it will be rendered useless without the private key. Both these methods aid in reducing the chances of hackers making any use of data they intercept once within a company's computer system. *(Young, P2)*

Password cracking is one of the most common methods of unauthorized access. Passwords that are predictable or with few characters can be particularly vulnerable. Methods like Brute force hacking which simply attempts to guess every combination can easily work out a person's password however "The feasibility of brute force depends on the domain of input characters for the password and the length of the password" *(Martin 2012, P4)*
Dictionary attacks are like brute force attacks but take a more logical approach to password guessing taking into account average english words and capitals at the beginning further reducing the time taken to crack. A way to mitigate this type of attack is by using hashing to encrypt the passwords such as MD5 which creates a 32 digit hexadecimal number which is much harder to revert to its original.

To conclude the best way to mitigate data as a company is simply by assessing the data before it has a chance to be exposed, they must identify the critical data and assess where it's used, how it's used, and who is using it. companies of today must take into account their business however their security is more important than ever, computers play such an important role in the way businesses function and where there's data assets there is likely someone externally or internally with an interest in possessing it for either profit or for malicious intent. Companies must take this into account and ensure the best security measures to mitigate the damage done when data is stolen and in preventing the chances of it being intercepted.

References

1. *Gordon, peter (2007) Data Leakage – Threats and Mitigation* *https://uk.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931*

2. *Password Cracking Sam Martin and Mark Tokutomi, 2012* *https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf*

3. *Cisco. (2016). Mitigating Web Threats with Comprehensive, Cloud-Delivered Web Security.* *https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/mitigating-web-threats.pdf*

4. *Etsebeth, V. (2011). Defining the Current Corporate IT Risk Landscape. Journal of International Commercial Law and Technology* *http://www.jiclt.com/index.php/jiclt/article/view/127/125*

5. *Foundations of Computer Security, Dr. Bill Young* *https://www.cs.utexas.edu/users/byoung/cs361/lecture44.pdf*