Next Era of Information Security: A Review

Madhavi Dhingra
Asst. Prof. Amity University, Gwalior, Madhya Pradesh
madhavi.dhingra@gmail.com
Contact No. 8085136555

Abstract - Now a day's Information Security breaches are occurring on a wider scale. The incidents are not only covering commercial activities, but are also affecting the networks of several countries of the world. Web is enhancing the efficacy of everyone whether work is for local personal level or professional global level. Web has now become the information warehouse as well as medium of transferring the information. Hence web security assumes great importance in order to ensure its accuracy and authenticity. These years, several kinds of attacks are occurring on the network from smaller to big ones. In view of these attacks which are being launched every other day, the information on the web needs to be secured. The need of the hour is to understand the gravity of recent attacks and come up with requisite security solutions. This paper attempts to highlight the impact and security areas that will be concern of IT professionals in the coming years.

Index Terms- Information Security, Security Risks, Data Security

1 INTRODUCTION

Information security is associated with protection of information in terms of its confidentiality, integrity and availability. Over the last few years the tools for storing information and gathering information has moved towards web. Everything that is stored on the web is susceptible to attack. And thus the need of security of the information stored over the web assumes great significance.

Today, organizations are taking part in making security policies as well as spending huge sum of money in buying security services for their confidential and sensitive data. Simultaneously attacks are redefining themselves every hour. Therefore newer and better security techniques are being developed.

This paper begins with outlining security incidents of 2014 and follows it up with major security concerns in the current year. Finally it attempts to cover the security imitative which the organizations will need in order to attain reasonable degree of security.

2 IMPACT OF SECURITY INCIDENTS

Consumers and organizations have faced huge number of privacy attacks and security attacks in last year. Malware, Hacking, viruses, bots have affected both smaller and larger businesses. 2014 has proven that wealth and status don't guarantee immunity from wrongdoers seeking to misuse technology for their own ends; Tech Pro Research, conducted a survey on IT security and found that about two-thirds of the respondents said they were most concerned with security after several media news reports of breaches and leaks. As things stand today only large organizations are focusing to implement security services. Smaller companies are not able to follow them because of the unawareness and higher cost involved [9].

Increase in global information security threats remains as much a certainty as death and taxes, at least according to the latest Information Security Survey from PWC. PWC has indicated that cyber security is the biggest risk for the economical and intellectual assets of the enterprise. Its report has identified some really severe incidents that include [11] -

- More than half (53%) of global securities exchanges have experienced a cyber attack (IOSCO Survey)
- In South Korea, some 105 million payment card accounts were exposed in a security breach (Symantec Corp)
- City officials in Verden, Germany announced the theft of 18 million email addresses, passwords and other information (TechWeek, Europe)
- Cyber thieves stole more than $45 million from worldwide ATM accounts of two banks in the Middle East (CNet.com)

These incidents imply that attacker's motive is mostly financial. And as a result most secure organizations are also prone to attacks. Hence the efforts of the cyber crime specialists aim to protect the assets and to devise more powerful methodology for security so as to meets the concerns of the businesses. Strategies for risk management need to be upgraded so as to handle the potential threats and thereby minimize the financial losses.

Impact of security incidents are measured in terms of information losses and financial losses. Larger organizations are more concerned about their information security, so they spend more on implementing the security strategies and using the security systems. They consider all possible impacts like costs regarding loss of customer business, loss of assets and damage of reputation in the market.

The global annual estimated reported average financial loss attributed to cyber security incidents was 2.7 million USD. In India, it rose to 1.2 million USD, almost 20% more than the previous year.

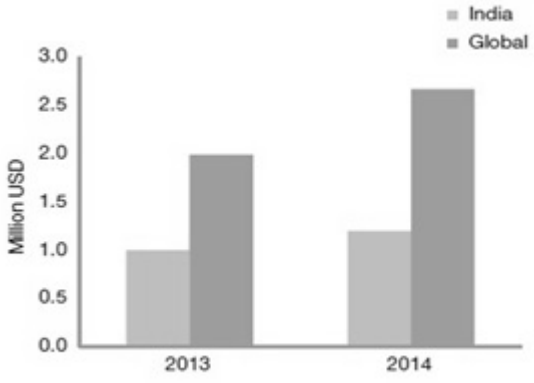

Fig. 1
Average financial loss attributed to security incidents [2]

3 INFORMATION SECURITY AREAS IN COMING YEAR

Last year, high profile information security incidents are targeted multinational companies like Sony. Their vulnerabilities like Heartbleed had the potential to affect a large part of the web.
The areas where information security will be noticeable this year will be following [11] –

3.1 Insider Threats

Insider threats come from inside the organization. Just like hackers hacking the computers remotely from anywhere. Moreover, it can be from the insider employees of the organization. If information is being leaked or modified or corrupted by any of these, then it will be harder to find out and determine the impact and level of problem. This clearly implies that the threats occurred from inside are more harmful and damaging in comparison to the outsider attacks. This problem becomes worse, when proper needed security systems are lacking in the organizations, especially smaller organizations that are not spending on the security. Also cost cutting and budgets of the organization are affecting their security expenses. This can be a serious issue as information in these organizations will be too insecure to be dealt.

3.2 Mobile Security

These days use of mobile phones has become universal. Use of Smart phones and tablets is also increasing day by day. And thus connecting them online requires security of the devices as well as the information. Companies are increasingly turning to mobile device management (MDM) and mobile application management (MAM) solutions. These allow separation of business and personal data and provide a 'kill switch' to wipe data should the device be lost or stolen.
Thus companies need some security policy to identify the threats attacking the mobile devices and disrupting the flow of information that they are passing.

3.3 Ransomware Threats

Ransome threats are here from the past ten years. This kind of threat encrypt the data of the computer and this malicious software worked by encrypting data o stop the overall working of the computer there by flashing the message on the screen which asks for the money as a fine otherwise the machine will be forever in the locking state. The culprits are sometimes caught, but this malware is gaining popularity and new techniques for hiding are being invented. This threat is refining its methods and techniques of attacking.
According to security company McAfee, ransomware will seek to target systems that are linked to cloud storage solutions. By encrypting storage like Dropbox or Google Drive it will have a much more severe impact. Users may find that their cloud backup copies have also been locked by the malware making it harder to recover. Nowadays, companies are employing cloud for their storage and platform requirements, and therefore these attackers are targeting the cloud for making huge amount of money from bigger enterprises.

3.4 State-Sponsored Hacking and Hacktivism

John Nesbitt, founder of Cyber Senate, a community of global cyber security business leaders famously warned recently that, "The next world war will be fought on a keyboard." With the recent Sony hack we've seen increasing evidence that some national governments may be involved in the attack or use it for obtaining a political benefit.
This type of hacking will not only harm other governments but also instigate other governments to attack their own government economy by other foreign governments. Terrorists can also take the advantage of these cyber crimes that are done by the group of hacktivists. Any country's confidential information can be the target of attackers. High-profile industries like power generation and defence are more attractive areas for the snoopers.

3.5 Cyber Insurance

To protect the data from disruption and attacks, organizations are now opting for cyber insurance. The price paid for having the security safe systems are same as the cost given to the investigators following the breach of data. These insurance companies will apply better security measures to secure the information of the enterprise.

4 SECURITY INITIATIVES

Due to increased number of security incidents and their heightened impact, corporations and industries are trying to find ways for protecting their data and networks. This poses a driving force for the growth of cyber security solutions and devising newer technologies for security of the information.
Following are the four key drivers for information security market growth in India according to the Key findings from The State of Information Security Survey 2015, India [2].

- Increasing sophistication and frequency of attacks
- Increasing number of financially and politically motivated attacks
- Slew of legislations focused on security and privacy
- Increasing IT expenditure

This report predicts that India's security market size will jump to 1 billion USD in 2015.

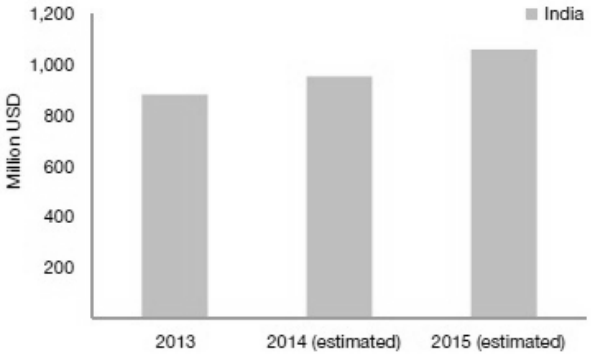

Fig. 2 India's security market size [2]

For securing information, security initiatives must be taken by the organizations dynamically. Strategies and technologies are developing to prevent, protect, detect and respond to the security risks. Organizations are lagging behind in using these four approaches. Also, employee training and awareness programmes to know about the security practices are not being undertaken as per needs.

- Prevention of attacks are done by organizations at different levels using biometrics, disposable passwords or token for authentication, user-activity monitoring tools, Governance, risk and compliance tools.
- Protection of information is done by organizations by encryption of smart phones, data loss prevention tools, encryption of networking transmissions, and intrusion prevention tools.
- Detection is done by using mobile device malware detection, vulnerability scanning tools, malicious code detection tools, unauthorized devices discovering tools.
- Responding against risks will involve Security information and event management (SIEM) technologies, and threat assessment tools.

The NIST has given a similar security framework (NIST Cyber security Framework) that stresses management over technology and highlights several best practices that will help in preventing against threats.

Following two additional points are to be employed for better security management.

- Identifying will build an institutional understanding of cyber security risk to organizational systems, assets, data and capabilities
- Recovering will develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cyber security event.

4.1 Security trends for the organizations in the coming year

- Focusing more on responding to threats rather than preventing them – It is inevitable now for the organizations after seeing the data breaches, that the incidents will anyway occur, so the need is to prepare for the threats.
- Managed security service providers – Larger organizations spend heavily on the security. As security service providers have deep insight of knowledge of the threats and the attacks, thus they are more experienced dealing with the situations.
- Cloud Security – More and more organizations are moving their data and applications over cloud, and thus security of the same data over the cloud is essential. There are many security policies that are provided by cloud, but still there is lot more to be done in this field.
- Secure platforms – In the coming year, it is predicted that the development of secure platforms is the foremost rather than developing newer secure technologies. A secure platform enables the organization to run multiple applications without compromising any mobility or change in technology. Organizations will have a single secure platform rather than multiple security products.

5 Conclusion

Information Security is the major agenda for the near future. Securing data, securing platform, securing applications, everywhere security is the major goal. Various security technologies, security controls, policies and service providers emerged in 2014. But this is not the end. The newer trends and the areas of security in 2015 are highlighted in this paper. Attacking methods are refining and thus newer security controls need to be developed for every area, whether it is at local level or for global level.

References

[1] Alshaikh, Moneer; Ahmad, Atif; Maynard, Sean B; Chang, Shanton. Towards a Taxonomy of Information Security Management Practices in Organisations, 25th Australasian Conference on Information Systems; Dec 2014, Auckland, New Zealand

[2] Managing cyber risks in an interconnected world Key findings from The State of Information Security Survey 2015, India: pwc.in; October 2014

[3] Michael Whitman, Herbert Mattord. Management of Information Security , 4th ed. ;2012

[4] Mikko Siponen, M. Adam Mahmood, Seppo Pahnila. Employees' adherence to information security policies: An exploratory field study, Elsevier Information & Management, vol. 51, issue 2; Mar 2014, pp. 217-224

[5] Mikko T. Siponen, Harri Oinas-Kukkonen. A review of information security issues and respective research contributions; ACM SIGMIS ,vol. 38 issue 1; Feb.2007, pp. 60 – 80

[6] Peter Hough. Understanding Global Security 3rd ed.; 2013

[7] Richard Baskerville, Paolo Spagnoletti, Jongwoo Kim. Incident-centered information security: Managing a strategic balance between prevention and response, Elsevier Information & Management, vol. 51, issue 1; Jan. 2014, pp. 138-151

[8] Robert E. Crossler, Allen C. Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, Richard Baskerville, Future directions for behavioral information security research, Elsevier Computers & Security, vol. 32; Feb.2013, pp. 90-101

[9] Survey: Top security issues for 2015. Available online at: http://www.techrepublic.com/article/survey-top-security-issues-for-2015/
[10] Top 5 IT security trends to watch in 2015, dimensiondata; 2014
[11] 2015 prediction: Expect massive spikes in global information security threats. Available online at: http://www.techrepublic.com/article/2015-prediction-expect-massive-spikes-in-global-information-security-threats/