ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS

Cybersecurity: Data Governance & Information Security

John Wang, P.Eng., CISSP, CISA, CRISC and Ryder LeBlanc, B. Sc.

Defining Data Governance, Information Security, and Cybersecurity

Data governance is a data management concept concerning the capability of an organization to ensure high data quality throughout the complete lifecycle of data.[1] Data governance also refers to data controls and data strategies that are implemented to support business objectives (SAS). Key focus areas of data governance include data availability, usability, consistency, integrity, and security. It involves establishing processes to ensure effective data management such as accountability for the adverse effects of poor data quality and ensuring that data within an enterprise can be used effectively by the entire organization (Vaughan, 2020).

Information security is a subset of data governance. In accordance with the US government National Institute of Standards and Technology (NIST), information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Cybersecurity is a subset of information security that involves protecting electronic data. In accordance with the US Government Cybersecurity & Infrastructure Security Agency (CISA), "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

Typical Steps in Data Governance

A key element of data governance is information asset management.[2] For organizations to properly implement data governance, they need to inventory and classify their informational assets. Creating an inventory of informational assets means that the organization knows where informational assets are stored, transmitted, and processed. Classifying informational assets means that the organization understands the business impact if proper data governance is not applied.

Assessing Business Impact

Within the context of information security, classification is typically based on the business impact to (a) confidentiality, (b) integrity, and (c) availability. For example, using the Royal Canadian Mounted Police / Communications Securities Establishment (RCMP/CSE) Harmonized Threat Risk Assessment (TRA) methodology (Canadian Centre for Cyber Security, 2018), information security classification is based on the criteria outlined in Table 1.

Table 1: Information Classification Criteria

[1] The data life cycle is the sequence of stages that a particular unit of data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life (https://whatis.techtarget.com/definition/data-life-cycle)

[2] Information assets are bodies of knowledge that are understood, shared, protected, and exploited because they have value within an organization.

Level of Injury	Injury to People		Financial Impact
	Physical	Psychological	
Very High	1. Widespread Loss of Life	1. Widespread Psychological Trauma 2. Potential Civil Unrest	> $1 billion
High	1. Potential Loss of Life for Some 2. Permanent Disability for Some 3. Serious Illness or Injury for Many 4. Serious Physical Hardship for Many	1. Serious Embarrassment for Many 2. Serious Doubts/Uncertainty for Many 3. Widespread Public Suspicion 4. Alienation of Large Groups	> $10 million
Medium	1. Serious Illness/Injury to Some 2. Serious Discomfort for Many 3. Minor Pain for Many	1. Serious Embarrassment for Some 2. Serious Doubts/Uncertainty for Some 3. Serious Inconvenience for Many 4. Minor Embarrassment for Many 5. Minor Doubts/Uncertainty for Many	> $100 thousand
Low	1. Serious Discomfort for Some 2. Minor Pain for Some 3. Minor Discomfort for Many	1. Serious Inconvenience for Some 2. Minor Embarrassment for Some 3. Minor Doubts/Uncertainty for Some 4. Minor Inconvenience for Many	> $1 thousand
Very Low	1. Negligible 2. Minor Discomfort for Some	1. Negligible 2. Minor Inconvenience for Some	< $1 thousand

In this information security classification model, all data is classified using the three questions and using the table above to determine the level of injury.

1. **Confidentiality:** How much injury can occur if data is leaked to unauthorized people?
2. **Integrity:** How much injury can occur if data is not accurate, not complete, corrupted, or not up to date?
3. **Availability:** How much injury can occur when information is not accessible to authorized people when they need it or in a format that can be understood by them?

By preparing an inventory and classifying information, an organization can understand the sensitivity of its data and apply the appropriate controls based on classification. For example, encryption may be required if the data is of High confidentiality.[3] On the other hand, the same data may have Very Low availability, which means redundant information technology infrastructure for storing, transmitting, or processing the data is not required.

Identity Theft Protection

The ultimate target of most cyber-attacks is personal information. Identity theft is one of the most common types of fraud and costs society millions of dollars each year. Interestingly, the size of an enterprise does not indicate how vulnerable it is to cyber-attacks, and in North America, 80% of these attacks are classified as phishing.[4] Thankfully, there are some general rules that can protect against these threats.

Identity Theft Protection – Golden Rules

- Never provide information to people who have contacted you, even if you know them.

[3] Encryption is "any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data." (https://csrc.nist.gov/glossary/term/encryption)
[4] Phishing is considered "A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person." (https://csrc.nist.gov/glossary/term/phishing)

- Never click on a file/link/site that you do not know the nature of.
- Never act in a physical environment before making sure it is safe (be cautious of cameras / skimmers/ etc.).

Identity Theft Protection – Silver Rules

- Use strong passwords (combinations of numbers, letters, characters).
- Use at minimum 2-factor authentication.
- Never respond to emails from an unknown source.
- Always use a virtual private network to connect to the internet when in a public place.
- Always set up a reliable backup system.
- Always disconnect devices from the internet when they are idle.

As engineers, we design the electronic systems, write the software, integrate various electronic systems to an information technology system which stores, processes, or transmits data. These systems are used in critical industries such as power generation, aerospace, mining and oil, and financial services to name a few.

Poorly written software or errors in configuring systems can allow an attacker to exploit such vulnerabilities and compromise systems. Inadequate documentation can lead to improper implementation or use of the system. This can lead to loss of life, massive destruction of property, massive ecological damage, significant financial loss, and endangerment of national security.

Data governance and especially information classification is the foundation for ensuring that systems are designed with the appropriate controls in place. By classifying data within a system based on defined levels of confidentiality, integrity and availability, systems and software engineers understand the security expectations and design accordingly. For example, the information within a public web site that publishes boilerplate advisories would likely be classified as low confidentiality, high integrity, and high availability. By understanding the security expectations, this system can be designed and the proper security controls can be implemented. The system engineers would likely ensure that the system is highly redundant to maintain high availability. The software engineers would likely implement strict input validation controls to minimize input errors into the system. Since the information is publicly accessible, controls to protect the confidentiality of boilerplate advisories would not be considered.

Before designing any information system, classification of the information within the system must be completed to ensure that appropriate security controls are designed into the system as opposed to be implemented as an afterthought.

Works Cited

Canadian Centre for Cybersecurity. (2018). Harmonized TRA Methodology (TRA-1). *Canadian Centre for Cybersecurity.* https://cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1

Cybersecurity & Infrastructure Security Agency (CISA). (2019). What is cybersecurity?. *CISA.* https://www.cisa.gov/uscert/ncas/tips/ST04-001

Vaughan, J. (2020). What is data governance and why does it matter?. *TechTarget.* https://searchdatamanagement.techtarget.com/definition/data-governance