International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

The Language of Information Security

Mahesh P G

Senior Manager, Syndicate Bank, Center for Information Security, Risk Management Department,
Corporate Office, Bangalore, Karnataka 560-009, India

Abstract: ***This paper examines the concept of information security; the threats it faces, its relevance and prospects in the 21st century. Information security is vital to every industry but much more importantly in the financial industry. This is because of the threat of hacking is greater in this industry than in every other industry. A lot has been done in the area of enhancing the security measures to guard against such threats however the best solution to these security challenges is to embark on effective training and manpower development of IT professionals in each organization with the support of Senior Leadership. Senior Executives are ultimately responsible for the security of information entrusted to their organization. A well supported information security program by the management will enhances the work safety to the employees, confidence and trust to customers, meets regulatory requirements and provides continuity of business.***

Keywords: Information Security, Cyber Security, Compliance, Hackers, Risk, DDOS

1. Introduction

The first information security threats were actually created before the advent of modern computer systems. Decades ago, criminals often looked to tap into phone systems. In fact, starting from the 1960s, AT&T decided to closely monitor calls in order to catch “phone freaks.” These “phreakers,” as they were called, used “blue boxes” to generate the right tone to get free calls [1].

During the early years of computing, the mainframes used by the military were connected through dedicated phone lines to form ARPANET, the precursor to the modern internet. While this allowed easy synchronization of information between data centers, it also provided unsecure points between the data centers and the public. Although, this vulnerability was addressed by securing physical locations and hardware; a task force formed by ARPA (Advanced Research Projects Agency) to study internet security in 1967 found this method to be inadequate, and the Rand Report R-609 determined additional steps must be taken to improve security. This report marked an important stage in the development of today's information security [2].

Some early security efforts focused on the mainframe operating system. MULTICS (Multiplexed Information and Computing Service) was an effort by MIT, Bell Labs and General Electric to build security into mainframe operating systems using multiple security levels and passwords. It became obsolete when the era of personal computers arrived [2].

2. Background

The first PC virus named “Brain” was developed in 1986, but it was not destructive in nature. In fact, the men behind it actually included their names and contact information which was inputed within the code. More harmful viruses eventually followed, including “Form” and “Michelangelo” and the first sets of self-modifying viruses were first created in 1990, although rapid infection rates didn’t take off until several years later. The threat continued with various incidents like “Solar Sunrise”, Distributed Denial of Service attack towards e-Commerce sites, Code Red worm, Nyxem virus, Storm Worm to name a few till to the more recent threat known as Ransomware. Certain attacks were for fun and other attacks infected millions with losses in the range of several billions of dollars incurred [1].

However, as the world evolves, the range of threats the internet is exposed to is changing as well. Nowadays, the biggest future threat to information security is a lack of skilled and educated professionals in the industry. Come to think of it, the success of any security threat on the internet itself is contingent upon inexperienced engineers on the other end to counter and tackle the imminent security threat. This is why there is an ongoing need for network security engineers, information systems security engineers and other digital security specialists.

The threats or attacks mentioned above irrespective of their nomenclature has made organizations to think of developing a different vertical for Computer Security as a tool for safeguarding valuable assets as well as maintaining customer confidence. Nowadays, the scope of Information Security has taken on other technical areas like systems, network etc and the name Cyber Security is more in use.

The new vertical in organizations paved the way for specialized staff to perform the task which requires more technical knowledge of Systems and Network. Security tools are now required to be infused in the host and networks to detect, prevent and recover from security breaches against a network. Consequent upon this, defense in depth strategy has been developed. This is a security discipline that refers to having layers of protection in an IT infrastructure. This means that multiple security solutions are required to have a defensive in-depth strategy which mainly requires budget from the senior management, which was one of the challenges faced by the Security vertical to justify and convince the senior management about the loss the organization will incur if the solution is not implemented in case of a security breach. A risk analysis or similar approach to estimating risks, vulnerabilities, exposures,

countermeasures, etc. is just not sufficient to convince a senior manager to accept large allocations of resources.

Quantifying the Security for every threat is not an easy task like the reputation loss due to a DDoS attack, the actual loss when an alternate transaction channel of a financial organization is down etc. Quantifying is difficult, if not impossible, especially as it entails comparing the cost of controls with the risk of loss in order to determine which controls are the most cost-effective. Ultimately, business managers and security specialists must rely on the best information available and their best judgment in determining what controls are needed to convince the business or senior management, that the language of information security has gone bilingual. Bilingual means the language between Business (Senior Management) and the ground level security functions [3]. The best strategy in dealing with the top leaders of the organization in getting them to shore up their cyber security apparatus is Respect. Never talk down to them, or try to confuse them with buzzwords or technical jargons. It is also helpful if you can explain any lessons learned and discuss strategies to avoid breaches in the future.

3. Solution

The cyber security industry is fast paced and dynamic and require curious individuals who understand digital communications and software, and value the structure of a regulated environment. This is because the responsibilities involved are enormous; Social Engineering for example can even trick the tech savvy people in the IT industry itself. The security knowledge of Information Technology workforce is even limited to the extent of safeguarding their credit card or debit card details, online credentials for financial transactions etc, they could also fall as a prey when it comes to organizational security. For instance in a situation where general users (non tech savvy) working in organizations like banking sector dealing with Core Banking Systems using user ID and passwords which are considered to be a weak authentication mechanism might be unable to adequately respond to hacking attempts launched at their organization. As serious as these threats are, the focus on phone networks would soon pave the way for greater risks to computers. Cyber criminals are going to greater lengths to ensure their attacks pay off [5]. Hackers, for example, are increasingly posing as CIOs and CFOs in order to convince victims to download malicious payloads [5].

Presently, Cybersecurity has moved from tech to a CEO and Board-level business issue. Senior Executives are the ultimately responsible for the security of their organization. They now have legal responsibilities to provide adequate resources to protect the information system of the organization. The responsibility for information security is owned by senior management, whether they want it or not and whether they understand its importance or not because information security can only work when senior management supports it, and that support can only occur when they can be convinced of the importance of information protection. Recent high-profile security breaches have made it easier to secure senior executive buy-in for security investments.

4. Benefits to Management for Aligning Security to Business

- **Business success/ resilience** - Information is one of the most important assets to an organization. Effective security ensures that vital services are delivered in all operating conditions. Ensuring the confidentiality, integrity, and availability of this strategic asset allows organizations to carry out their missions.
- **Increased public confidence and trust** – Strong security helps to increase customer confidence, loyalty and trust towards the business which leads to more business growth.
- **Permits staff to work safe and Enhance productivity** – Security controls translates the high level management policy in the information security to procedures to be followed by the staff and gives a confidence to the management that the internal threats are mitigated to a certain level.
- **Regulatory Compliance and Advisories** – Proper security mechanism in the organization helps to meet with regulatory requirements for the service organizations, which also enhances the confidence of management.
- **Business Continuity** – A well aligned information risk with the business continuity management prevents the business to stop its function during any unforeseen events. This provides continued business process and growth.

5. Challenges in the area of Information Security

1) **Identifying Information Resources to be protected** – Classifying information assets in the organization is as important as placing the security measures [4].
2) **Preparation of Risk Assessment Procedures that link security to business** – As security is a business enabler; there is a need to be decisive in dealing with the risk. Many senior managers don't want to listen how bad everything will be if they don't invest in risk management and security. The best way to get the senior management to act is to enumerate the value that accrues to the business and the survival threats that cyber-attack poses [4].
3) **Continuous Assessment and management of Risk** – It is important to continuously assess the security risk and evaluate the existing controls to ensure they are appropriate and effective.
4) **Allocation of funds and dedicated staff** – Funding and dedicated staff to be provided to drive the information security of the organization.
5) **Enhancement of staff technical strength in the area of security** - Staff expertise had to be frequently updated to keep abreast of ongoing changes in threats, vulnerabilities, software, security techniques, and security monitoring tools.

6) **Imparting Continuous Education** to Users and Others stake holders with respect to Information Security Policy of the organization.

6. Conclusion

Information Security vertical in an organization will achieve its goal only when there is a full support from the senior management with regards to directions to improve the security risk of the organization by various controls.

The team performing the Information Security functions must have highly experienced personnel requisite understanding of technology as well as the necessary tools to combat security threats. They should have direct access to the management so as to communicate the Information security risks in the organization to the senior management more effectively as they arise.

Information Security program developed in the organization must adhere to the baseline controls outlined in the High level policy of the organization provided by the Senior Management. A well supported information security program by the management will enhance the work safety to the employees, confidence and trust to customers, meets regulatory requirements and ensure continuity of the business enterprise. Essentially, Information Security is a program and not a project with a defined beginning and end.

References

[1] Digital Dangers: a brief history of Computer Security threats https://www.informationsecuritybuzz.com/ articles/digital-dangers-brief-history-computer-security-threats/
[2] History of Information Security by Bisk https://www.villanovau.com/resources/iss/history-of-information-security/#.WynhBfV9jcs
[3] The business case for information security: selling management on the protection of vital secrets and products Sanford Sherizon - http://www.ittoday.info /AIMS/DSM/82-01-32.pdf
[4] Executive guide Information Security Management for the protection of electronic Information and automated systems https://www.gao.gov/assets/80/76396.pdf
[5] Peak ransomware": incidents are declining, but attacks are increasingly disruptive by Oscar Williams http://tech.newstatesman .com/ security/peak-ransomware-disruptive

Author Profile

Mahesh P G received the B.Tech in Electronics and Communication Engineering from Mahatma Gandhi University, Kerala in 2007 and MBA in Information Systems from Sikkim Manipal University in 2013. During 2007 - 2010, he stayed in Multimedia Technology Department, Tata Elxsi, Technopark, Trivandrum, Kerala. He is a Certified Information Systems Security Professional (CISSP) from ISC2 since March 2015. He is now with SyndicateBank as Senior Manager (IT), Center for Information Security, Risk Management Department, Bangalore.