Leader Update-Cyber Crime

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

Organizations and businesses these days are facing challenges and threats which were not even known some decades ago. Cyber criminals use modern technology as a tool very effectively for their criminal and malicious intents. A cybercrime is referred to as a crime related to information technology where the aim of the offender or attacker is to get access to a computer system or device or to deny access to a legal user. In recent years, a number of cases are reported where cyber criminals accessed sensitive data of the organizations and imposed huge damages in terms of finance, reputation, and important information(*Cybercrime*, n.d.). In this background paper, some important cases of cyberattacks are going to be identified with the analysis in order to determine what lessons PBI-FS can learn and how can we improve the security to prevent such attacks.

The financial sector has experienced several cyber-crimes in previous years. One of the examples in the data breach of Capital One. The attack happened when a hacker gained access to one of the credit card applications. The breach was detected on July 19 and according to the report, about 80,000 bank account numbers and 140,000 social security numbers were exposed(Thomas, n.d.). In short, one significant gap in the security of the IT-related aspect caused massive damage. Historically, web applications and web sites are considered a weak spot and have been exposed a lot of times.

Another breach identified is Westpac which was a cyber attack on PayID. PayID is an authentication service and a third-party account of the payments platform. The attack resulted in the exposure of banking details of almost 98,000 customers(*Westpac security breach: Almost 100,000 customers exposed, cybersecurity news update*, n.d.). Although the application was supported by government organization it does not mean that it is secure and cannot be exposed to the cyber attack.

These attacks suggest that it is essential to have a compatible, state of the art and secure plan for cybersecurity especially its infrastructure of the financial services of PBI-FS. It is the prime time to continuously monitor and assess the performance of the third parties which are in possession of sensitive information irrespective of whether they are privately held and operated organizations or government departments.

For an effective cybersecurity program of Padgett-Beale, it is very necessary to have an automated detection anomalous behavior and a least privilege model(*What is Anomaly Detection?*, n.d.). Because in many cases the insider attacks are very difficult to detect and prevent as compared to outside attacks. In order to protect the financial services of the organization, a combination of tech solutions and robust policies is necessary to help the organization in protecting the sensitive data and financial services of the company.

References

*Cybercrime*. (n.d.). Retrieved February 24, 2020, from https://www.interpol.int/Crimes/Cybercrime

Thomas, B. (n.d.). *Financial Data Breaches 2019: Capital One, First American, Desjardins, More*. BitSight. Retrieved February 24, 2020, from https://www.bitsight.com/blog/financial-data-breaches-2019-capital-one-first-american-desjardins-more

*Westpac security breach: Almost 100,000 customers exposed, cyber security news update*. (n.d.). Retrieved February 24, 2020, from https://finance.nine.com.au/business-news/westpac-data-breach-100000-australian-customers-at-risk/84c91581-90b6-464e-9137-a2d973492614

*What is Anomaly Detection?* (n.d.). Retrieved February 24, 2020, from https://www.anodot.com/blog/what-is-anomaly-detection/