INFORMATION SECURITY

Keeping Up with Cyber-Threats

INDEX

Abstract

In the world of information and technology, many businesses are confronted with multi-faceted problems in leveraging the value of IT usage and implementation.

The most common problem is properly securing their business information against growing security threats.

This white paper has covered some of the security threats, vulnerabilities, mitigation techniques and services.

Half of midsize and large organizations will add bigger, more advanced inspection-oriented features to their network firewalls by 2019, according to Gartner, Inc.

Introduction

Today, organizations depend heavily on computers to store sensitive business and customer information and the need for the proper information security system is becoming imperative to address emerging threats.

If proper security management is not followed and information is stored electronically and is accessible on networked computers, intruders can delete, steal, change, or misuse information, and they can hide evidence of their unauthorized activity.

Information Security is as inevitable as the technology that is being used as a medium for data storage, communication, and processing.

What is Information Security?

Information Security means protecting an organization's data from unauthorized access or modification to ensure its:

Integrity: means securing against improper information modification or destruction, and it also covers ensuring information nonrepudiation and authenticity.

Confidentiality: means protecting personal privacy and proprietary information.

Availability: means ensuring timely and reliable access to information.

The proper information security helps deliver information values such as accuracy, reliability, rapidity, timeliness, privacy and relevancy. Information security has managed to get a huge amount of attention from different industries in the past few years.

People think about security in different ways and some of the most common understandings are, security is all about keeping the Hackers and Cyber-Thieves out of their systems, elimination of all threats, and management of risk.

Annual expenditures on security products and services are growing year by year. But still, many security incidents are taking place, and those incidents are becoming quite expensive.

As more and more companies are relying on computers to store sensitive corporate and customer information, the role of information security is becoming very vital.

Valuing and protecting information are the important tasks for a modern organization.

Many companies have been looking for appropriate techniques to handle and solve issues in the discipline of information security management.

Making continuous improvements to information security will help ensure sustained business success and continuity, and minimize the impact of information security breaches.

It is paramount to think about information security because much of the value of a business lies in the information.

Why Information Security Is Necessary?

Information security is the protection of information and systems from a wide range of threats. Businesses use an extensive amount of information every day from computers and networks. Information is arranged in a way that it can be retrieved easily from the resources.

Computer systems and mobile devices access and tackle different information resources easily. Information security is crucial to all organizations, as years of sensitive data can be lost or destroyed in the absence of security, backup and recovery plan.

Data security is a primary concern of any organization.

As technology continues to develop at a rapid pace, organizations feel the pressure to become as up-to-date as possible. One of the common concerns many companies have is keeping their data secure as technology grows with new capabilities.

The organizations have the responsibility to ensure the safety and soundness of their information, be it their comprehensive business information or customer information. Taking some security measures like installing and updating anti-virus software to local desktops and servers, backing-up key files and storing them in a secure offsite location, can help in avoiding loss of data.

The technological advancements and internet quickly becoming a medium for cost-effective and efficient medium to share information among consumers, and businesses.

But, many businesses overlook proper security measures due to lack of awareness about the importance of security, which results in vulnerabilities in their software and network devices.

With increase in the vulnerabilities, it is becoming easier for cyber criminals penetrate information systems. The unauthorized access and the exploitation of vulnerabilities will occur due to weak or non-existent information security practices and not identifying and mitigating risks as early as possible.

The cost to protect against information threats will increase as the number of threats and vulnerabilities also increase. However, the cost of a security breach to an organization can be much higher than the cost of security implementation. Many organizations are still slow to adopt proper information security practices to protect business and customer information.

Information is the most important asset of an organization. Therefore, objective of security is to build protection against the enemies of those who would do intentional and unwarranted actions that lead to adverse consequences.

Selecting the proper information security methods will help protect the data that an organization collects and uses on a regular basis. An unprotected information can be accessed by anyone and if it falls into the wrong hands, it can destroy a business.

Managing Director, the Information Security Forum (ISF), Steve Durbin says, "Unfortunately, while organizations are developing new security mechanisms, cybercriminals are cultivating new techniques to evade them.

In the drive to become more cyber resilient, organizations need to extend their risk management focus from pure information confidentiality, integrity and availability to including risks such as those to reputation and customer channels, and recognize the unintended consequences from activity in cyberspace.

By preparing for the unknown, organizations will have the flexibility to withstand unexpected, high impact security events."

Types of Threats

The information security threat factor is constantly evolving. There are many information security threats that businesses need to protect against to make sure the crucial information remains secure.

There are several various internal and external threats to information. Below are some of the common threats to most information systems:

- **Unauthorized Access:** The successful access to information or systems without any permission
- **Cyber Espionage:** Gaining illicit access to confidential information
- **Malware:** Injecting malware to damage a computer system
- **Data Leakage:** An unauthorized transfer of key information
- **Social Engineering:** Deceiving and Manipulating others by phone, email, online or in-person, to access company information or systems
- **Insiders:** An employee committing fraud or causing damage to company systems or information by stealing sensitive company information
- **Phishing:** Emails containing unasked requests for sensitive information from unknown senders
- **Spam:** Unasked email sent in bulk to many people for spreading malware
- **Denial of Service:** An attack on a system, making it unavailable and inaccessible to authorized users
- **Identity Theft:** Stealing unknown individual's personal information to commit a crime for financial gain

Vulnerabilities That Can Be Attacked

Simply put, vulnerability means susceptibility to attack.

A vulnerability is a weakness which enables an attacker to reduce a system's information assurance.

'Many vulnerabilities are directly related to the technology advancements.

If the unauthorized users get an access to the website, they may modify, steal or put any information to produce negative public opinion.

Attacks that result in blockage of internal and external communications, or may domain name get blacklisted.

Below are some of the vulnerabilities that can be attacked for the wrong reasons.

- ☑ Installing unauthorized software and apps
- ☑ Opening spam emails
- ☑ Connecting personal devices to company networks
- ☑ Writing down passwords and sensitive data
- ☑ Lack of information security awareness
- ☑ Misconfiguration of hardware
- ☑ Software bugs and design faults
- ☑ Software complexity
- ☑ Open physical connections, IPs and ports
- ☑ Insecure network architecture
- ☑ Excessive privileges
- ☑ Configuration errors and missed security notices
- ☑ System operation errors
- ☑ Customers access to secure areas
- ☑ Complicated user interface

- ☑ Default passwords not changed
- ☑ Inadequate network management
- ☑ Inadequate or irregular backup
- ☑ Inadequate physical protection
- ☑ Inadequate replacement of older equipment
- ☑ Uncontrolled download from the internet
- ☑ Uncontrolled use of information systems

Once vulnerabilities are identified, the necessary remedial actions to be taken to fix these vulnerabilities to reduce the impact of threats.

Vulnerabilities emerging from flaws may need system reengineering or design efforts to fix the deficiencies.

Vulnerability scanning on a system is used to identify the security weaknesses in it and alert system administrators about these.

The organizations need to ensure information security by performing an security assessment on a routine basis.

The organizations must follow security diagnostics such as security audits, vulnerability scanning and penetration testing.

Threat Mitigation Techniques

There are many threat-mitigation techniques available that businesses can use to better secure their information. Cyber-attacks have become a very common threat to businesses in the last few years, showing devastating effect on the service delivery and recovery.

Keeping critical IT assets safe from cyber criminals is not easy, but it can be done. Cybercriminals continuously develop their techniques to penetrate systems and use data for destructive purposes. The organizations need to find a multifaceted approach to reduce risk. With cybercriminals targeting large businesses, it can be reckoned that the personal information and small business information might be a very tiny project to target.

To avoid threats that deliver disastrous consequences for the business, businesses should find an approach that covers factors like Prevent, React, and Plan meaning backup, storage and recovery. Businesses can leverage network and software technologies that detect and block threats.

Firewalls, Proxy Servers, Spam Filters, Web Filtering and Isolated Demilitarized Zone (DMZ), Endpoint Protection System, Intrusion Prevention System, Intrusion Detection System, Traffic Monitoring Software, Privileged Access Management System, Encryption Software, Password Management Policy, and Data Leakage Protection System are some of the solutions that can be considered.

As cybercriminals advance, security professionals need to find additional technology to reduce company's risk.

They can install firewalls to allow or deny access to data. The organizations also need to have Anti-virus protection to avoid malware and worm access, that can spread across the entire system very fast if access is allowed inadvertently.

Also, businesses can follow some of the security measures such as:

- ☑ Giving limited access to system sensitive information
- ☑ Blacklisting all hosts and ports, white listing only those required
- ☑ Checking that no critical systems interface directly with the internet
- ☑ Before discarding a disk drive, erasing all information from it
- ☑ Configuring a backup system

Gartner says, the average selling price for firewalls was expected to increase by at least 2 or 3 percent year over year until the end of 2018.

Digital Forensics

Digital Forensics is said to be an investigation, recovery and analysis of data and finding evidence of malicious activities within digital devices such as computers, smartphones, etc.

Digital Forensics exposes the fraud. Digital forensics helps organizations identify unauthorized access by employees, identify intellectual property theft, identify information security breaches, identify fraud and recovery of deleted files and file carving.

Digital Forensics helps deal with a wide variety of crimes by giving good guys the ability to keep up with the bad guys. While Law enforcement is already using digital forensics, industries such as banking, IT and national defence sectors looking to leverage Digital Forensics capabilities.

The utilization of this technology is growing because of the immense increase in the use of electronic devices. In the society, interaction with electronic devices is inevitable.

Here is an example of a typical digital forensics investigation: A company suspects an ex-employee of stealing data of the company.

A digital forensic investigator will be called for the recovery, analysis and presentation of data found on computers.

The investigator will make a duplicate copy of the computer's hard drive without altering it.

Then, the investigator will use some tools to properly investigate the duplicate copy to identify an electronic evidence and create a report based on the findings.

In the process, the investigator will document Chain of Custody (CoC) that features all items of evidence.

An investigator can find the digtial evidences such as Metadata, Website data, Deleted files, Regular files that include photos, Word documents, e-mails, videos, and even software.

To keep up with the rapidly-changing digital world, the right expertise in digital forensics investigation would help address day to day emerging digital challenges and ward off cybercriminals.

Artificial Intelligence in Security

Artificial Intelligence (AI) has a multitude of capabilities. It can anticipate issues before they occur through threat analysis, threat detection and threat modelling.

The security field stands to benefit enormously from AI as it supports humans in fighting cybercrime. Security threats and vulnerabilities are a big concern for many individuals and organizations.

Computer scientists have come up with artificial intelligence that have the ability of determining malicious codes in software.

AI enables the “development of algorithms designed to identify security threats in real time and provide a quick response.” AI can also simplify the identification, processing and response to security threats.

The use of AI in security systems helps produce a calculated approach to security for accurate results.

At the same time, AI can undertake multiple tasks such as monitoring, securing devices and systems.

Hence, it can significantly reduce large scale attacks, whereas legacy cyber security systems can’t.

It is difficult for the IT Security personnel to quickly detect a cyber hack. It is difficult to identify suspicious activity from an external source and then determine it as a cyber breach as there are many things involved.

AI-based information security can help IT security personnel save time, and accurately report a computer system hack. AI capabilities will play a key role in the security sector, if IT Security personnel use it as a tool to detect potential cybercrime activity.

The use of artificial intelligence in security systems provides more flexibility, particularly with new security threats always rising. Additionally, machine learning concepts have earned attention for their involvement and improvement of security systems.

Machine learning is a type of AI that enables a computer to learn, grow, and change when presented with new data.

Applying machine learning algorithms to security will improve detection and expose new or unknown threats as the algorithms can be fed all information about current malware so that it can learn to find a similar behavior in new or unknown malware.

Conclusion

The information security is all-important, since many companies depend on information, technology and systems. They need to secure their corporate and customer information against any sudden theft or misuse to sustain in the competitive business world.

However, many companies today still do not take proper precautions on information security. Therefore, many companies are under a serious threat.

Approaching a comprehensive and reliable security service provider will help in avoiding the loss of crucial business information.

info@veritis.com

1-877-VERITIS (283-7484)

972-753-0033

US Corporate Headquarters

1231 Greenway Drive

Suite 1040

Irving, TX 75038

India Headquarters

#607, 6th Floor,

Ashoka Bhoopal Chambers,

S P Road, Begumpet

Hyderabad – 500003, India.

Phone no: 040 42211730

For more information, contact info@veritis.com

www.veritis.com