Legal Awareness and Cyber Protection

Legal Awareness

The legal system on information systems and technology develops daily as technology grows. These developments can have meaningful effects on organizations such as the following:

- **Security Expectation**: Clients and partners expect extensive security to protect their data.
- **Organization Expectation:** They expect organizations to adhere to lawful paths in achieving commercial goals.
- **Damages:** If organizations miss a new legal ruling, it could hurt the organization, its brand, and everyone involved.

Legal Issues

Here are four (4) legal issues that organizations with information systems and technology should be aware of:

1. **Net Neutrality**

It is the notion that equally treats all content flowing through the cables and towers of internet service providers (ISP). It requires ISPs to not slide additional data into "*fast lanes*" that block or discriminate against the contents of other ISP.

No law, rule, or regulation in the Philippines limits or promotes net neutrality. With this, ISPs can purposely increase or decrease the bandwidth allocation depending on their customers' pricing. It affects any small- or medium-sized company that relies on the internet.

For example, telecommunications companies like Smart and Globe provide add-on packages for their users in their services, such as free YouTube access and free Facebook data. Although it does appear a good deal for users, in hindsight, these companies forcefully influence their users to use services from other companies agreed upon over money.

2. **Data Protection**

Most of the public wants their online data and information to be private and secure. Working with the personal information of partners, clients or stakeholders requires covering the bases and confirming the structural soundness of the network, prevention of cybersecurity breaches, and transparency with them.

For instance, in the United States, Facebook was criticized for leaking users' data to consulting firm Cambridge Analytica during the 2016 Presidential Election. It poses a personal information breach and other potential legal repercussions. This cybersecurity failure adversely affects businesses, the economy, and the country.

It is encouraged to be truthful and transparent in handling personal data by giving precise and timely reports and updates.

3. **IP Theft**

Intellectual property (IP) theft is stealing data from a company. IP involves ideas, design, artistic works, images, videos, symbols, and names that are assets to a company.

IP theft covers patent trolling, trademark infringement, software pirating, and counterfeit production that is widespread across the globe.

Specifically, patent trolling deals when a massive company purchases patents in the market instead of creating their own for their products and services. For example, Apple lost a legal battle regarding patent trolling for infringing the patent licensing of VirnetX Holding Corp.'s internet security technology for Apple's FaceTime features. Apple is ordered to pay a settlement of more than $500 million.

To prevent facing and becoming a victim of IP theft, establish stricter security policies and procedures to protect valuable data. This includes educating the employees, monitoring their activity, and finding the company's cybersecurity lapses and weak spots.

4. **Non-Compete Laws**

With frequent transitions and resignations, non-compete clauses have become a legal challenge for some. These are signed agreements between employees and employers that prohibit the employee from going to a rival company after resignation.

The tech industry opposes non-competes clauses as it stifles innovations and hinders startup activities. On the other hand, others argue that it protects their business interests and trade secrets. But it all depends on how the company views its assets and the lengths it would take to protect them from being ripped off or stolen.

Pointers to Avoid Legal Problems

To further understand and be fully legally aware, here are some pointers to avoid legal problems:

Communication

Expectations should be communicated, and timeframes should be identified as the scope of work changes from time to time, affecting the timeline previously stated.

As soon as issues arise, notify the other party about the events and what solutions are in place. It is also essential to document these expectations and time frames, as one of the most important things about communication is the documentation to back-up future claims.

If a matter is significant, a contract should be prepared, while a simple form for routine issues is enough. Though at a minimum, email communications and confirmations should be noted.

Picking the Right Battles

If failures happen, own them. It is much cheaper to apologize than to be served to the court.

Do not try to cover errors or problems by glossing over them, as a situation is almost always worse than the problem itself. It always leads to legal problems and trust issues, as the nature of a business relationship is based on trust.

Source of Legal Advice

Just because certain legal advice works for a similar situation, it does not guarantee that the exact advice will work on another alike. If legal matters arise, it is a must to involve qualified and trusted legal counsel.

Sourcing through the internet for legal opinions is acceptable, but there is nothing more valid than advice from a qualified and experienced lawyer.

Following Through

Timely performance regarding expectations is another way to avoid legal problems. It is essential when dealing with employees. If an employee handbook is available, follow it for proper procedures and policies in dealing with issues.

It is also important to follow through or perform by the expectations when working with another party or client, as it will effectively minimize legal tendencies. Always possess proof of performance that can be a type of receipt, acknowledgment, or even a simple email.

Cyber Protection

Cyber Protection

It combines the benefits of data protection and cyber security needed for business operations in the current cyber threat landscape.

As data and information become the core of all business operations, effective cyber protection is necessary to safeguard organizations, people, and society.

Cyber Protection vs. Cybersecurity

Cyber protection and cybersecurity differ in their relationship to data and information. Cybersecurity safeguards the systems that make data access, storage, transfer, and authentication possible instead of mainly focusing on data protection.

It is still an essential part of staying protected online, but it does not fully support the challenges that data and information protection are at risk. Therefore, cyber protection is formed by integrating cybersecurity with data protection to address new forms of malicious cyber-attacks fully.

Scopes of Cyber Protection

Here are the scopes of cyber protection that address the needs of modern cyber threats.

1. **Safety**: This deals with ensuring that a reliable copy of the data and information is always available. It will be a backup whenever the original copy gets corrupted or compromised due to cyber-attacks. Time would not be wasted restoring and recovering the data if a reliable copy is available.

2. **Accessibility**: This deals with ensuring that data and information are available from any location at any time. Storing valuable data and information to various mediums ensures safety and accessibility whenever a copy gets corrupter or compromised.

   It is ideal to put copies on various physical devices and cloud storage for faster accessibility.

3. **Privacy**: This deals with ensuring full control and transparency over who can view and access the data and information. As data and information get easily replicated, monitoring the people who can access and view the files is vital to prevent an insider attack.

   Only grant access to trusted people, especially those who directly use the data and information.

4. **Authenticity**: It deals with ensuring that backed-up data and information is an exact and unmodified copy of the original data. Doing this avoids the risk of forwarding or disseminating wrong information through different networks that could jeopardize the whole operation.

   Practice putting multi-factor authentication on files or encrypting data that only trusted people can access to prevent modifications.

5. **Security:** It deals with ensuring that data, information, apps, and systems are protected against cyber threats. It all comes down to security regarding ensuring the safety of confidential files, so it is best to monitor wherever or whomever the data is passed along.

   Another form of security is installing antivirus software to prevent cyber-attacks and malware from affecting the files and the whole system.

References:

Acronis (2020). *What is cyber protection?* [Web Article]. Retrieved on July 21, 2022, from https://www.acronis.com/en-us/blog/posts/what-is-cyber-protection/

Ekran (2021). *7 best practices to prevent intellectual property theft.* [Web Article]. Retrieved on July 21, 2022, from https://www.ekransystem.com/en/blog/best-practices-to-prevent-intellectual-property-theft

Kreamer Law Firm (2022). *5 tips to avoid legal problems.* [Web Article]. Retrieved on July 21, 2022, from https://www.kreamerlaw.com/5-tips-to-avoid-legal-problems/

Tulane University (2022). *4 IT legal issues you need to pay attention to now.* [Web Article]. Retrieved on July 21, 2022, from https://sopa.tulane.edu/blog/it-legal-issues-need-attention