International Journal of Management and Commerce Innovations ISSN 2348-7585 (Online)
Vol. 4, Issue 1, pp: (167-173), Month: April 2016 - September 2016, Available at: www.researchpublish.com

Information Security for Professional Counseling in Organization

[1]Abdikadir Yusuf Mohamed, [2]Yusree Abubaka, [3]Jamaludin Ibrahim

Kulliyah of information and communication technology, International Islamic university Malaysia Gombak, Malaysia

Abstract: **An Information Security Consultant (ISC) provides subject matter expertise and analysis to First Info Tech clients. The role of the ISC is to bridge the gap between high-level security policies, requirements and technical/operational implementation of those requirements. Information security is a never ending game where the playing field consists of computer networks, servers, software applications, users, and data. The information security consultant is the coach with a job of helping organizations (team) balance two separate balls. One ball is ease of access, storing, and transmitting data. The other ball is ensuring information confidentiality, availability, and integrity. In this paper we will discuss much about information security consultant service and we will also highlight information security policy, security awareness, security certified, professional security organization and the business canvas model for information security consultant.**

Keywords: **information security, privacy, policy, counseling, Professional Counselor.**

I. INTRODUCTION

An Information Security Consultant (ISC) provides subject matter expertise and analysis to First Info Tech clients. The role of the ISC is to bridge the gap between high-level security policies, requirements and technical/operational implementation of those requirements.

The growing importance of IT in the business world brings an increased risk with it if the confidentiality, integrity and availability of information systems and networks are not handled correctly. Frost and Sullivan predicts a global increase of 195,000 information security professionals in the next year; an increase of nearly 6% over 2014. Hence we see an increased demand for independent services related to IT security risks and controls and business continuity. With this in mind, our Information Security Consultants ensure identification of IT security risks and implementation of controls during the re-engineering of business processes, IT processes and/or during the implementation of new applications and related infrastructure.

As an Information Security Consultant, you will work for large national and international companies and multinationals. Together with your colleagues you will work on engagements in the field of information security, internet/cyber security and in digital trust services, from a technical as well as from an organizational perspective. You will help clients identify IT-security risks and assist them regarding the implementation of relevant technical and organizational security controls. You will develop IT-security strategies, continuity strategy, processes and architectures in order to ensure the reliable management of processes, services and processing of information.

II. INFORMATION SECURITY AND PRIVACY

[1] Stated that failure of some security mechanisms (hacking, stolen or lost equipment, poor process, and others) has seen many business firms vanish from the market, experience negative impact on stock price, and lose customer trust. Information security includes everything from security policies and analysis to technology and compliance and it involves your whole organization. Professional counselors ensure that clients are provided sufficient information to adequately address and explain the limitations of computer technology in the counseling process in general.

The protection of information assets requires a multi-disciplinary approach that is supported by the government's information security organization. This chapter describes the management structure needed to coordinate information

security activities including required information security activities, who coordinates them and what agreements are required. This coordination applies to internal organizations and to external parties accessing or managing the organization's information assets. The information security organization requires the support of a network of contacts in the information security community to elicit advice, trends and to deal with other external factors [2]

III. SECURITY AWARENESS AND TRAINING

IT Security Consultancy in Malaysia has been studied in this issue that there are many reasons that have prevented organizations and companies form hiring IT security consultants such as the cost and budget, privacy, and so on.

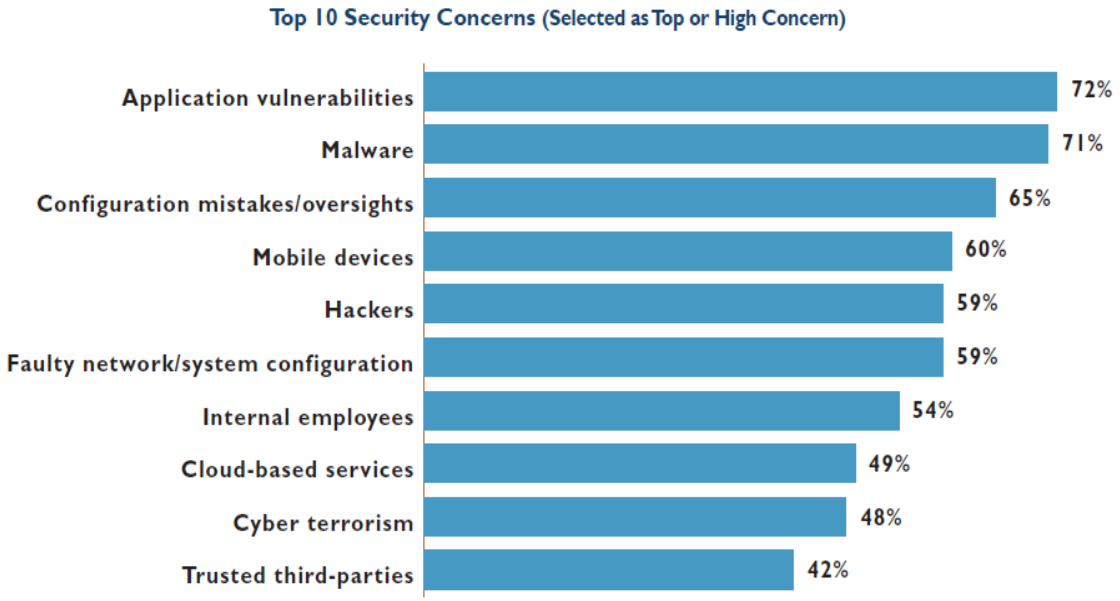

Figure 1: Top 10 Security Concern

From IT security consultancy of Malaysia research, it can be shown that the respondents gave much concern on application vulnerabilities which about 72% similarly with malware 71%. Similar to the diversity of security concerns, the threat techniques employed by attackers and hackers are equally diverse which is 59%. And the lowest concern is on trusted third parties.

Figure2: the important retention of Information Security

From the survey has been discussed about the important of information security in an organization that the consultants need to offer training program to all employee understand the significant of information security and protect all information from unauthorized. It is 61% offer training and 59% paying for professional certification.

IV. CERTIFIED SECURITY

The International Association of Professional Security Consultants has created the Certified Security Consultant designation for professional, independent security consultants. The CSC reflects a high level of professionalism, knowledge and integrity, and will be the recognized standard for Security Consultants. [3]

The CSC demonstrates your depth of knowledge, professional objectivity, skills as a security consultant, and level of integrity. In keeping with the professionalism of the IAPSC, the CSC qualifications are designed to screen out product-affiliated salesmen who call themselves security consultants. The CSC requires a combination of experience and education, as well as independence (professional objectivity) and adherence to a Professional Code of Ethics. No grandfathering of the CSC will occur. The CSC is another wrench in your marketing tool box that separates you from the competition. Our clients recognize the value of certification, especially one that has the backing and credibility of the premier security consulting association.

V. SECURITY POLICY

The Information Security Policy establishes requirements to ensure that information security policies remain current as business needs evolve and technology changes. This policy must be published and communicated to employees and relevant external parties. [2]

The Information Security Policy contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of government services. Secure service delivery requires the assurance of confidentiality, integrity, availability and privacy of government information assets through:

Management and business processes that include and enable security processes;

- Ongoing personnel awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Reporting information security events and weaknesses;
- Creating and maintaining business continuity plans; and,
- Monitoring for compliance.

VI. THE CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)

The Certified Information Systems Security Professional (CISSP) is an information security certification that was developed by the International Information Systems Security Certification Consortium, also known as (ISC). [4]

In an increasingly complex cyber world, there is a growing need for information security leaders who possess the breadth and depth of expertise necessary to establish holistic security programs that assure the protection of organizations' information assets. CISSP is the most globally recognized certification in the information security market. Required by the world's most security-conscious organizations, CISSP is the Gold Standard credential that assures you have the deep technical and managerial knowledge and experience to effectively design, engineer, and manage the overall security posture of an organization. [4] Backed by (ISC), the globally recognized, not-for-profit organization dedicated to advancing the cyber, information, software, and infrastructure security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. [4]

Certification is also a key component of any qualified information security professional's résumé. Certifications fall into two categories – those that measure understanding of vendor security products, such as Microsoft or Cisco, and those that are vendor-neutral and measure a broad understanding of information security policies and processes. Information security has evolved into a profession with recognized best practices so people working at many levels can understand

each other and have confidence in each other's level of knowledge and competency. Certification helps identify those that have reached this level of competency, which can aid HR staff during the recruiting process. [5]

As organizations seek to find qualified individuals to perform the critical task of securing the information infrastructure, the importance of certification, which provides a baseline of knowledge, skills and abilities, continues to increase. According to the 2006 GISWS, 85 percent of hiring managers believe that information security certifications are either somewhat or very important when making hiring decisions. [5]

(ISC)2 certifications are based on the CBK®, a continuously updated taxonomy of information security topics developed and maintained by the organization with the input from its certified members. The CBK establishes a common framework of information security terms and principles that allows information security professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding. [5]

(ISC)2 certifications include the Certified Information Systems Security Professional (CISSP®), considered the "gold standard" in the profession and the first certification designed to validate the knowledge, skills and abilities of information security professionals and managers and to be accredited under ANSI/ISO/IEC Standard 17024. The CISSP is a credential for information security managers with responsibility for strategic security planning and writing and enforcing policies. Candidates must have at least five cumulative years of relevant work experience in two or more of the 10 domains of the CISSP CBK and receive an endorsement of their application by a CISSP or other (ISC)2 credential holder. For veteran professionals, there are also CISSP concentrations in management, architecture and engineering. [5]

Another (ISC)2 certification is the Systems Security Certified Practitioner (SSCP®) for those that enforce implementation of, monitor and maintain requirements and policies for information security, as well as for IT or physical security personnel who encounter information security issues on a regular basis. [5]

A vendor-neutral information security certification ensures an organization's security staff can demonstrate a broad knowledge in information security and professional judgment, has professional access to a network of global industry and subject matter/domain experts, and is committed to continuing professional education to maintain certification. In many cases, salary increases often result immediately after an employee earns his/her CISSP or other vendor-neutral certification.

Other organizations offering security certifications include the SANS Institute, validating technical understanding of security issues, and ISACA, validating security auditing functions and risk assurance. [5]

VII. PROFESSIONAL COUNSELOR

Professional counselors provide a readily visible notice advising clients of the identities of all professional counselor(s) who will have access to the information transmitted by the client. Here is the BMC of business for security Consultant Company.

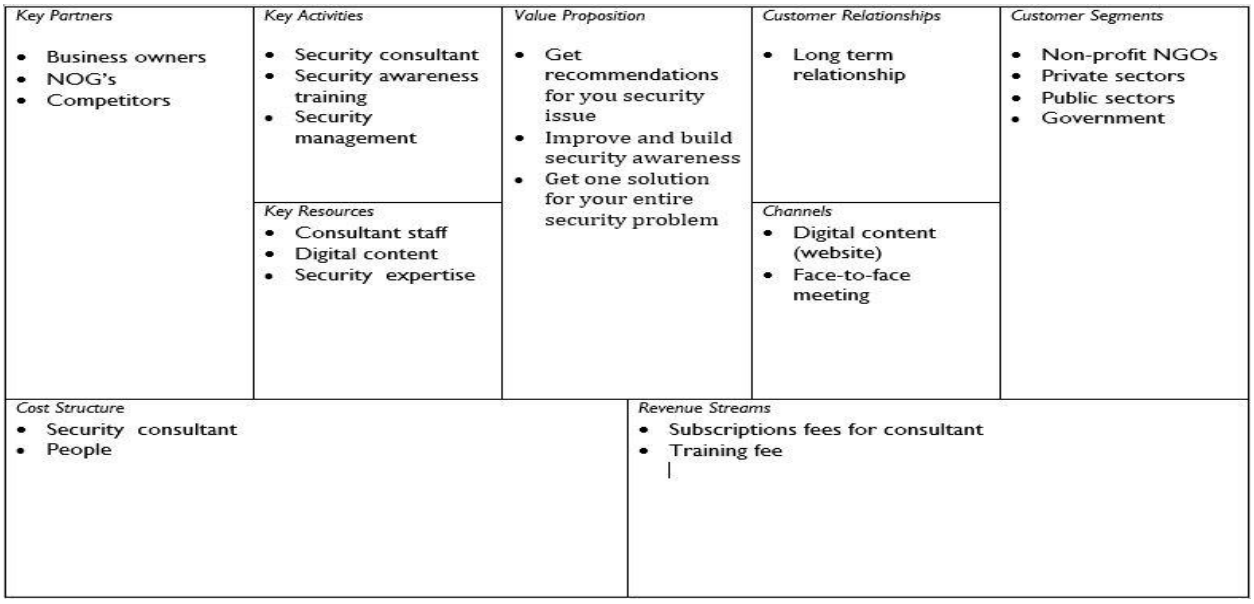

Figure 3: BMC for Consultant Company

VIII. SECURITY PROFESSIONAL AND ORGANIZATION

Security professional is a key important role to play and lead all performance and functions in an organization. According to Whitman and Mattord identified that the roles of information security professionals are aligned with the goals and mission of the information security community of interest. Therefore, IT professional have to have wide knowledge and experience such as IT management and skilled professional in system design, programing, network and other related skills.

The international standard for information security management, ISO/IEC 17799, describes information security as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities." If not mitigated, these threats can destroy a company's reputation, violate a consumer's privacy, result in the theft or destruction of intellectual property, and, in some cases, endanger lives. [5]

Twenty years ago, the field of information security was in its infancy. Many companies did not take threats to their infrastructure seriously. For those companies that did, the majority of people responsible for protecting information assets did not have a formal background or education in the field and obtained their experience in information technology or related disciplines, transferring into information security only as the need arose. Information security professionals frequently reported to someone in IT and did not carry much weight with upper management. [5]

Today, driven by increasing regulations and the desire to maximize global commerce opportunities, protecting information assets has become one of the most important functions within any organization, public or private. For this reason, organizations increasingly rely on information security professionals to implement a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, and continually monitored, reviewed and improved to ensure that the specific security and business objectives of the organization are met. [5]

The 2006 Global Information Security Workforce Study (GISWS), sponsored by (ISC)2 [pronounced "ISC-squared"], reported that the number of information security professionals worldwide in 2006 was approximately 1.5 million. This figure is expected to increase to slightly more than 2 million by 2010, displaying a compound annual growth rate (CAGR) of 7.8 percen from 2005 to 2010, compared to 4.6 percent of projected growth in the number of IT employees globally in the same timeframe. [5]

After surveying more than 4,000 information security professionals worldwide, the GISWS indicated that more than 37 percent of respondents work for organizations with annual revenue of one billion or more, and more than 62 percent work for organizations with at least 1,000 employees. Often, information security professionals are found in the greatest numbers in organizations whose mission is to safeguard critical infrastructure, such as government defense agencies, telecommunications and the financial industry. Because the profession is still relatively new, many small to medium businesses do not have a security department at all. [5]

A common misconception of information security is that is a function of IT. While it may have begun in the IT department, information security is a highly specialized function, and its influence has grown exponentially in recent years as executives have seen both the necessity for and return on investment in information security. Today, information security professionals often have a seat in the executive boardroom, enabling them to make valuable recommendations during the earliest stages of business initiatives. [5]

Another common misconception is that the information security professional's job functions are similar to those of IT professionals. In fact, information security responsibilities can run the gamut, from risk management to computer forensics. Each responsibility can require vastly different skill sets and experience beyond the "bits and bytes" of IT. [5]

IX. INFORMATION SECURITY CONSULTING SERVICES

Frontier [6] offers a wide range of consulting services to address the complete spectrum of information security requirements of enterprises through the complete information life-cycle.

A. Assess:

- Enterprise Security Audit: To audit against international standards and frameworks and report on the compliance of processes, applications, technical security and user awareness.

- Vulnerability Assessments: Assessment of Technical Controls and Prioritize the Implementation of Controls. Establish an effective Technical Vulnerabilities Reduction Metrics
- Penetration Testing: Our Proof of Concept documents add value to the Customers in taking immediate necessary action to ensure that the Systems are hardened.
- Application Security Assessment: To check for the security of the applications as per the OWASP guidelines. Evaluate the portfolio of applications on web connected devises and each layer of application logic for potential vulnerabilities.
- Compliance Audit: Compliance audit against ISO27001, GLBA, HIPAA, SAS 70, SOX, SEBI Clause 49, RBI Guidelines and other international security standards/ guidelines
- Security Process Review: To check for the adequacy and compliance of the security policies, procedures and standards.

B. Design:

- BCP/ DRP Consulting: Ensuring Business Resilience and providing immediate, accurate and measured response to emergency situations. Facilitate the recovery of Critical Business Process to reduce the overall negative impact on Business and revenue
- ISO/IEC 27001:2005 Consulting: Top Driven and Consistent approach to address Compliance and Risk Management. Establishes Information System/Process Assurance. Frontier's Information Security Consulting follows established methodologies to enable Organization get Certified to ISO 27001 and sustain the ISMS certification.
- Security Policy Design: Designing and Developing Information Security Policies, procedures, standards and guidelines after a detailed study of the business process and security requirement.
- Network Security Architecture: Study the existing network design, network and security device positioning and suggest/ recommend redesign of the network taking into consideration confidentiality, integrity and availability of information and ease of network and security administration

C. Deploy:

- Security Policy Deployment: To implement organization wide information security policies and procedures to ensure that corporate information and assets are protected from unauthorized access, disclosure and modification.

D. Manage:

- Enterprise Security Management: To manage the security process and controls organization wide 24/7 and provide real time alerts and recommendations thereby ensuring proactive security measures and preventing disruption of service
- Security Product Management: To manage the networking & security devices (servers, routers, firewalls, IPS, UTM's etc) organization wide 24/7 and provide real time alerts and recommendations thereby ensuring proactive security measures and preventing disruption of service.
- Education & Training: Customized sessions focusing on security concepts, policies & procedures for organizations. Interactive

X. CONCLUSION

Several organizations have adopted Information Security Governance as a holistic approach towards systematic enterprise risk management. This helps ensure that information security is aligned with the company's strategic goals and meets the organizational objectives. We discussed in this paper the important of having information security consultant in organization and how organization get benefit from information security consultant and improve their business goals.

REFERENCES

[1] Acquisti, A., Friedman, A. & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study, Proceedings of the 5th Workshop on the Economics of Information Security, 2006; Retrieve on 10 March 2016 from http://weis2006.econinfosec.org/prog.html

[2] Columbia, B. (2012). Information Security Policy. Security Classification: PUBLIC, 5-8.

[3] CSC. (n.d.). Becoming a Certified Security Consultant. Retrieved from iapsc.org: iapsc.org/about-us/certification/

[4] ISC2. (2016). CISSP. Retrieved from www.isc2.org: https://www.isc2.org/cissp/default.aspx

[5] ISC. (n.d.). Securing the Organization: Creating a Partnership Between HR and Information Security. White Paper, 2-6.

[6] FRONTIER'S. (n.d.). Information Security Consulting. Retrieved from frontier.in: http://www.frontier.in/services/information_security_consulting.html

[7] Whitman, M., & Mattord, H. (2011). Principles of information security. Cengage Learning.

[8] Suby, M. (2013). The 2013 (ISC) 2 Global Information Security Workforce Study. Frost & Sullivan in partnership with Booz Allen Hamilton for ISC2.

[9] Adam, M. E., Rahman, M. A., Barzak, O. M., Salah, M. A., & Ibrahim, J. B. (2013). IT Security Consultancy in Malaysia: Hindrances and Impacts. Middle East Journal of Business, 8(3), 17-22.

[10] Bimrose, J., & Barnes, S.-A. (2010). Labour Market Information (LMI), Information Communication Technologies (ICT) and Information, Advice and Guidance (IAG): the way forward. London: UKCES. Retrieved from http://www.ukces.org.uk/upload/pdf/424721%20LMI%20report_2.pdf.