Data Security – Tabletop 8

Background
IT Security has three main components: data security, user security, and infrastructure security. Data security covers the concepts or strategies used to keep data secure. Data security involves defining what data needs to be secured, creating data tiers based on the importance of the data or level of PII (Personal Identifiable Information) in the data, and then creating (IT) security strategies that best align with each data tier. Data security focuses on protecting PII from unauthorized access such as a cyber breach or other significant cyber incident.

Currently, numerous and effective data security best practices guidance has been published by a multitude of companies and organizations, including SANs and NIST. Yet PII information continues to be lost due to data breaches and other cybercrimes. Not all organizations implement best practices, cyber hygiene, layered defenses, or even encryption of data. There is a patchwork of state laws that cover data security to varying degrees. There is no national law that assesses the cost of data breaches to the parties that are responsible for the breach and subsequent loss of PII.

Discussion Questions
1. Does your institution deploy security safeguards that adequately protect customer PII information? How or why not?
2. Do you feel that other businesses in the payments or banking ecosystem, also deploy adequate safeguards to protect consumer PII? Why or why not?
3. Do you feel that the cost of breaches, such as those that lose credit and debit card information, are correctly assigned to the company where the breach occurred? Why or why not?
4. Should data security standards be set? By Congress or by private agreement?
5. Should liability standards be set? By Congress or by private agreement?
6. How does your organization look at Data Security?
7. How does your organization look at Data Privacy?
8. What are the differences?
9. Does your organization feel in control of Data Security inside of your organization?
   - Banks?
   - FinTechs?
   - Regulators or Gov Partners?
10. In regards to Data Security and Cybersecurity does your bank, company, or agency us language like this or have you ever heard this said, “We don’t know what we don’t know”, “If we are targeted there is not much that we can do”, “If a large company can not protect themselves, it is unlikely we can”.
11. Do you feel this type of language is taking a strong stance or is this a representation of a victim mentality?
   - Banks, how can this type of language or attitude on security affects the financial sector?
   - FinTechs, how can this type of language or attitude on security affect your business or your role in the financial sector?
   - Regulators or Gov Partners, how does this language impact governmental agencies or the financial sector?
12. How can we work together to change this language within the sector and IT?
   - Training?
   - Joint Exercises?
   - Guides?

Reading Material

- Department of Labor – PII Defined
- FFIEC – GLBA on PII
- NIST – Guide to Protecting PII
- NIST – Cybersecurity Framework
- NIST – Zero Trust Architecture
- Ransomware Self-Assessment Tool
- Money makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report