Slide 1: What is a data breach

A data breach occurs when a hacker accesses/distributes/monetizes information obtained from a server. For context a server is just a machine that hosts a variety of applications, in this case a web server. Data breaches typically effect not just the company but employees. Most the time the information leaked is employee information including SSNs and other sensitive information. This can result in additional costs to businesses.

Slide 2: Who's responsible for data breaches?

Script kiddies, this is often a term referred to novice hackers who use a variety of publicly available tools to hack various sites. The reason they do this is either monetary or to get fame i.e. a news article. It's typically teenagers and they usually are doing it for the fame or the challenge. Another subset includes state sponsored hackers. These are hackers that work off the books for various government agencies to perform sabotage or espionage against other countries assets. Finally organized cyber-crime groups often perform attacks with the intention of monetary gain. They would attempt to sell data they were able to steal from the website.

Slide 3

The global impact of a data breach on an organization is $3.86 million dollars. That's a hefty sum for some data that could have been protected better. Each record stolen typically costs about $148 and on average it took an organization 197 to identify they've been affected by a data breach and it took them on average 69 days to secure the entry used by attackers and further protect customer data. Usually customers affected are offered life time credit monitoring services on behalf of a company which can make it a costly ordeal.

Slide 4

The reason why a data breach can cost a business so much is due to the amount of time to find the breach. A report from IBM concluded that an organization impacted by a data breach can save $1 million dollars if they discover the breach within 30 days. In addition to this the associated cost can raise when new technology is needed to be purchased/third party companies need to be hired to help assist the security process. Another cost is linked to lost/stolen records, on average they cost a company about $148 as mentioned earlier. There may even be an increased cost if they're demanded to provide credit monitoring for those impacted. An example of this was Equifax who offered everyone credit monitoring for life at no cost. In addition to this government fines may also be assigned if the investigation concludes that the proper security precautions were not taken. An example of this can include not encrypted stored credit card data. Encrypting simply refers to making a String of any characters into a variety of randomized characters.

Slide 5

In addition to costing a lot a data breach can also harm a business in several ways. One of the most common characteristics associated with a data breach includes diminished reputation. For example, a security company were to get impacted by a data breach what companies would hire a security company that couldn't protect itself. According to a study 46% of organizations they suffered damage to their reputation and brand value as a result of a data breach. Another effect of data breaches includes a

decreased competitive ability. This is especially true if a hacker were to steal propriety information from the business rather it would be information on existing projects or ideas they hope to pursue in the future. This is referred to as corporate espionage. Another way a business could affected is through loss of customer trust. Clients share their sensitive information with companies and it only makes sense they would want to make sure their information is safe. Reduced revenue is another factor when a data breach occurs as they might need to completely turn off their systems to find the vulnerability. This can result in no access to their site and possible lost sales as well

Slide 6

Data breaches can be prevented. Some of the common ways include regular security audits. This typically includes a team of ethical hackers attempting to break into the company network and patching vulnerabilities. In addition to this software updates typically fix large scale vulnerabilities discovered by software vendors. In addition to this a company can also purchase cybersecurity insurance which can be used to help cover the costs of a data breach. However these policies are typically very strict. A good example is Equifax, they attempted to claim money however one of the clauses in their insurance was it doesn't protect against acts of war. And since the hack was attributed back to North Korea they refused to pay out the company. They are currently in the midst of a court battle to determine the outcome.