SWOT Matrix Enhancement for Online Protection of Personal Information

Da-Yu Kao

Department of Information Management, Central Police University, Taiwan

No. 56, Shujen Rd., Takang Village, Kueishan Hsiang, Taoyuan County, 33304, Taiwan

camel@mail.cpu.edu.tw

Abstract

Rapid improvements in computing technologies have increased concerns about information privacy. Protecting online information for many organizations may be an impossible task. SWOT is as an acronym for strengths, weaknesses, opportunities, and threats. Reviewing SWOT analyses and its matrix strategies gives a broad overview of the legal and practical issues. The proposed privacy enhancement based on SWOT analysis and its matrix development improves online information privacy. The following strategies are applied to solving personal information processing problems: (1) plan new projects; (2) deploy team leadership; (3) follow suitable procedures; and (4) apply new technologies. Recommendations for privacy and security good practices for information managers are provided. We have applied these strategies to Taiwan government agencies many times, and it has been endured real testifying.

Keywords: SWOT analysis, SWOT Matrix, Information Security, Personal Information Protection

1. Introduction

Information technology is bringing together people from around the country and around the world. Personal privacy is being increasingly eroded as modern technologies evolve [20]. In fact, many groups, individuals and firms feel that they are losing control over their own information and information that refers to them.

1.1 An Online Change in Personal Information Privacy

Personal information is readily available on the internet. Common definitions for privacy protection include being able to control release of information about oneself to others and being free from intrusions or disturbances in one's personal life [10]. Furthermore, the term "privacy" has many meanings, each of which depends on the context in which it is used. Among the many information technologies that increasingly impact privacy, the internet offers many possibilities to collect, process, and distribute personal data. Privacy protection, often a vague concept, is the ability to control the acquisition and use of one's personal information. Many countries recognize the right to privacy [7]. Unfortunately, many users are oblivious about online privacy and accept the fact that their online privacy will be

compromised.

As human activities have migrated to the internet, the number of information systems is increasing daily. Online shopping is becoming a major economic force; as such ecommerce must strike a balance between privacy and security. Online activities, including electronic cash and mobile payments, are proving superior to conventional monetary instruments [3]. However, significant security/privacy problems have emerged. The concern about the collection of personal information in various contexts is widespread. Rapid improvements in computing technologies have increased the concern about personal information privacy. Once one shares personal information, control over this information is lost. Different parties may have opposing interests and views about individual information. For many, online privacy is related to human dignity, which can be compromised by the proliferation of personal information.

1.2 An International Trend in Personal Information Protection

Many organizations collect massive amount of data about individuals. Media reports show that citizens are increasingly concerned about information protection and their rights. Privacy concerns have resulted in many laws and regulations. Dealing with potential privacy invasions proactively could preclude government interventions that tighten controls over what can be done with an individual's personal data. Personal information incudes name, birthdate, Identification card numbers, passport number, personal characteristics, fingerprints, marital status, family composition, education, occupation, medical records, medical treatments, genetic code, sexual practices, health examination findings, criminal records, financial status, social activities and other information that may be used to identify a person, both directly and indirectly [19]. Privacy rules differ markedly among countries, and these differences threaten to hamper the ability of international organizations to engage in transactions on the internet without risk of incurring penalties. In 1980, the Organization for Economic Co-operation and Development (OECD), a global group, published guidelines to harmonize the collection and use of personal information by governments and private organizations [10]. Widespread concerns were the impetus for new legislation. In 1998, the U.S. Congress enacted the Children's Online Privacy Protection Act to regulate the online collection and use of personal information about minors. Many interactions between consumers and organizations have changed significantly [18]. The USA Federal Trade Commission released a report on a preliminary framework for protecting consumer privacy; this framework had three major elements: (1) organizations should integrate privacy concept into their regular operations; (2) provide choices to consumers in a simpler, more streamlined manner; and (3) improve the transparency of all data practices [9].

Widespread privacy concerns gave impetus to the development of new privacy legislation. Laws and regulations in the USA, Australia, Canada, Hong Kong, or Taiwan have been extended to protect consumer credit reports, electronic communications, agency records, education records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, and customer

financial information [17]. In 2010, Taiwan's Personal Information Protection Act was amended to cover the collection, process, use and transmission of personal information and thereby protect personal privacy]. However, no comprehensive statute protects online personal information. Online information privacy is important and people desire control over their personal information and its collection, use, and transmission. Privacy protection relies on both legislation and self-regulation [11]. An organization may have personal information about individuals, and its collection and use must be for legitimate purposes. To balance the rights of organizations to gather data with the rights of an individual, the process of handling personal information should be regulated to protect personal data. The shift to a digital environment has altered our understanding of privacy protection [6]. First, it alters our understanding of the digital context in which incidents occur and the evidence where potential artifacts are stored. Second, our understanding facilitates new criminal offenses. Third, our understanding produces significant changes in managing online threats. Fourth, our understanding presents new challenges to existing legal processes. This study discusses the online protection of personal information based on SWOT analyses and its matrix strategies. The internal/external factors of personal information protection are analyzed. The following strategies are proposed and applied to solving personal information processing problems: (1) plan new projects; (2) deploy team leadership; (3) follow suitable procedures; and (4) apply new technologies. We have applied these strategies to Taiwan government agencies many times, and it has been endured real testifying.

The remainder of the paper is organized as follows. The literature review is given in Section 2. Section 3 presents a practical SWOT analysis on online privacy issues. The multi-faceted SWOT analyses address strengths, weaknesses, opportunities, and threats. Section 4 presents the SWOT matrix strategies for online privacy protection. Finally, conclusions are provided in Section 5.

2. Reviews

Changes in individual privacy rights can be understood in the context of a balance between government needs and civil liberties. Online researchers typically exploit digital data to discover knowledge embedded in individual records. The following subsections discuss the questions that are generally the most important to internet users.

2.1 Trust Relationship and Personal Information Protection

An organization can develop consumer trust and make investment decisions about technology infrastructure using a well-designed information policy. The cyberspace infrastructure facilitates easy and inexpensive collection of personal information. Effective privacy professionals generally combine their instincts and sound processes to minimize privacy breaches [18]. Many opinions and theories exist about privacy protection worldwide. Some commentators have proposed that laws should grant individuals a property right to their personal data [20]. Such a property right would enable individuals to trade and barter with their personal information. The ability to gather information on individuals is largely due of

advances in online technology. Having information system managers and professionals understand issues surrounding personal information protection is necessary to protect the rights of those about whom they collect data.

When a consumer accesses a consumer website and makes a purchase, he/she gives his/her credit card and address information. A number of systems and networks are involved, such that many security vulnerabilities exist. While consumers demonstrate their trust by making a purchase, these uses of their digital data potentially affects the organization-individual relationship, which is often rooted in high levels of trust [12]. Trust, respect, and personal integrity are strongly related to online privacy. Implementing security components may prevent disclosure of information to unauthorized individuals. However, if individuals do not believe an organization will protect their personal information, they will likely withhold or ask the organization not to record their information. With the proliferation of data warehousing and data mining, the likelihood that organizations will misuse personal data will generally increase. To foster confidence in information systems, organizations should maintain secure information systems. As information technology security is of primary importance in many societies [13], information systems should be reassessed periodically. Moreover, organizations should act in a timely and coordinated manner when responding to security breaches.

2.2 SWOT Analysis and Matrix Strategies

The SWOT analysis was credited by Albert Humphrey [16]. The SWOT analysis is an analytical process used in business environments to identify the strengths, weaknesses, opportunities and threats an organization faces [16]. Recognizing strengths and weaknesses before tackling opportunities or threats is best before analysis. A strategic plan for auditing an organization and its environment helps an organization focus on the status of their information protection, identify areas for development, and develop future management strategies. The SWOT analysis can discusses the internal/external factors to generate appropriate strategies. The objective of this matrix is to identify effective strategies [8]. This matrix identifies current conditions and plans methods that are necessary for strategic observation. Although there is no overarching right to privacy, various laws protect an individual’s personal information, such as Taiwan Personal Information Protection Act in 1995 (Amended in 2010) [19], Canada Personal Information Protection and Electronic Documents Act in 2000 (Amended in 2011) [4], and Australia Privacy Law in 2008 (Amended in 2013) [2]. They will outline various IT strategies, and identify the general principles of security policies. An IT strategy is an action plan that determines technology use within an organization. This strategy should be aligned with business strategies. This study attempts to offer an alternative to SWOT analysis, and applies practical and effective strategies for organizations.

Table 1: The SWOT Analysis on Privacy Enhancement

Factors	Helpful	Harmful
Internal Factor	Strengths: Build a Strategic Plan - Skilled or experienced staffs. - Current or superior IT. - Good or known reputation. - Strong financial resources. - Efficient or up to date equipment. - Sufficient financial resources to fund any positive changes. - A proper handling process in personal information protection.	Weaknesses: Fail to Change Management Processes - Unskilled or inexperience staffs. - Past or inferior IT. - Bad or unknown reputation. - Inefficient or outdated equipment. - Insufficient financial resources to fund any positive changes. - An improper handling process in personal information protection.
External Factor	Opportunities: Take a Constructive Attitude - Stable competition - Superior knowledge in R&D department. - High innovative skills to fulfill customers' needs. - Broadband internet service. - Tight regulations. - Good relationships with customers, suppliers, and employees.	Threats: Increased the Number of Potential Vulnerabilities - Increasing competition. - Inferior knowledge in R&D department. - Low innovative skills to fulfill customers' needs. - Non-broadband internet service. - Loose regulations. - Poor relationships with customers, suppliers, and employees.

3 SWOT Analysis on Online Protection of Personal Information

The patchwork of laws and regulations does not ensure online privacy. The SWOT analysis for privacy enhancement in Table 1 analyzes the pros and cons of various factors related to helpful/harmful decisions. Table 1 also presents a SWOT analysis of internet privacy, which can be divided into two factors [15, 20]: internal factor and external factor. Privacy analysis is analyzed in the following phases [3]: build a strategic plan; fail to change management processes; take a constructive attitude; and increase the number of potential vulnerabilities. These steps provide an informal analysis of privacy properties, and attempts to enhance privacy for innovative online services.

3.1 Internal Factor

Privacy and security are critical problems. Without both, consumers will not shop at a site, nor can sites function effectively. Security mechanisms can control network effects; however, these mechanisms are largely imperfect. Organizational policies for the internal factor of personnel, techniques, or equipment may play important roles in cyber security. The "cat-and-mouse" studies of security experts and hackers elucidate admittedly murky areas. Strengths and weaknesses can be applied to characterize internal factors. The internal factors of supporting any positive changes encompass staffs (skilled or unskilled), IT (current and past), an organization's reputation (good or bad), equipment (efficient or inefficient), financial resources (sufficient or insufficient) and handling process (proper or improper) [8, 15, 20].

(1) Strengths: Build a Strategic Plan

Internet users are vulnerable to privacy breaches, including hacking, identity theft or online exploitation. An organization should build a strategic plan to determine the current

decisions that will create best tomorrow. Strengths can be anything that is favorable for an organization [8, 15, 20]:

- Skilled or experienced staffs.
- Current or superior IT.
- Good or known reputation.
- Strong financial resources.
- Efficient or up to date equipment.
- Sufficient financial resources to fund any positive changes.
- A proper handling process in personal information protection.

(2) Weaknesses: Fail to Change Management Processes

Weaknesses may hinder problem solving capability. Weaknesses are core capabilities of an organization where competitors have an advantage, which customers value. In addition to technical factors, issues are related to budgets, managerial support, and staff. Privacy invasions can be ubiquitous and invisible. Organizations should involve individuals in the use of personal information and consent should be given before an individual's data is collected, processed, and used. Vulnerabilities can be eliminated or minimized by strengthening security. Recognizing weaknesses requires that individuals are honest and realistic. The following is list of example weaknesses [8, 15, 20]:

- Unskilled or inexperience staffs.
- Past or inferior IT.
- Bad or unknown reputation.
- Inefficient or outdated equipment.
- Insufficient financial resources to fund any positive changes.
- An improper handling process in personal information protection.

3.2 External Factor

While the internet plays a critical role, most users are not well informed about the potential impact of collected personal data. Many organizations are reliant on information about potential customers. Personal information is routinely collected for profiling, tracking and targeting. When a user makes a purchase, browses the internet, or responds to a survey, their identity is typically revealed. Consumers generally fear the loss of their financial data, and websites fear break-ins. Websites and consumers must explore security vulnerabilities and evaluate potential risks. Opportunities and threats are external factors. The external environment also determines whether an organization can improve its performance and profits. External factors of influencing any environments encompass competition (stable or increasing), R&D (superior or inferior), innovative skills (low or high), internet service (broadband or non- broadband), regulations (tight or loose), and relationships (good or poor) [15, 16, 20].

(1) Opportunities: Take a Constructive Attitude

Constructive attitudes attract people, as poor attitudes repel them. Much can be achieved with constructive attitude. If one decides on to concentrate on the positive, a good attitude is

likely. While the privacy and security of personal information remain concerns, several technological approaches have been proposed to safeguard personal privacy. The on-line identity of IT can be used to track and analyze vast amounts of data. Acquiring a technical capability is becoming easier with increasingly sophisticated tools and available guidance. Effective solutions should necessarily encourage people to have a constructive attitude regarding long-term privacy and security. The implementation of broadband internet increases the likelihood of instantaneous service. The external factors of a development plan must to be addressed by an organization. Opportunities for an organization can be influenced to achieve his success [15, 16, 20]:

- Stable competition
- Superior knowledge in R&D department.
- High innovative skills to fulfill customers' needs.
- Broadband internet service.
- Tight regulations.
- Good relationships with customers, suppliers, and employees.

(2) Threats: Increased the Number of Potential Vulnerabilities

The amount of high-value information that stored and communicated in cyberspace is increasing. Organizations generally use online systems that reduce costs and improve efficiency and quality. However, the proliferation of information technologies increases the number of potential vulnerabilities. Vast quantities of personal data in a system often become available for mining valuable knowledge. This also enhances the incentive for cybercrime for profit or political advantage. Because transferred data is not encrypted on the internet, everything sent or received is in plain text. A hacker can gain unauthorized access to computers, disable networks, intercept traffic packets or destroy information systems with commonly available applications.. Weaknesses can be immediate threats. An online system may be a vulnerably for an organization. Hackers may use inexhaustible programs to free-ride on others' computers. Programs that assist is online attacks include network scanners, packet sniffers, password crackers, buffer overflows. Threats are typically the following weaknesses [15, 16, 20]:

- Increasing competition.
- Inferior knowledge in R&D department.
- Low innovative skills to fulfill customers' needs.
- Non-broadband internet service.
- Loose regulations.
- Poor relationships with customers, suppliers, and employees.

4 SWOT Matrix Development for Online Protection of Personal Information

Cyber threats are becoming increasingly sophisticated and targeted. Assessing security risks can minimize vulnerability to cyber threats [1]. Online organizations that provide consumers with products or services should have privacy as their top concern. Although many

organizations manage consumer information responsibly, some treat recklessly and do not adequately respect privacy. When designing policies that ensure privacy and enhance security, the relative roles played by government versus private initiatives are often considered [3]. Organizations should adopt responsible approaches to protect themselves online. Security policies must account for human behavior by keeping alternatives simple and cheap. When problems are well defined, policy makers can craft effective laws. This section discusses the necessary strategies in SWOT analysis needed to make appropriate decisions about specific circumstances or business requirements. To develop workable strategies, SWOT factor analyses can be constructed in Table 2 [8, 16]. In Figure 1, Strategists can use this matrix to create and introduce the following four strategies on privacy enhancement: Strengths Opportunities (SO), Weaknesses Opportunities (WO), Strengths Threats (ST), and Weaknesses Threats (WT) strategies. An organization's strategy should be evolving and changing to keep pace with internal and external changes. A key skill for any online protection enhancement tasks is the ability to help an organization clarify these strategies and develop specialized services on a segmented basis as required.

Table 2: The SWOT Matrix Strategies and Guidelines on Privacy Enhancement

SWOT Matrix	**(Opportunities) Take a Constructive Attitude**	**(Threats) Increased Numbers of Potential Vulnerabilities**
(Strengths) Build a Strategic Plan	SO Strategies: Plan New Projects (1) Implement an Insurance Policy for Security (2) Retain Passion for Innovation (3) Prevent Data Misuse	ST Strategies: Deploy Team Leadership (1) Develop a Security Culture through Staff Education (2) Understand the Cyber Threat Environment (3) Maintain Team Collaboration
(Weaknesses) Fail to Change Management Processes	WO Strategies: Follow Suitable Procedures (1) Be Prepared to Respond to a Security Incident (2) Implement Necessary Requirements	WT Strategies: Apply New Technologies (1) Use Ongoing Processes to Secure Us against Threats (2) Make Links between the Virtual Identities of an Individual

Traditionally the SWOT Matrix strategies have recognized four key strategies: SO, ST, WO and WT. These strategies construct a hierarchy management pyramid with geometric proportions illustrating the strong interdependent relationship between these strategies. In Figure 2, the privacy enhancement hierarchy of management pyramid is proposed and discussed in the following perspectives: visionary policy, team collaboration, control

procedure, and daily work. It is a graphic aid to illustrate that the IT success of privacy management is measured by the team's ability to manage the online system. The expected results are produced while an organization can manage its strategies, processes and perspectives. Figure 2 also explores a set of related actions that managers may take to increase their organizations' performance on privacy enhancement. This hierarchical structure can promote developing employees as specialists. Employees may narrow their field of focus and become experts in IT privacy protection.

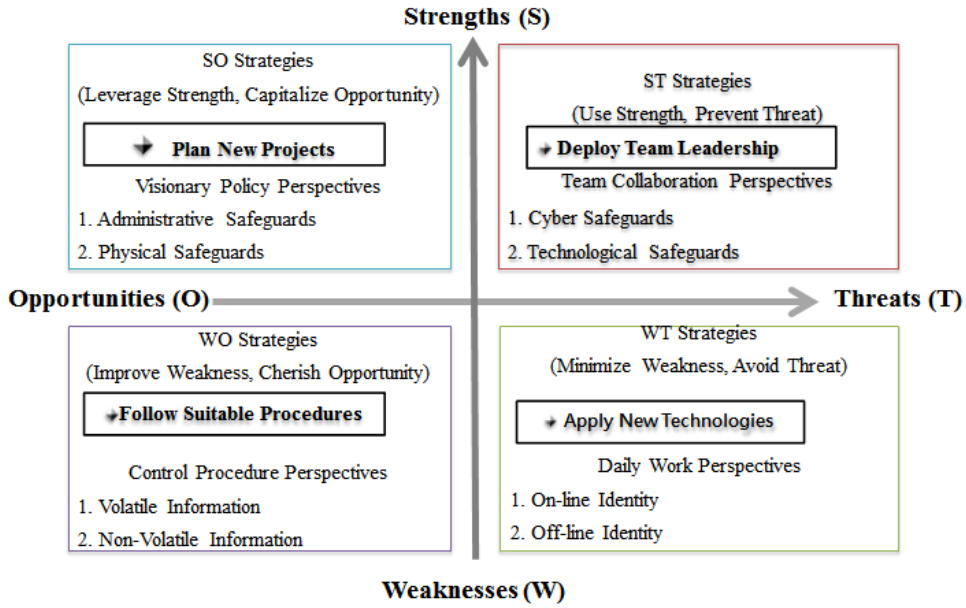

Figure 1: The SWOT Matrix Strategies and Perspectives on Privacy Enhancement

4.1 SO Strategies

The SO strategies use strengths to take advantage of opportunities, and leverage internal strengths to capitalize on external opportunities.

4.1.1 SO Strategies: Plan New Projects

Based on preliminary experience, the following guidelines were developed [7, 16]:

(1) Implement an Insurance Policy for Security

Effective security can eliminate the direct costs of lost productivity and indirect costs of reputation loss.

(2) Retain Passion for Innovation

A security incident may provide opportunities to exchange views. To safeguard an organization, one should question the protection ways and develop ways to explore issues.

(3) Prevent Data Misuse

Personal privacy is under siege online and offline. Government intervention has increased the responsibilities of organizations collecting personal information, and should prevent data misuse.

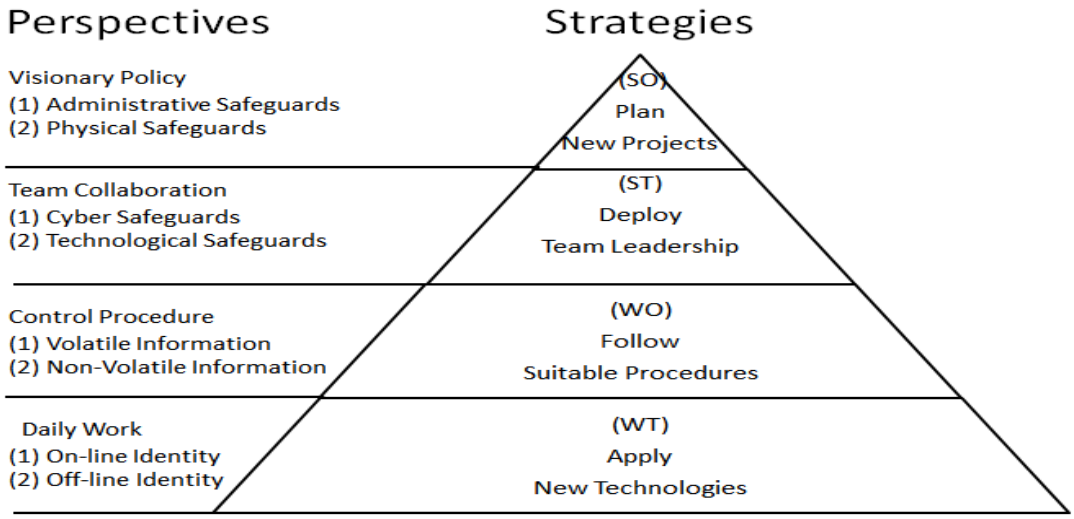

Figure 2: The Privacy Enhancement Hierarchy of Management Pyramid

4.1.2 Visionary Policy Perspective

A visionary plan intends to achieve an organization's goals, fulfill its mission, and succeed in reaching its strategic vision. Any organization that collects data may proclaim that they are concerned with consumer privacy and then proceed to explain in copious rhetoric how their data collection process, data use, and data transmission are carried out. An appropriate online privacy protection solution is needed to enhance online privacy. Privacy professionals must assist organizations in objectively developing privacy and security policy that meets risk management and legal compliance goals. Risk management requires that organizations develop policies for administrative or physical safeguards that ensure appropriate collection and use of personal information [11, 14].

(1) Administrative Safeguards

Increasing administrative surveillance has diminished individual privacy threats and adversely impacted many aspects of life. The need to block viruses and the fear of hackers are prompting organizations to focus on core competencies and deploy appropriate countermeasures. Administrative safeguards include attending security training seminars, executing confidentiality agreements, or enforcing security policies. An organization can develop a plan for threat prevention, sufficient resources, and prioritize activities. The plan should include prevention measures and emergency response procedures.

(2) Physical Safeguards

In recent years, law enforcement agencies have been given broad surveillance powers in response to perceived threats. Physical safeguards include the deployment of routine surveillance, retaining records in a secure area, or access control to personal information areas.

4.2 ST Strategies

The ST strategies use strengths to reduce threats, and use internal strengths to avoid external threats or prevent adverse effects.

4.2.1 ST Strategies: Deploy Team Leadership

An organization should use these strengths to reduce the effects of external threats via strategy implementation. Some guidelines are as follows [8, 17].

(1) Develop a Security Culture through Staff Education

Being aware of cyber threats can reduce risk that valued information will be stolen. Effectively trained staff can comprise a strong security culture.

(2) Understand the Cyber Threat Environment

The guideline focuses on providing organizations with an understanding of cyber threats, and it is used to develop information security policies.

(3) Maintain Team Collaboration

To secure an organization against threats, one should respect each individual and listen to opposing opinions.

4.2.2 Team Collaboration Perspective

Team collaboration can used to complete a task faster than when performed by an individual. Collaboration can be used to share knowledge, generate productive conversations in cyber safeguards [13].

(1) Cyber Safeguards

Cyber safeguards may limit those with access to personal information or be applied to conduct privacy impact assessments of information systems, technologies or programs that involve personal data. If attention is inadequate, psychological harm may result, including a loss of trust, or the time consumed to remedy privacy breaches increases.

(2) Technological Safeguards

Numerous examples exist of disclosure of personal data that has harmed individuals. Technical safeguards include implementation of auditing systems, institution of strong authentication measures, and design of privacy systems. Technological advances have expanded the number of methods by which an organization may engage in surveillance of individuals.

4.3 WO Strategies

The WO strategies overcome weaknesses by taking advantage of opportunities, and improve internal weaknesses by capitalizing on external opportunities. Courts have begun to take steps to create special laws for cybercrimes.

4.3.1 WO Strategies: Follow Suitable Procedures

The current criminal procedure often makes little sense. Investigations and prosecutions of cybercrime require many tools to collect sufficient evidence, which tends to be fragile, volatile, and easily manipulated. An organization can use external opportunities when applying new technologies to eliminate internal weaknesses. Some guidelines are as follows [12, 16].

(1) Be Prepared to Respond to a Security Incident

Many organizations do not take information security seriously until they are compromised.

(2) Implement Necessary Requirements

The control procedure provides a set of detailed controls in suitable environments, and helps organizations adhere to information security policies. A set of control procedures can be implemented to mitigate risks to their information and systems.

4.3.2 Control Procedure Perspective

Adequate privacy regulations require in-depth understanding of how the distribution of personal data affects society. The many forensic professionals in law enforcement and private practice know that the tradition of first pulling the plug on a PC under examination is an outdated approach that can destroy valuable evidence [5]. Control procedures provide reasonable assurances of management control of volatile and non-volatile information [13, 15].

(1) Volatile Information

Volatile memory is sometimes referred to as dynamic because it can change and be changed [3]. Forensic computing specialists are experienced in quarantining, extracting and evaluating volatile evidence from computers and communication devices. Live forensics provides for the collection of digital evidence that has a life expectancy. If people cannot properly handle it, digital evidence may be lost forever. The most important evidence to be gathered today and for the foreseeable future exists only as volatile data within RAM. Some samples of volatile information are listed below.

- Cache and register content in the CPU.
- Content in the routing table, ARP cache, process table, kernel statistics.
- Content in the memory.
- Content in the temporary file system / swap space.

(2) Non-Volatile Information

Non-volatile forms of memory are sometimes referred to as static memory. Static memory can be stored and is stable. A computer has short- and long-term memories [5]. The ability to reliably collect volatile evidence in a forensically sound manner has effectively rendered the practice of “pulling the plug” obsolete. Some samples of non-volatile information are as follows.

- Hard disk data.
- Remotely logged data.
- Archival media data.

4.4 WT Strategies: Daily Work

The WT strategies, the most defensive position on the matrix, minimize weaknesses and reduce threats.

4.4.1 WT Strategies: Apply New Technologies

The goal of WT strategies is to minimize weaknesses and avoid threats. Deploying team leadership and leveraging resources may be necessary. Some guidelines are as follows [5, 14].

(1) Use Ongoing Processes to Secure Us against Threats

No silver bullet exists for information security. As cyber-attacks become more

sophisticated, so do information security techniques and processes. To secure an organization against threats, appropriate security governance, clearly defined policy, user education and third party assessments are all vital.

(2) Make Links between the Virtual Identities of an Individual

An individual on the internet can have more than one identity. Online activities have privacy risks. Information technology can be used to split on-line and off-line identities or make links between the identities of an individual for any practical application.

4.4.2 Daily Work Perspective

Information is collected from surveillance data reported daily, weekly, monthly and at a six-month review. In organizations that have problems (e.g., possible privacy breach, or download of web files), the routine surveillance report can be analyzed from daily auditing records and abnormalities monitored. The on-line and off-line activities of an individual's identity engender different privacy concerns and economic implications [12, 13].

(1) On-line Identity

The transaction of on-line identity is often associated with cookies, IP addresses or timestamps that track customer behavior across the internet. An on-line identity might carry information about an individual's tastes, browsing behavior, purchase history, or personal evaluation of a product.

(2) Off-line Identity

The off-line identity is the actual identity of an individual, as revealed by credit card numbers and social security numbers.

5. Conclusions

Privacy is should be ensured for individuals in all societies. The privacy violation on the internet is a significant problem and internet users have a right to adequate privacy. This study examines some efforts to protect personal information, and provides a brief SWOT analysis of privacy enhancement via an innovative online service. Strong security measures require may resources. This study addresses privacy violations while using the internet. It also explores the concept of privacy protection. The internet has provoked much discussion about how to investigate crime and enforce criminal law. It has led to an increasing emphasis on new systems of law enforcement. Privacy is well worth fighting for since it a fundamental right in a democratic society. The proposed solution attempts to meet and discuss developments in online activities for practitioners and policy makers of organizations. We hope these analyses will encourage the development of efficient privacy practices over time through aggressive public and private participation.

Acknowledgements

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 103-2221-E-015-003-.

Reference

[1] Australia Government (Department of Defense), “2014 Australian Government Information Security Manual Principles”, 2014: http://www.asd.gov.au/publications/Information_Security_Manual_2014_Principles.pdf。

[2] Australian Law Reform Commission, “For Your Information: Australian Privacy Law and Practice (ALRC Report 108),” 2014: http://www.alrc.gov.au/publications/report-108。

[3] Baddeley, M., ”A Behavioral Analysis of Online Privacy and Security,” 2014: http://www.econ.cam.ac.uk/dae/repec/cam/pdf/cwpe1147.pdf。

[4] Canada Minister of Justice, “Personal Information Protection and Electronic Documents Act 2000,” 2014: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html。

[5] Casey, E., *Handbook of Digital Forensics and Investigation*, Burlington, Academic Press, 2010.

[6] Cotter, A. M., *Law Society of Ireland - Information Technology Law*, Cavendish Publishing Limited, 2004.

[7] Ekberg, A. G. S., "Invasion of Privacy: Spam - One Result of Bad Privacy Protection," 2014: http://www.essays.se/essay/fe577888cf/。

[8] Farhangi, A. A., Far, M. S. and Danaei, A., “Development SWOT Matrix for Strategic Planning in Media Organizations,” *International Journal of Business and Commerce*, 2012, 1, (5), pp.1-12.

[9] Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,” *A Preliminary Federal Trade Commission Staff Report*, December 2010.

[10] Stevens, G., "Privacy Protections for Personal Information Online," *Congressional Research Service Report*, April 2011.

[11] Gross, G., “FTC Sticks With Online Advertising Selfregulation,” *IDG News Service*, Febrary 2009.

[12] Jewkes, Y. and Yar, M., *Handbook of Internet Crime*, Willan Publishing, 2010.

[13] Jonathan, C., *Principles of Cybercrime*, Cambridge, Cambridge University Press, 2010.

[14] Marcella, A. J., *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Auerbach Publisher, 2008

[15] National Institute of Justice, *Investigations Involving the Internet and Computer Networks*, U.S. Department of Justice, 2007.

[16] Nikolaou, I. E. and Evangelinos, K.I., “A SWOT Analysis of Environmental Management Practices in Greek Mining and Mineral Industry,” *Resources Policy*, 2010, 35, pp. 226-234.

[17] Stevens, G., "Privacy Protections for Personal Information Online," *Congressional Research Service Report*, April 2011.

[18]Lenard T. M. and Rubin, P. H., "Privacy and the Commercial Use of Personal Information:

The Case of Customer Proprietary Network Information," *Technology Policy Institute*, August 2007.

[19]TW Ministry of Justice, "Personal Information Protection Act," 2014: http://pipa.moj.gov.tw/。

[20] USA White House, "National Strategy for Trusted Identities in Cyberspace - Enhancing Online Choice, Efficiency, Security, and Privacy," 2014: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf。

16 SWOT Matrix Enhancement for Online Protection of Personal Information