precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 16 December 2022

Good Security Policy Practices in the businesses

TODAY WE ARE FOCUSING ON THE IMPORTANCE OF SOME GOOD SECURITY POLICIES THAT BUSINESSES NEED TO EMPLOY.

Dr. Ronald Walcott
Managing Director

In all organizations, there are some rules and standards that govern the operation of the organization. These rules are known as policies. These policies dictate how everything is done and maintain an overall order so that they can operate with maximum efficiency and to protect themselves and their customers/clients. Today we are going to look at some of the reasons why good security policies are important for businesses to employ as well as what some of these policies are.

IMPORTANCE FOR GOOD SECURITY POLICIES

Good security policies are important because they provide protection for an organization's physical and digital assets and the threats to those assets.

Physical Security Policies

There are many different physical security policies that businesses put in place to protect their physical assets. These assets include IT equipment, servers, computers, hardware peripherals, tablets, phones, etc. Protecting physical assets is particularly important because they contain sensitive information and company data. If these physical assets are compromised, it can be speculated or assumed that it is likely that the data on these physical asset devices have also been compromised and at risk. With this in mind, information security policies are dependent on physical security policies to operate as an extra layer of security to keep company data safe and secure.

Some physical security policies include:

- Restricted access to buildings, rooms and other areas within the organization.
- Restricted access to who can access physical assets.
- Security verification systems such as biometrics.

INFORMATION SECURITY POLICIES

Just like physical policies, organizations put these policies in place to protect their digital assets. These assets include PII (Personally Identifiable Information), credit card in-

In this Issue:

formation, client information, accounting information, etc.

Protecting digital assets is very important and also very difficult to significantly reduce the chances of being the victim of a cyber-attack. The Information Security Policies offers some advantages to the organization. Some of these include:

- **Protecting Valuable Assets:** Policies enforce the CIA triad, confidentiality, integrity, and availability, to protect customer data and personally identifiable information.
- **Guards the organization's reputation:** Data breaches and other information security incidents can negatively impact and affect an organization's reputation. Customers trust organizations with their confidential information, therefore, if their information is compromised then their trust in the organization would be broken.
- **Dictates how data within the organization is treated:** Security policies provide guidance on the procedures required to protect data and intellectual property. In some cases, vulnerabilities come from organizations that may have differing security standards. The security policies in place help identify potential threats and security gaps.
- Ensures compliance with legal requirements: There are legal requirements that are aimed at security sensitive information, for example, Payment card data security standard. These requirements guide companies on how to make policies to enforce good information security practices.

KEY ELEMENTS IN A SECURITY POLICY

- Statement of purpose: - Defines the overall goal of the policy.
- Definition of the policy: - Defines what the policy is about.
- Objectives of the policy: - Breaks down the purpose of the policy into subparts that the policy must achieve.
- Statement of responsibility and duties: - A clear description of employee duties and who will be responsible for overseeing and enforcing the policy.

Frequently Asked Questions:

WHAT TO CONSIDER WHEN DEVELOPING POLICIES?

Security professionals must consider a range of areas when creating policy. Does it align with international standards? How is the data being distributed? How is data being categorized?

IS IT IMPORTANT TO UPDATE POLICY OFTEN?

An organization's IT environment and vulnerabilities change as it grows. Security policies must also evolve to reflect the changes and secure the organization against cyberthreats.

Upcoming Events

CYBERTECH GLOBAL:
January 30, 2023
Tel Aviv, Israel.

ZERO TRUST WORLD:
February 1, 2023
Orlando, US.

IOTSSA CYBERSECURITY CONFERENCE:
February 16, 2023
Arizona, US.

Headline News

Government Sets Out New Rules to Enhance App Security

The UK government has thrown down the gauntlet to app store operators and developers, requesting they sign up to a voluntary code of conduct designed to enhance user security and privacy.

In what it described as a "world-first" today, the Department for Digital, Culture, Media and Sport (DCMS) said the rules would help to reduce consumers' exposure to malicious and bug-ridden apps.

The code will stipulate that app store operators and/or developers:

- Share security and privacy information in a user-friendly way with consumers, such as where user data is stored and when the app was last updated
- Allow their apps to work even if a user chooses to disable optional functionality and permissions, such as location tracking
- Have a "robust and transparent" vetting process to ensure only apps that meet a minimum security and privacy baseline are published
- Provide clear feedback to developers when an app is not published on their store for security or privacy reasons
- Have a vulnerability disclosure process, such as a contact form
- Ensure developers keep their apps up to date to reduce the number of vulnerabilities

The government acknowledged that many app store operators and developers already adhere to many of these rules. However, it will also look at where current laws may need to be tweaked and/or where regulation is needed to improve security in the industry.

Over the coming nine months, the DCMS will work with companies such as Apple, Google, Amazon, Huawei, Microsoft, LG, Epic Games, Nintendo, Valve, Sony and Samsung to help them implement the code.

"Apps bring a lot of convenience to our everyday lives, but rogue apps making their way onto the biggest app stores are a security and privacy minefield – putting consumers at huge risk from data theft and scams," argued Which? director of policy and advocacy, Rocio Concha.

"The government's announcement of a new voluntary code is a positive step towards making apps more secure. The app market must now be monitored closely for improvements and to check whether tech firms are falling short in protecting consumers."

Although designed for consumers, the new rules could also enhance corporate security by ensuring BYOD devices are better insulated from app-based risks. However, threats may persist from some third-party app stores hosted outside the UK.

Source: www.infosecurity-magazine.com