

Initial Post: Discuss Data breach and cyber attacks

It has a ripple effect on businesses, consumers, and government agencies because of the growing risk of data breaches. When a company has a data breach, it can lose money, reputation, legal fees, regulatory fines, and records. Consumers can lose money, have their identities stolen, and be in pain because of fraud or identity theft. (Le & Zemora, 2018).

Governments have taken steps to strengthen information security by demanding government agencies and enterprises to adopt security standards and promoting cybersecurity infrastructure. Along with national, regional, and international data protection legislation, nations and intergovernmental organizations have developed and implemented guidelines and principles for the public and private sectors worldwide. (UNODC, N.D.)

Many data breaches go unnoticed for longer periods of time; on average, it takes 9 months to detect a breach, with a total cost of \$5.33 million for a company with 25000 employees. (IBM, 2021). Phishing attacks, human error, privilege misuse, or even a wrong decision leading to malware infection account for 85 percent of all breaches. (Spitzner, 2021).

Government agencies and nonprofit are providing framework and guidelines how the response to the cybersecurity breach. This includes notification procedures to government agencies, credit agencies, business and individuals. (FTC, 2021).

The rise of cybersecurity laws indicates a growing realization of the high importance of good IT infrastructure in preventing data breaches. In recent years, it is clear that cybersecurity has become a priority for business budgets. Many businesses focus their security budgets on practical areas of operations while maintaining compliance and development. (Le & Zemora, 2018).

Reference:

1. Van Ha, L., & Bianca, Z. (Aug,2018) CyberSecurity Privacy and Data Protection. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-4/the-price-of-a-data-breach> [Accessed 12 March 2022].
2. UNODOC (N.D.) CyberCrime Education of Justice, Data protection legislation. Available at: <https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/data-protection-legislation.html> [Accessed 12 March 2022].
3. FTC (2021) Data Breach Response: A Guide for Business Available at: <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> [Accessed 12 March 2022].
4. Lance Spitzner (2021) 2021 Verizon Data Breach Incident Report Insights. available at: <https://www.sans.org/blog/2021-verizon-data-breach-incident-report-insights/> [Accessed 12 March 2022].
5. IBM, & Ponemon Institute LLC, (2021) Available at: [https://www.ibm.com/downloads/cas/OJDVQGRY#:~:text=Figure%201-,The%20average%20total%20cost%20of%20a%20data%20breach%20increasei%20by,\)%20represents%20a%209.8%25%20increase.](https://www.ibm.com/downloads/cas/OJDVQGRY#:~:text=Figure%201-,The%20average%20total%20cost%20of%20a%20data%20breach%20increasei%20by,)%20represents%20a%209.8%25%20increase.) [Accessed 12 March 2022].

