ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-198

(Approved and Registered with Govt. of India)

CYBER WARFARE : A GLOBAL THREAT AND KEY FINANCIAL RISK

Suman

Assistant Professor

Department of Hotel Management

BPS Women University, Khanpur Kalan

ABSTRACT

When it comes to creating cybersecurity resilience, the financial industry has particular problems. In addition to preventing web application assaults, bad bots, ransomware, and phishing attempts, financial institutions must also examine how to sustain uptime before, during, and after these sorts of breaches in order to offer uninterrupted service to consumers and preserve regulatory compliance. Terrorism is a problem in many nations, including India, where it is both domestic and external. Terrorism should not just be associated with the use of metal weapons, but also with cyberattacks. Weapons in cyber warfare can have a wide range of devastating consequences on the target. Typically, cyber weapons are designed to protect or attack a specific target. Some of these digital weapons may be found freely on the internet, while others are private or commercially available. Because non-military targets are likewise linked to military infrastructure, there is no distinction between military and civilian infrastructure when it comes to cyber warfare. Weakening the economy or destroying public infrastructure may have a far greater impact than nuclear weapons, hence it is critical to develop a strategy to make the world aware of what an adversary is capable of. Keeping a country safe, prosperous, and stable is a top priority for cyber warfare groups. If a disaster occurs, treatment should be provided to protect national security and aid in disaster recovery. A country's future military could now be determined by how well-trained and experienced its cyberwarfare units and cyber-forensic professionals are, rather than the strength of regular military formations. Strategic and economic infrastructure is already under attack from the enemy. Banking, insurance, and investment organisations are all prominent targets for hackers aiming to steal money or information, disrupt operations, destroy vital infrastructure, or compromise data in other ways. If you take into account both internal costs and external effects, financial services institutions top the pack when it comes to how much a company pays on average to combat cybercrime. It topped $28.3 million in 2015, which is much more than the six-year average of $19.4 million for FSIs. The increasing risk of cyberattacks and the potential impact on banks is a top concern for financial institutions and the government.

Keywords: Cyber Warfare, Cyber Warfare Training, Cyber Threats, Cyber Warfare Arsenal, Cyber Terrorists, Digital Weapons, Cyber Combat

1.0 INTRODUCTION

There is nothing wrong with a country's right to protect itself against any destructive force and to use whatever measures necessary to take down its adversaries.. Today's battlefield is increasingly dominated by cyberwarfare, which has an impact on both the growth of armies throughout the world and the advancement of weapon technology. Because of its great degree of adaptability and difficulty in detection, its usage should not be undervalued. Cost-effectiveness means any government could afford to train or recruit teams that could accomplish more than an entire army could. To win control over the battlefield or compel the opponent to flee, such teams might effectively shut down their command infrastructure or communication network. When traditional military tactics are digitised along with more sophisticated electronic gadgets, new dangers and vulnerabilities are created, allowing cyberwarfare units to cause more harm than they ever could before.

Threats to Banking and Financial Perspectives

1. Unencrypted Data

This is a very basic yet crucial part of good cyber security. All data stored on computers within your financial institution and online should be encrypted. Even if your data is stolen by hackers, it cannot be immediately used by them if it's encrypted – if left unencrypted, hackers can use the data right away, creating serious problems for your financial institution.

2. Malware

End user devices – such as computers and cell phones – that have been compromised by malware pose a risk to your bank's cyber security each time they connect with your network. Sensitive data passes through this connection and if the end user device has malware installed on it, without proper security, that malware could attack your bank's networks.

3. Third Party Services that Aren't Secure

Many banks and financial institutions employ third party services from other vendors in an effort to better serve their customers. However, if those third-party vendors don't have good cyber security measures in place, your bank could be the one that suffers. It's important to look into how you can protect from security threats imposed by third parties before you deploy their solutions.

4. Data That Has Been Manipulated

Sometimes hackers don't go in to steal data – they simply go in to change it. Unfortunately, this type of attack can be difficult to detect right away and can cause financial institutions to incur millions of dollars in damages, if not more. Because the altered data doesn't necessarily look any different than unaltered data on the surface, it can be challenging to identify what has and hasn't been altered if your bank has been attacked in this manner.

5. Spoofing

A newer type of cyber security threat is spoofing – where hackers will find a way to impersonate a banking website's URL with a website that looks and functions exactly the same. When a user enters his or her login information, that information is then stolen by hackers to be used later. Even more concerning is that new spoofing techniques do not use a slightly different but similar URL – they are able to target users who visited the correct URL.

As a bank or financial institution, it is absolutely imperative that you find ways to mitigate the threats to your cyber security while still being able to provide your customers with convenient, technologically advanced options. At SQN, we've partnered with cyber security industry leader Q6Cyber to help provide increased security against potential data breaches.

Computers, mobile phones, and other IP-enabled devices can be used to wage war over the internet in cyber warfare. It is part of information warfare, which entails gathering tactical information, distributing propaganda or disinformation to demoralise the adversary, and leveraging information to overload hostile systems, servers, and put regular life to a stop. Cyber vandalism, espionage, the destruction of essential services, and equipment failure are all examples of cyber war tactics. Using disruptive activities, or the threat of doing so, against computers and/or networks with the intent to harm or further social, ideological, religious, political, or similar objectives can be defined as "cyber terrorism" in the United States Military's Handbook 1.02 on Cyber Operations and Terrorism. Or to scare anybody in order to achieve these goals."

China has demonstrated the capacity to "Blind" US satellites by using lasers to destroy them in a recent anti-satellite weapon test. For the time being, China has launched a total of 15 rockets and 17 satellites into orbit. According to an article published in the venerable daily Guardian on November 20, 2008, this information was obtained. As the paper points out, China's cyberwarfare capabilities are now "so advanced that the United States may not be able to oppose or even detect" the operations.

There are more than 140 nations throughout the world that have developed defensive cyber weapons, but there is no unified doctrine and legal framework for reacting to cyber assaults and for utilising offensive cyber weapons against attackers and enemies

2.0 CYBER WARFARE ARSENAL

- Computer worms
- Software vulnerability exploitation
- Denial of service attacks
- Info-blockades
- Root kits
- Botnets
- Malicious code
- Keyloggers

- IP spoofing
- Logic bombs and missiles
- Sniffing
- Spamming
- Trap doors
- Trojan horses
- Video morphing
- Carder
- Viruses

3.0 STAGES IN CYBER WAR

A full-fledged cyber attack may involve three steps.

1. Breaking the transportation and control systems.
2. Breaking the financial systems (stock markets, financial organizations and banks)
3. Taking control of the nations' utilities.

As a result of a full-scale cyber attack on all important institutions, such as the parliament and the Rashtrapati Bhavan, there may be an emergency situation in all of them. Hacking into traffic signal systems has the potential to devastate roadways by increasing the frequency and severity of collisions and injuries. The consequences of a cyber-attack on the metro's computer systems might be catastrophic. In the event of a security breach at your bank or tax office, your PAN Account, wages, investments, assets, and even the automobiles you own might be accessed. Demat account hacking might cost you money.

Recovery may take days if a full-fledged attack takes down the servers of vital public utilities or transfers control of them to a competing party. A multi-city power outage was caused by a cyber attack on IT systems last year, according to the CIA's findings. As far as we know, electrical grids outside the United States have been targeted by cyber assaults. Several cities were left without electricity as a result of the disturbance. "We don't know who did it," CIA senior analyst Tom Donahue said at a seminar in the United States.

On a regular basis, the United States conducts cyber War games such as Cyber Storm II (Annual Cyber War Game), which focuses on simulations for IT, communications, aviation and energy sectors..

Involved in the war simulation were Microsoft, Cisco, McAfee, and Dow Chemicals, as well as US military and intelligence organisations. It was estimated that the exercise would have cost around $6 million. In India, there are no large-scale cyber war games. However, commercial corporations such as telecommunications providers and Internet service providers (ISPs) are involved in such drills.

More than 5,000 Indian websites were hacked by hackers in 2006, according to India's CERT-In. The bulk of hacked and defaced websites were in the commercial domain (90 incidents), followed by 26 on the.in domain. In the.org domain, there were as many as 11 occurrences of defacement. In October, 61 percent of all hacking instances were due to phishing, 27 percent were related to unauthorised scanning, and 8 percent were related to harmful code. The number of phishing assaults in India has increased by 180 percent since 2005, and the trend is expected to continue.

According to a report by Al Jazeera, a US congressional panel has warned that China has built a cyber warfare programme so advanced and active that the US "may be unable to resist or even notice" an assault.

China's hackers were able to "take data" from the United States' nuclear weapons facility at Oak Ridge, Tennessee, according to the New York Times in December 2007. China's cyber-spies are now practically a part of the American computer network, as this article shows.

China's cyberwarfare force is advancing, according to sources, and India is feeling the effects. Officials claim that China has been attacking Indian computer networks, both public and private, virtually daily for the past year and a half, demonstrating both its willingness and capacity to do so. The attack is based on the fact that Chinese cyberwarfare experts are constantly examining and mapping India's governmental networks. That information helps them understand the topic and how to disable or distract their opponents during a confrontation. As a result of China's rapid development of cyberwarfare capabilities, a US congressional panel has warned that it may soon be able to delay or disrupt the deployment of American military personnel anywhere in the globe, giving it an advantage in any future confrontation.

4.0 STRATEGIES TO FIGHT AGAINST THE CYBER ATTACKS

a) RECRUITMENT OF EXPERTS

The investigating cyber attack team should be sent in escorted by Special Forces to investigate and neutralize potential threat. Special Forces should be well equipped technically to secure the confidential data and neutralize any threats. They should ensure safety of cyber attack team and help them reaching the objectives of the training. The team should remain undetected by local authorities.

Cyber attack team should be composed of:

- Forensics specialists
- Firewalls specialist
- System security specialist
- Specialist in energy industry's applications security

In order to better protect the country, forensics experts should gather any and all evidence of an upcoming attack or other potential threats. Upon completion of the forensic investigation, other members of the cyber attack team should evaluate any potential dangers that may have been spotted by the forensics specialists. The remainder of the team should strive to deactivate any external automatic attack mechanisms and notify the local defensive teams of these external sites if they detect them.

b) LOGICAL SECURITY

This is the main cyber-security battlefield where digital information is being exchanged or stored. Every security measure that is performed by a non-human device in the digital world is a member of this group.

There are many sub-fields here:

- Encryption
- Network security

- System security
- Application security
- Security monitoring/auditing

c) TRAINING THE CYBER TROOPS

It's impossible to assemble a cyber army of volunteers even if they're some of the most prominent computer security professionals in the country. For all their speed and accuracy, these soldiers will not be able to succeed in logistics and tactics. There has to be a mechanism in place to train a cyber army effectively. Procedures must be established to assist deal with these kinds of circumstances. Before any training can begin, all of this infrastructure must be put in place. Standard army field guides can't be utilised to train cyber warriors since quality, not quantity, is what's important. In order to attain the desired results, new strategies and tactics must be devised from the ground up. It's easier to distinguish between offensive and defensive training than in actual combat training.

THERE ARE 3 TYPES OF TRAINING

1. Proactive securing of a target
2. Immediate reaction on an attack and security of the target
3. Security forensics after attack and securing of target's infrastructure to prevent more attacks

Type 1 Training includes the deployment of a system with the applications of security checklists in order to bring the system and network components to a securely configured level. There are passive security measures deployed to monitor the system as well as provide sufficient auditing data to identify what happened.

Type 2 Training is analogous to security drills on a military base. Here, an alert is issued to team members have to gain control over the system and remove all the attackers from the system. It is done with cooperation with offensive warfare teams. After alert is issued there needs to be an escalation procedure executed which informs global security control center (GSC2) of an ongoing attack.

Type 3 Training takes place in systems which are already hacked. Its main objective is to analyze system state and logs and reconstruct the actions that attackers did. This can help to secure the system as well as give some information to offensive warfare teams how to perform similar attacks. Its objective is to detect what has been changed in the system to prevent further damage or fraud.

CONCLUSION

New technology is needed for online banking, smartphone apps, and fast payments. Increasing the industry's reliance on technology leads to an increase in attack vectors and the creation of new vulnerabilities. Financial services organisations are increasingly being targeted by cyberattacks because they have resorted to technology as a means of solving many of their problems. Big data is increasingly being used by financial organisations in an effort to gain market share. Social media, consumer databases, and news feeds can help financial institutions better understand their current consumers and recruit new clients. Because of the inherent dangers of modern technology, universities are under increasing need to produce an ever-increasing number of highly trained security specialists. The banking sector may have faltered at the start of the fight to keep ahead of cyber bad actors. Because of the world's dependence on computers, networks, and technology, cyber assaults are extremely harmful. These computers are responsible for everything from power plants to telecommunications to air traffic. All countries face the threat of a disastrous economic impact from cyber assaults on banks and stock exchanges. Global regulation of cyber crime and cyber war is trailing behind; it's the Wild West of cybercrime and cyberwarfare (untamed territory). There is still a lot of work to be done to fight cyber warfare threats, despite the government's efforts. When sending emails, for example, there are a number of strategies to employ in order to prevent being intercepted. Rajat Khare, Director of Appin Networks, a network security organisation that manages security for big facilities like the DMRC, Rashtrapati Bhavan, etc., warns that some satellite phone brands are tough to tap. When it comes to this situation, the best people can make a big difference. In terms of developing the capacity to counter cyber assaults, this is only the beginning. Aside from fighting on the ground, enemy cyber warriors may knock down defence computer systems, all government systems, black out nuclear plant data, and introduce deadly pollutants or viruses that can disrupt all communication lines. There's no doubt that India needs an army of cyber fighters to deal with the threat that is out there. Terrorists communicate over the internet, and the Indian government, notably the cybercrime units of Delhi Police and the Ministry of IT, does not have enough skill to intercept these communications. An concern is the company's inability to attract high-quality employees.

REFERENCES

[1] Walters, R. (2015). Cyber attacks on US companies since November 2014. The Heritage Foundation, 4487.

[2] Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. NC Banking Inst., 20, 277.

[3] Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).

[4] Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund.

[5] Trojan Dragons: China's International Cyber Warriors, John J. Tkacik, Jr., 2007

[6] Notes from a presentation by Dr. Andrew Palowitch entitled, "Cyber Warfare: Viable Component to the National Cyber Security Initiative?" at Georgetown University, November 27, 2007.

[7] Stephen Fidler, "Steep Rise in Hacking Attacks from China," The Financial Times, December 5, 2007, at www.ft.com/cms/s/0/c93e3ba2-a361-11dc-b229-0000779fd2ac.html. Source cites Yuval Ben-Itzhak, chief technology officer for Finjan, a Web security group based in San Jose, California.

[8] John Markoff, "China Link Suspected in Lab Hacking," The New York Times, December 9, 2007

[9] Marchetti, M., Colajanni, M., Messori, M., Aniello, L., & Vigfusson, Y. (2012). Cyber attacks on financial critical infrastructures. In Collaborative Financial Infrastructure Protection (pp. 53-82). Springer, Berlin, Heidelberg.

[10] Mbelli, T. M., & Dwolatzky, B. (2016, June). Cyber security, a threat to cyber banking in South Africa: an approach to network and application security. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 1-6). IEEE.