6.4: Threat Impact

Chapter 5 discussed the different security threats and solutions. However, users need to safeguard their personal information as well.

Personally identifiable information (PII)

According to the FBI's Internet Crime Complaint Center (IC3), $13.3 Billion of total losses has been reported from 2016 to 2020 (IC3, 2020). Examples of crime types include phishing, personal data breach, identity theft, credit card fraud. The age of the victim ranges from 20 to 60 years old. For a detailed report, see the 2020 Internet crime report. The true number may be even higher since many victims did not report for a variety of reasons.

Personally identifiable information (PII) is any information that can be used to identify a person positively. Particular PII Examples include:

- Name
- Social Security number
- Birthday
- Credit card information
- Bank
- Account Numbers
- Government ID
- Address (street, email, telephone numbers)

One of the cybercriminals' most lucrative targets is acquiring PII lists that can then be sold on the dark web. The dark web can only be accessed through special software, and cybercriminals use it to shield their activities. Stolen PII can be used to build fraudulent accounts, such as short-term loans and credit cards.

Protected Health Information (PHI) is a subset of PII. The medical community produces and manages PHI-containing electronic medical records (EMRs). In the U.S., the Health Insurance Portability and Transparency Act (HIPAA) governs PHI handling. In the European Union, a similar law is called data security.

Lost Competitive Advantage

In cyberspace, companies are constantly concerned about corporate hacking. Another major concern is the loss of trust that occurs when a firm cannot protect its customers' personal data. The loss of competitive advantage may result from this loss of confidence rather than from stealing trade secrets by another firm or country.

Major security breaches can severely impact organizations by disrupting operations, enabling cybercrime, eroding customer trust, and tarnishing reputations. Financial losses can also be substantial. Some examples:

- The 2013 Target data breach impacted 41 million payment cards and contact information for 60 million customers. This resulted in a 46% profit drop the following quarter, a 5% share price decline, and over $200 million in legal settlements. (Stempel J. and Bose N., 2015)
- The 2020 Twitter hack compromised high-profile accounts, causing Twitter's stock to drop 3% and highlighting security vulnerabilities. The FTC fined Twitter $150 million. (FTC, 2022)

Reference:

2020 IC3 Report. Retrieved April 6, 2021, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Stempel J. and Bose N. (2015). Target to Pay $39 Million in Settlement With Banks Over Data Breach. Retrieved August 2, 2023, Reuters.com

FTC (2022). FTC Settles with Twitter for Misusing Users' Phone Numbers and Email Addresses. Federal Trade Commission