ISSN:0975-9646

Securing Classified Information:
A Six-Step Approach to Data Classification

Siti Hazwah Abd Karim[1], Dr. Zahri Yunos[2], Mohd Shamir Hashim[3], Rahayu Azlina Ahmad[4]

CyberSecurity Malaysia,
Seri Kembangan, Malaysia

***Abstract*—The Internet's implementation and reach over businesses, governments and individuals are ever-increasing. Thus, it is not at all an overreaction to anticipate for cyber-attacks to be subsequently on the rise, which will in turn ultimately lead to data breaches. Malware and cyber-attacks intended to breach data will continue to evolve and organizations must take the necessary steps to secure their valuable assets and mitigate potential risks through appropriate data classification approaches. The SANS Institute's six-step approach is recommended as a possible solution to secure classified data.**

***Keywords*—cyber-attacks, malware, data breaches, data classification**

INTRODUCTION

Internet users all over the world are constantly at risk of information breaches and identity theft - yet most of the time, they do not even realize it until it is too late. In 2012, a survey on information security cited by Susanto et al. [1] revealed an increasing trend of information breaches that has led to enormous losses. It was argued that since information is the lifeblood of organizations, i.e. a vital business asset in today's IT-enabled world, securing information resources is extremely important in order to ensure that resources are well-protected.

Three years later, in just the span of the first three months of 2014, 669 major information security-related incidents were reported, affecting approximately 176 million records. Risk-Based Security [2] cited a single incident of insider fraud involving Korea Credit Bureau in January 2014, whereby 104 million credit cards were exposed along with their expiration dates, 20 million names, social security numbers and phone numbers.

Such a disastrous incident only further supports the fact that the primary concern in today's e-world is indeed the protection of information and critical data. Sharma and Dash [3] maintained that given the immense value of information to organizations, securing information assets through a system of information security is of utmost importance. Not surprisingly, a research by Memarzadeh et al. [4] has shown that information systems and networks of various organizations are progressively becoming the subject of security problems, such as embezzlements, spying, sabotage and subversions.

According to Ahmad and Yunos [5], cyberspace and the Internet are at the center of modern life and have become an important medium for businesses, economics, politics and communities. They also stressed the fact that many nations worldwide are constantly and increasingly dependent on cyberspace by maximizing the use of Information and Communication Technology (ICT). ICT is a double-edged sword, which aptly explains why cybercrime will always be on the rise.

Yunos et al. [6] also maintained that ICT can simultaneously serve as a powerful tool for perpetrators, such as extremists and terrorist groups who wish to promote radical ideologies and propaganda materials as well as create public fear by damaging assets vital to national interest and security. Their argument further proves how fragile the current situation is with regards to the well-being of global Internet users as the receiving end of various possible threats lurking within today's highly connected world.

CAUSES OF DATA BREACH

Malware Threats

Nowadays, the traditional network perimeter is fading, while single endpoint solutions are becoming the main choice for active threat mitigation when it comes to information and data security. This is evidently the case when looking at findings by the NNT Group [7], which reported that 43% of incident response engagements were the result of malware against particular endpoints and the significant factors in such engagements were the lack of basic information system controls, such as anti-virus, anti-malware and effective lifecycle management.

The report also indicated that anti-virus fails to detect 54% of new malware collected by honeypots and further research on this shows that 54% of malware designed to take over compromised systems goes undetected by the anti-virus solutions in place. The research also discovered that 71% of new malware designed to siphon money or information from compromised systems goes undetected as well [7]. The finding supports the premise that simple endpoint solutions, while useful at controlling some malware threats, are not fully capable of defending those endpoints against many modern and new attacks, and the solutions must be amplified with network malware detection and purpose-built solutions. The report [7] additionally stated that open environments such as education have been receiving the majority of attacks, likely due to the open access models that are commonly implemented in higher-learning institutions besides the inability to enforce security controls over thousands of student-owned devices.

Application Security Weaknesses

This trend has ultimately created a new perspective for application security, which is now regarded as a business capability. In the past, application security has been viewed

as an aid to ensure effective business capability. However, more recently, the application end is at the forefront of services, so much so that its performance (or lack thereof) affects the corporate image of the application service provider. Consequently, the security and ability to maintain application security are becoming a core task in sustaining business trust in most, if not all organizations – large or small. Nonetheless, time and time again, application security remains the most vulnerable point.

NNT Group [7] has found that basic application security is often the primary cause of information security incidents, which can be costly. A single unsanitized field during an automated SQL injection attack can cost an organization figures amounting to USD 196,000. Even more startling, 77% of organizations supported during incident response activities appear to have no incident response plan ready and the majority of organizations have little or no investment in defining and validating a plan to help them handle critical information security incidents and minimize damage to their systems, customers and brand.

DDOS Attack

It was also stated in the NTT Group report that Distributed Denial-of-Service (DDoS) attacks accounted for 31% of incident response engagements [7]. Most organizations fail to realize the effects of DDoS attacks and some even believe they will not be targets of such attacks, which aptly explains their neglect to provide the necessary expenses to acquire proactive controls to mitigate DDoS attacks. More often than not, awareness only seems to emerge during actual DDoS attacks and by then, it is already too late.

Botnet activity was also reportedly responsible for 34% of information security-related incidents observed in 2013, where targets such as healthcare, technology and finance sectors accounted for 60%. This shows to what extent these three industries rely on the use and flow of information, how dependent they are on maintaining application security for business continuity and how vulnerable they have been all along. And given the Internet's ever-increasing implementation and reach into businesses, governments and private lives [8], it is not an exaggeration at all to anticipate that cyber-attacks, which ultimately lead to data breaches, will keep evolving and be on the rise unless necessary steps and effective measures are taken to address such risks.

IMMINENT THREATS OVER THE LANDSCAPE

Information storage and retrieval technologies have evolved drastically during the past decade. The world's information and data as we know it is being stored in a distributed manner and without any real dependency on specific physical locations. Yet there are ongoing issues, debates and concerns over how the various types of information and data are being handled on the Internet, particularly with regard to the security aspect.

Today, according to Memarzadeh et al. [4], the expansion of computer networks and availability of various computer hardware, software packages, and network complexities have amplified the risk and vulnerability of organizational information systems. They also added that the security risks involved are now at a stage where merely installing firewalls or routers will not provide adequate protection to information systems.

To make matters worse, according to a report by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) [8], business data is regularly stored in the cloud with no security beyond what is provided by the cloud storage facility; and although private-key encryption is an available option for extra security measures, it is not without problems. Thus, there will always be compromises between security, functionality and efficiency in this respect.

File sharing and other similar cloud-based services also have problematic security. Companies and staff are hastening to adopt cloud technology in order to stay abreast of the changing world – which, among others, necessitates fast and fault-tolerant storage solutions that are practically accessible from all over the world at all times. Unfortunately, the security measures surrounding these information facilities cannot be guaranteed, as information and data reside outside the corporate network parameters. This can potentially introduce risks to unencrypted data, which would not even be of concern should the said data be kept internally in the first place.

The report [8] also addresses concerns regarding information security in critical infrastructures. Findings made by two researchers from the security consultancy InfraCritical are cited, who used the Shodan search engine to find critical infrastructure systems that are connected to the Internet. Shockingly, they have discovered there are more than 7,000 servers and industrial control systems directly connected to the Internet, including energy, water and building automation control systems. Given the far-reaching and scathing effects of cyber threats over such systems, one cannot help but wonder why these systems are even connected to the Internet in the first place.

The threat is real. In 2009, Iran suffered the Stuxnet attack, which used specialized knowledge of industrial control systems employed by Iran for processing uranium. The attack was aimed to destroy the nation's refinement capability, but fortunately, it was discovered and mitigated before the situation got any worse. Although the incident was attributed to Stuxnet malware that was accidentally brought into the system via an infected USB drive (since the industrial control system was not connected to the Internet), it did not take much to conceive the magnitude of the threat and damage that could have occurred should a given system have been well-connected to the Web and waiting to be discovered through a simple Shodan search.

This further indicates that as governments, businesses and institutions rely more and more on data and intelligence to operate efficiently, cyber-attacks aimed at acquiring such information will increase concurrently. Given the rapid advancement that is evident in malware creation and propagation, it may no longer be a question of *whether* a cyber-attack will be suffered, but rather *when*.

THE COSTS OF DATA BREACHES

The costs of data breaches can be enormous. Other than the expenses required to recover or redo all affected

services and infrastructure, there would also be damage to reputation and loss of confidence with a lasting impact on business continuity and profitability. It is said [8] that many companies never recover from a major data breach. According to Pathak and Khajuria [9], data breaches are now a fact of life together with taxes and death, but the issue of main concern here is how nations, businesses and institutions can better manage the risks related to data breaches and reduce the significant costs incurred as a result.

Verizon [10] reported over 63,000 security incidents in 95 countries, of which 1,367 were confirmed data breaches, including first-time Denial-of-Service (DoS) attacks. Although these rarely result in data loss, they are still considered a significant threat. According to a study conducted by the Ponemon Institute [11], malicious attacks were the main cause of 31% of data breaches examined, up from 24% in 2009 and 12% in 2008. Such attacks cost companies the most because they are harder to detect, investigate and contain. The study also found that the average cost of a data breach for US companies rose 7% from USD 6.8 million in 2009 to USD 7.2 million in 2010.

The overall cost of data security breaches is seemingly huge. In 2013, breaches were estimated to have cost organizations in business in New York State over USD 1.37 billion [12]. It was also found that hacking intrusions were the leading cause of data security breaches among organizations conducting business in the state, accounting for approximately 40% of all breaches between 2006 and 2013.

In a research on the effectiveness of ISO 27001 as an information security system, Sharma and Dash [3] outlined three categories of consequences of information security incidents on organizations, namely operational, legal and reputational. Operational consequences have immediate impact and may be in the form of loss of crucial information assets, thus impacting businesses in terms of decreased profitability and revenue. Legal consequences may have impact over a period of time and occur due to contraventions of regulatory and statutory requirements and/or contractual agreement breaches. Lastly, reputational consequences, which could be associated with an organization for a lifetime, may affect future growth and negatively impact employee morale and motivation, and ultimately, their productivity too.

In the pre-digital age, businesses may have been able to conceal data breaches from the general public, but this is no longer possible; nowadays, organizations must fully and timely disclose data breaches or data loss. It has become as much a business problem as a technology problem [12], especially in an era in which confidentiality, integrity and availability of information and data mean everything. Essentially, the real solution to be sought is an information security management system that can prevent crucial data from being breached in the first place – which, as argued in this paper, can be achieved by adopting an information and data classification approach.

A Six-Step Approach to Data Classification

The number of organizations considering employing information and data classification best practices and solutions as part of their security approach is increasing [13]. Also, the first step to build a secure organization is through a data classification program. This refers to the process of categorizing data assets based on nominal values according to sensitivity, for example, the impact of applicable laws and regulations. The information or data of concern here is classified as public, internal, confidential (or highly confidential), restricted, regulatory, or top secret [14].

One of the fundamental objectives of classifying and labeling information or data is to ensure consistent understanding of value and purpose amongst those responsible for handling it. This shared understanding is central to an effective collaboration that requires, for instance, users to apply correct safeguarding procedures up until the implementation of automated systems that control the dissemination of the respective information or data [15].

An information classification system can be implemented in several ways, but the most fundamental factor is facilitating people within a given organization to comply with endorsed and implemented information protection measures. The most important rule to follow when developing an effective information and data protection strategy is to protect the data itself. To do this, one must understand the data flow and build a strategy around protecting data throughout the various data flow stages.

The SANS Institute [16] recommended a six-step approach to be considered for classifying data (see Figure 1) and in due course, to safeguard against the risk of breaches due to cyber-attacks. The steps to the approach are as follows:

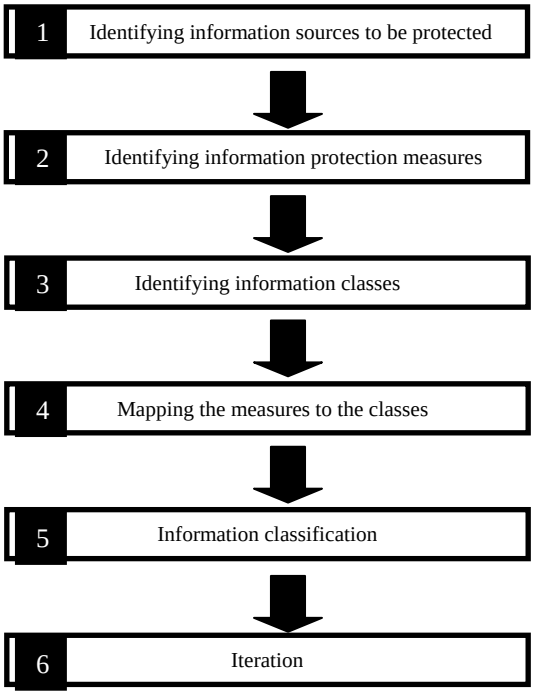

Figure 1: A Six-Step Approach to Data Classification

Step one requires identifying all information sources that need to be protected. Completing this step is expected to produce a high-level description of the organization's information sources, such as information or data location, existing protection measures, data owners (e.g., individuals responsible for establishing the related policies), data custodians (e.g., individuals/users responsible for maintaining the information) and the resource types.

Step two involves identifying the information protection measures that map onto the information classes. Information protection objectives can be obtained from various sources, for example an organization's security policy as well as existing organizational structure and informal data segregation approaches that are in place.

Step three entails identifying information classes. Information class labels should convey the protection goals being addressed. Classification labels, such as Critical and Sensitive, mean different things to different people; therefore, it is vital for high-level class descriptions and associated protection measures to be meaningful to individuals who will classify the information or data as well as those responsible for protecting it.

Step four is the stage in which the information protection measures are mapped to the information classes. Before the information or data can be classified, the protection measures (identified in Step 2) must be mapped to the information classes (identified in Step 3). This is done in order to reflect the organization's protection goals. For example, the classification of the first iteration is based on one data class that has identified four varying degrees of protection for confidentiality, integrity, availability and assurance. The four degrees are Proprietary, Discretionary, Internal and Public.

Step five entails classifying information. In this step, the classification labels and protection measures (mapped in Step 4) must be applied to the sources (identified in Step 1). The main objective here is to validate that the protection measures associated with the classification are appropriate for the given information source.

Step six is where the iterative process of adjusting classes, protection levels and sources begins. This step is to be repeated as necessary, which explains why information classification is considered an iterative and on-going process. Furthermore, an organization's security policy should always state that information and data classification is expected. Relevant standards and procedures must also be reviewed and implemented to ensure that the introduction of each new information source triggers the information classification process and that retiring information sources and/or related classifications are removed.

It is also worth noting that in the absence of information and data classification, decisions related to protection will be made at lower levels in a given information eco-system. This involves the security, system, and database administrators and their discretion over information, data-related issues at hand and obviously not long-term solutions that can be relied upon.

Today, organizations of all sizes are seeking new ways to gain assurance over information and data security. There has been a significant increase in small businesses spending on information security [17]. Governments above all, should indeed be at the forefront in addressing this and come to terms with the fact that information and data classification systems are what is really needed in order to ensure any efforts to successfully secure classified information and data.

CONCLUSION

All in all, it goes without saying that information and data security is of paramount concern to any organization that is connected in the modern-day wired world. In order to survive without experiencing breaches and consequently paying the price and enduring the aftermath of such incidents, it is of utmost importance for organizations to adopt information and data classification as a solution to protect their valuable and intangible assets. And rather than being considered a replacement for existing security solutions, information and data classification should actually be adopted as a mandatory complement to existing technology-based security measures, whereby both are expected to work together to cover all possible endpoints in an organization's information eco-system that may be under the scrutiny of those with ill intentions.

REFERENCES

[1] H. Susanto, M. N. Almunawar, and Y. Chee Tuan, "Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level," *Int. J. Eng. Technol.*, vol. 2, no. 1, pp. 67–75, 2012.

[2] "Data Breach Trends in the First Quarter of 2014." Risk Based Security, 2014.

[3] N. K. Sharma and P. K. Dash, "Effectiveness of ISO 27001 as an Information Security Management System: An Analytical Study of Financial Aspects," Far East J. Psychol. Bus., vol. 9, no. 3, pp. 42–55, 2012.

[4] G. Memarzadeh, S. Fayez, D. Kiakojuri, and F. Bozorgi, "Risk Assessment of Information Security Management Systems in Large Corporations," Life Sci. J., vol. 10, no. 6s, pp. 842–845, 2015.

[5] R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," Int. J. Comput. Sci. Inf. Secur., vol. 10, no. 2, pp. 149–158, 2012.

[6] Z. Yunos, R. Ahmad, and N. A. A. Sabri, "A Qualitative Analysis for Evaluating Cyber Terrorism Framework in Malaysia," Inf. Secur. J. A Glob. Perspect., pp. 1–9, 2015.

[7] "2014 Global Threat Intelligence Report." East Palo Alto: NTT Innovation Institute, pp. 6–7, 2014.

[8] "Emerging Cyber Threats Repot 2014," Georgia Tech Information Security Center (GTISC), 2014. [Online]. Available: https://www.gtisc.gatech.edu/pdf/Threats_Report_2014.pdf.

[9] S. Pathak and K. Shiny, "A Statistical Study on a New Era of Information Security and Cyber Risk Management: Cyber Insurance," Int. J. Sci. Res. Dev., vol. 2, no. 11, pp. 17–20, 2015.

[10] "2014 Data Breach Investigations Report." Verizon, 2014.

[11] U. Mattsson, "Choosing the Most Appropriate Data Security Solution for an Organization," ISACA J., vol. 6, pp. 1–6, 2014.

[12] "Information Exposed: Historical Examination of Data Breaches in New York State," Attorney General Eric T. Schneiderman, 2014. [Online]. Available: http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf. [Accessed: 22-Dec-2014].

[13] D. Langton, "The Year Of Data Classification?," Boldon James Blog, 2014. [Online]. Available: http://www.boldonjames.com/data-security-blog/security-trends-for-2014-the-year-of-data-classification. [Accessed: 28-Nov-2014].

[14] C. Rodgers, "Data Classification: Why Is It Important for Information Security?," Secure State, 2012. [Online]. Available: http://blog.securestate.com/data-classification-why-is-it-important-for-information-security. [Accessed: 28-Nov-2014].

[15] J. Boldon, "Standards for Information Classification: A Benefit to Collaboration?," 2013. [Online]. Available: http://www.boldonjames.com/assets/downloadableFiles/Standards-For-Information-Classification-Whitepaper.pdf. [Accessed: 19-Dec-2014].
[16] S. Fowler, "Information Classification - Who, Why and How," SANS Institute InfoSec Reading Room, 2003. [Online]. Available: http://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846. [Accessed: 03-Dec-2014].
[17] S. Fowler, "2014 Information Security Breaches Survey," *Welcome to GOV.UK*, 2014. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf. [Accessed: 13-Dec-2014].