ST. KITTS BRANCH
Financial Services Regulatory Commission

NewsLetter

June 2022
Issue No. 99

Modern society is characterized by the routine use of computers, communication networks, mobile communication devices and other Information Technology (IT) equipment. Government institutions as well as banking, utilities, transportation and other systems can no longer properly function without the reliable and sometimes, flawless operations of computer and communication equipment. IT is not just used by persons in their everyday occupations but is integrally engrained in almost every aspect of human life. At the same, the IT environment has unfortunately become instrumental in the playground for crime. Criminals no longer need to have physical contact with their intended targets. All they require is a computer or other IT equipment and access to the information to carry out their illicit activities. It is therefore important to employ robust **CYBERSECURITY** measures to mitigate and protect against these IT threats.

Cybersecurity Defined

Cybersecurity involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit. Additionally, Cybersecurity includes implementing mechanisms to mitigate instances of the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. Effective Cybersecurity practices promote the safekeeping of data, computer systems and networks.

Importance of Cybersecurity

Cybersecurity is SAFETY. Organizations should protect computers and data in the same way that doors and windows are secured in homes. Employees and key personnel should behave in ways that protect the organization against risks and threats that emanate from the use of technology. Risks posed by poor implementation of Cybersecurity knowledge and practices include the following:

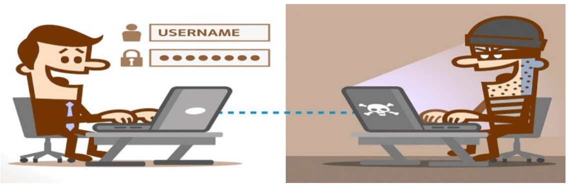
- Identify Theft;
- Monetary Theft;
- Legal Ramifications; and
- Sanctions/ Business Closure .

Leading Threats to Cybersecurity

Threats refer to any circumstances or events that can potentially harm an organization's information system by destroying it, disclosing sensitive information stored on the system, adversely modifying data or making the system unavailable to users.

Cybercrime acts are most times relatively easy to commit since computer equipment is continuously becoming cheaper and accessible. Uniquely, cybercrime can be committed from any place around the world while targets may be located thousands of miles away. It can also be difficult for investigators to identify and seize relevant information to be used as evidence for prosecution.

The leading threats to cybersecurity include the following: Viruses, Worms, Trojan Horses/Logic Bombs, Social Engineering, Rootkits, Botnets/Zombies. These would be discussed on the following page.



Cybercrime and Money Laundering

The “traditional' money laundering methods usually rely on the banking system however, money laundering in the cyber-realm depends mainly on the use of various types of cash transactions and financial services providers ranging from wire transfers, cash deposits/withdrawals and e-money transactions. Illicit funds may be integrated into the financial sector using electronic cash conversions making the task of identifying and tracing the illegal funds by law enforcement extremely challenging. The majority of organizers and perpetrators of cybercrime related schemes tend to be well educated and technically savvy. This translates into quite complex and unconventional money laundering mechanisms. These include the purchase of electronic money and use of e-wallets, the use of international payment systems and using remote access to conduct financial transactions via multiple bank accounts.

In this Issue

LEADING THREATS TO CYBERSECURITY

Virus: A virus is a malicious software that attaches itself to a program, file or disk. Viruses can disrupt systems, cause operational issues and result in data loss and leakage.

Here are signs which may help to identify computer viruses:

The time taken to open applications becomes longer and the entire system may work slowly.

One may start getting too many pop-up windows on his/her screen.

If the virus spreads to files and programs, the entire device may crash.

Social Engineering: This is where individuals are manipulated into performing actions or divulging confidential information. It involves the use of deception to gain information, commit fraud or access computer systems.

Phone Call: This is John, the System Administrator. What is your password?

Email: ABC Bank has noticed a problem with your account…

I have come to repair your machine…

Worm: A worm is an independent program that replicates itself and sends copies from computer to computer across network connections. Once a worm breaches a computer's defenses, it can perform several malicious functions such as steal data, delete files, overload networks and deplete hard drive space.

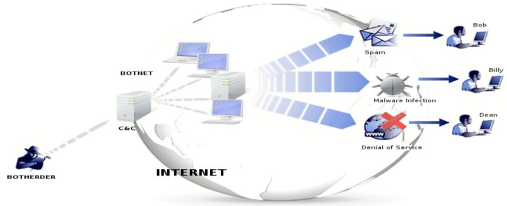
Rootkits: Upon penetrating a computer, a hacker can install a collection of programs called a rootkit. Rootkits enable easy access for the hacker (and others) into the enterprise to spy and access information as they see fit. They also eliminate or hide evidence of the "break-in".

Trojan Horses/Logic Bombs

A **trojan horse** masquerades as a harmless program while quietly destroying data and damaging the system. For example: a game may be downloaded which is very fun but contains a hidden code that gathers personal information without the users' knowledge.

A **logic bomb** is executed upon certain conditions. This includes a software that malfunctions if a fee is not paid or a database erase is triggered if an employee is fired.

Botnets/Zombies: A botnet is a number of compromised computers used to create and send spam or viruses or flood a network with messages as a denial of service attack. The compromised computers are called zombies.



Identifying Cybersecurity Breaches

The following Red Flags may be indicators of Cybersecurity Breaches:

- √ Antivirus Software detects a problem;
- √ Pop-ups suddenly appear;
- √ Files or transactions appear that should not be there;
- √ The computer slows down to a crawl;
- √ Unusual messages or sounds on your monitor;
- √ The mouse pointer moves by itself; and
- √ The computer spontaneously shuts down or reboots.

REPORT A CRIME

Cyber Incident Reporting

If a cybersecurity incident or breach is suspected, immediately notify the organization's Help Desk or IT Department. Be prepared to give details and information about the breach. All organizations should have a Cybersecurity Plan with policies and procedures to identify, respond to and mitigate cyber security incidents.

1. Do not attempt to investigate or remediate the incident without the assistance of IT.
2. Inform other users on the system and instruct them to stop work immediately.

Best Practices for Effective Cybersecurity

The best way to avoid Cybersecurity threats is to use multiple layers of defense to address technical, personnel and operational issues.

1) Install and maintain anti-virus and anti-spyware software;
2) Install a firewall which helps to prevent many hackers from connecting to computers. They act as a barrier between the network and the internet;
3) Ensure that patches and updates are regularly applied to the system software. Failure to do so leaves the system vulnerable to hackers;
4) Encourage employees to make passwords easy to remember but difficult to guess. They should be at least ten (10) characters and include numbers and symbols;
5) Train employees to surf the internet safely. Avoid opening emails from unknown senders and strange links.; and
6) Be sure to have an effective system to back up information.

References

- 2014 Cyber Crime and Money Laundering Eurasian Group on Combatting Money Laundering
- Cybersecurity Primer: Information Security Awareness: University System of Georgia