Author - Ariel Guerrero @aes604

Principles of Cyber Security

Small Business Cyber Security Model

Model Background

The **Information Technology Laboratory** at the National Institute of Standards and Technology promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. [1] Information Technology Laboratory develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. Information Technology Laboratory's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. ***This Security framework is based on NISTIR 7621 revision 1*** published by The Information Technology Laboratory, with the purpose of serving a concise yet robust and easy to understand security model for small business who may not have the expertise or understanding to answer many of the items found in detailed checklists, may not have a lot of time to dedicate to the process, or may not have the funding to bring in a 3rd party to conduct the audit.

Information Security

What is Information Security and Cybersecurity?

All businesses use information. If that information is compromised in any way, the business may not be able to function. Protecting the information an organization creates, uses, or stores is called "Information Security."

Key Components of Business Information Security

- Physical Security – the protection of property
  - fences
  - locks
- Personnel Security
  - Background checks
- Contingency Planning and Disaster Recovery – how to resume normal operations after an incident, also known as Business Continuity Planning
- Operational Security – protecting business plans and processes
- Privacy – protecting personal information.

Elements of Risk

- Environmental
  - fire

    - floods
    - tornados
    - earthquakes
- Business Resources
    - equipment failure
    - supply chain disruption
    - employees
- Hostile Actors
    - hackers
    - criminals

Managing Your Risks

Organizations must exercise ***due diligence*** in managing information and privacy risk. Employing effective risk-based processes, procedures, methods, and technologies ensures that information systems and organizations have the necessary trustworthiness to support business functions.

- Identify what information your business stores and uses

    - It is unreasonable to protect every piece of information against all threats so it is important to identify only the most valuable information

- Determine the value of your information and after identifying each information type, ask these three key questions:

    - What would happen to my business if this information was made public?
    - What would happen to my business if this information was incorrect?
    - What would happen to my business if I/my customers couldn’t access this information?

    Note that it may be easier to assign information to a scale when dealing with a large amount of information. i.e.

    - 0 to 3
    - “none,” “low,” “moderate,” and “high.”

Safeguard your information

- Identify and control who has access to your business information

    - Do not allow unauthorized persons to have access to any business hardware
    - Be aware of anyone who has access to computers
    - Physically lock up business electronics when not in use
        - Laptops
        - Mobile Phones
        - other mobile electronic devices

- Conduct Background Checks

    - Make sure the person you may employ does not have a history of

- Require individual user accounts for each employee.

    - Require strong unique passwords

    - Without individual accounts it will be harder to investigate data loss or manipulation

- Create policies and procedures for information security

    - Outline acceptable practices
    - Clearly define your expectations
    - All employees should sign a statement of agreement
    - Review policies annually and as changes to the company and technologies used occur

- Limit employee access to data and information

    - Only allow employees to access what they need
    - Prevent non-privileged users from executing privileged functions.

- ***Train your employees***

    - According to the cybersecurity education company, Cybint, 95% of breaches are caused by human error.
    - What Topics Should My Security Awareness Efforts Focus On?

        - **Phishing Attacks and Social Engineering**

          Phishing is a hacking practice to fool employees into turning over private data and system access credentials. Generally, phishing comes in emails modified to appear as if they came from people in the organization. 43% of cyber attacks target small business, 62% of which experienced phishing & social engineering attacks.

            - Employees must identify false messaging and understand how to report them to IT.
            - Human intelligence and comprehension is the best defense against phishing attacks.

        - **Passwords**

          One of the weakest points of an IT system is the authentication system, mostly due to the fact that many users will disregard best practices. Training in this scenario should include creating and maintaining a strong secure password and how to use different passwords for each account the employee may posses.

        - **Remote Work Tools and Practices**

          Remote work is more common, and interactions with outside forces can threaten the security of a professional network. Employees should have information and other resources on how to manage their devices and connect to business networks.

    - Continually reinforce the training in everyday conversations or meetings

- Patch your operating systems and applications

    - Only install what is needed to run your business
    - When a new device is purchased check for updates right away
    - Assign a day to check for updates.

        - Monthly or every two weeks depending on circumstances.

- Install and activate software and hardware firewalls on all your business networks
    - Firewalls are used to block malicious communications or browsing of inappropriate websites
    - Confirm there is antivirus software installed on the firewall.
    - regularly update a software firewall on each computer system
    - Enable logging
        - Useful in investigation of an event by providing evidence

- Secure your wireless access point and networks
    - Change the administrative password that was on the device when you received it.
    - Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID).
    - Set your router to use WiFi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption. Do not use WEP (Wired-Equivalent Privacy) as it is not considered secure.
    - **If your business provides wireless internet access to customers, ensure that it is separated from your business network.**

- Set up web and email filters
    - Helps remove emails known to have malware attached
    - Prevents inbox from being cluttered by unsolicited and undesired emails.
        - i.e. spam
    - If available enable web filtering

- Encrypt sensitive business information

  Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative where only authorized parties can decipher a the encrypted plaintext back and access the original information.

    - Use full disk encryption
        - Encrypts all information on the storage media

  Why use full disk encryption?

  When every drive on the system has full disk encryption enabled, your security is stronger. A stolen laptop is no longer an existential security threat. The data simply won’t be accessible to the thief without another form of attack.

- Install and update anti-virus, -spyware, and other –malware programs

- Maintain and monitor logs

- Make full backups of important business data
    - Make a full, encrypted backup of the data on each device used in your system at least once a month
    - Backups will let you restore your data in case a computer breaks, an employee makes a mistake, or a malicious program infects your system.

    - Data that you should backup includes, but is not limited to, spreadsheets, databases, financial records, human resources files, customer accounts account information and system logs.

References

- Small Business Information Security, Paulsen and Toth. (NISTIR 7621 REV. 1)
    - https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- Security and privacy control for information systems and organizations (NIST SP 800-53, REV. 5)
    - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- Reasons to require full disk encryption
    - https://jumpcloud.com/blog/reasons-require-full-disk-encryption
- SOC2 Type 1 and 2 Audits
    - https://socreports.com/soc-2-services/soc-2-audits
- 15 Alarming Cyber Security Facts and Stats
    - https://www.cybintsolutions.com/cyber-security-facts-stats/
- Employee Security Awareness Training: Why it's important
    - https://www.cisostreet.com/employee-security-awareness-training-why-its-important/