Research Assignment #1

Shawn Ziegler

CYSE 300

September 5, 2025

In today’s society, cybersecurity plays a crucial role in keeping information safe. Many organizations rely on security to protect credentials, financial records, and threats. Cybersecurity is crucial in making sure that things run smoothly within a working environment, as well as ensuring that people are safe within the working space. Organizations that have a security system are able to create structure for their organization by having a protected network that only people within the work environment have access to. Computer systems that require login information to ensure that only people within the organization can have computer access. All of these security measures allow a company to reduce the risks of potential threats from happening.

Allianz Life is an insurance company based in Germany that provides services to over 128 million customers. On July 16, 2025, the insurance company experienced a malicious attack on a third-party cloud-based system used by the company. The attacker impersonated as an IT help desk employee and persuaded employees within the company to allow access to a system used by the company. Salesforce data loader tool is the system that Alliance Life uses to store sensitive data. The company was able to gain access to full names, social security numbers, policy and contract numbers, dates of birth, mailing addresses, and phone numbers of customers who use the insurance company's services. All of this information was exposed due to the attacker being able to use social engineering as a way to gain access to the system. This breach of the Salesforce system shows that a weak link outside of the network could lead to the exposure of sensitive data, which is what the Alliance Life insurance company experienced with this attack. A website known as Bleeping Computer provides technology news reported that hackers had gained access to the system was a cyber extortion group known as the ShinyHunters. The extortion group has been focusing on Salesforce customer relationship management (CRM) systems. Shiny Hunters have a well-known history of executing similar breaching tactics on big

companies such as Microsoft, Santander, Ticketmaster, Tokopedia, and AT&T (Uberoi, 2025). ShinyHunters was a term originally used in Japan by members involved in the Pokémon community. In April 2020 cybersecurity firm, Intel471, a cybercriminal group took the term and used it as a name to sell and steal data (Thierry, 2022).

Breaching attacks are one of the most common attacks that appear in cybersecurity. Many companies that encompass a system that stores personal information are the designated targets of these threats. While most companies have strong security systems, Alliance Life's case was proven otherwise. Since the attacker was able to manipulate their way by using social engineering to gain access to the system displayed that someone within the company lacked awareness. The insurance company should regularly implement training for employees to make sure they continue to stay up to date with the company's policies. The training should also include guidance on how to recognize different threats. Implementing simulated exercises and practical tools to ensure employees are well prepared and up to date to maintain a strong security system. The insurance company also implements access controls such as multi-factor authentication. In this case, though, it was user error. Access was granted based on the employees' allowing access to the system. In this case, the company could incorporate a more strict authentication protocol. The first authentication access point would be through multiple employees. After the information to confirm access has been relayed through multiple employees, that information should be sent to a higher-up role within the company to ensure validation that it is safe to allow access. Implementing this multi-step verification process ensures that it will not be easy for someone outside of the organization to gain access unless it is confirmed by a higher-up within the organization (G., N. 2025).

References

G., N. (2025, February 4). *How to prevent data breaches: Strategies for 2025*. Prey. https://preyproject.com/blog/how-to-prevent-data-breaches-5-essential-tips

Thierry, G. (2022, August 5). *Who are the shinyhunters, the hacker group a Frenchman wanted by the FBI is suspected of belonging to?*. Le Monde.fr. https://www.lemonde.fr/en/pixels/article/2022/08/05/who-are-the-shinyhunters-a-hacker-group-an-fbi-wanted-frenchman-is-suspected-of-belonging-to_5992595_13.html

Uberoi, A. (2025, July 28). *Allianz Life Data Breach 2025: Timeline, impact and analysis*. Home - Cyber Security Training. https://www.cm-alliance.com/cybersecurity-blog/allianz-life-data-breach-2025-timeline-impact-and-analysis