# From Risk Awareness to Security Controls: Benefits of Honeypots to Companies *

Sérgio Nunes[1] Miguel Correia[2]

[1] Novabase/Universidade Atlântica [2] Universidade de Lisboa

**Abstract.** Many companies are deploying their business on the Internet using web applications while the question of what is the risk to business operations of cyber-attacks remains unanswered. Risk awareness allows to identify and act upon the security risk of these applications. This paper analyzes different security frameworks commonly used by companies in order to evaluate the benefits of honeypots in responding to each framework's requirements and, consequently, mitigating the risk.

## 1 Introduction

Many companies are currently deploying their business on the Internet using *web applications*. From online shops to business-to-business applications, from web sites that allow making inquiries to applications that allow doing complex operations, more and more companies are getting in the Web 2.0 wagon. The data accessed through web applications is becoming more and more critical, containing private information that enables financial transactions in multiple online businesses. This vicious cycle is growing and organizations are unable to do risk awareness to be able to analyze these new web threats.

This new massification of web technologies poses multiple questions regarding information security: What is the role of security with this significant change? Is there a decrease in the confidentiality, integrity and availability of information with this new situation? Are there any new security threats that put information at risk?

By exposing web applications in a *honeypot*, attacks can be captured and investigated, as also can the tools and actions of the attacker after the intrusion [13,2,1,16]. The careful analysis of the gathered attack data and the know-how gained by managing honeypots provide an insight about the modus operandi and motives of the attacker, classifying him according to a pre-established profile. Having the attacker profile defined, the threat model can be specified in order to develop the necessary *risk awareness* and *risk mitigation controls*.

Risk mitigation is accomplished in organizations by employing a variety of information security, compliance and *risk frameworks* that address multiple domains across the wide information technology environment. This paper considers three frameworks: ISO/IEC 27001 [6], COBIT [4] and PCI-DSS [9]. These frameworks present a major focus in security guidelines by providing specific control

* This work was partially supported by the FCT through the CMU-Portugal partnership and the Large-Scale Informatic Systems Laboratory (LaSIGE).

requirements and objectives to mitigate risk in organizations integrating people, processes and technology as a whole. These frameworks present most of the time general guidelines that do not descend to specific security technologies, so it is important to evaluate how common security technology concepts adapt to these frameworks. Honeypots can bring added value to such frameworks by satisfying multiple enumerated control requirements.

## 2 Honeypots

A *Honeypot* was defined by Spitzner as an information system resource whose value lies in unauthorized or illicit use of that resource [13]. The value of this security mechanism relies on monitoring the real steps and tools of a real attack and learning where the unknown vulnerabilities lie and how to protect the critical information assets. These monitoring and decoy capabilities aid the security professional in developing the required know-how of the modus operandi of the attacker and infer the security situational awareness of his network to plan for the adequate safeguards and effective incident responses [15]. Detecting what is unknown via monitoring and providing information for the analysis of the attack is the main factor that differentiates this tool from the rest of the security toolset.

Another concept used in the terminology of honeypots is *honeytokens*. They serve as digital entities that reveal unauthorized access when used [7]. They follow the same principle of not being used for legitimate purposes and can be for example a fake credit card number, a supposed secret document, a false email or a bogus login that is carefully placed among legitimate information.

Honeypots can be classified as research or production [3]. The research honeypots are used by the academic community to study the attacker and gather information about his tools and actions. The production honeypots help an organization mitigating the attack risk by focusing the attacker's attention in useless decoy assets, while the critical assets are safeguarded. This deception enables timely and adequate security incident responses.

Honeypots can emulate vulnerable network services to gather attack information without being exposed to a real intrusion. This type of honeypots is called *low interaction* because of the limitation of malicious activities due to basic service emulation. The deployment of a real operating system with the vulnerable service is know as *high interaction* honeypot and is able to gather the real evidence of the intrusion and to follow the additional steps performed by the attacker after gaining control of the system. Some literature also presents the definition of *mid-interaction* honeypots as the attacker's ability to fully act against an integrated honeypot daemon service, but not being able to compromise the operating system below [10,14].

Honeypots are called physical when there is a real machine connected to the network and virtual when the machine is a guest system residing in a virtualization environment [11,12]. Honeypots can be static and stay implemented without change from the initial deployed architecture or be dynamic and adapt automatically to respond to the attacker's behaviour. The honeypot technology finds place in diverse fields of use, especially where awareness is necessary combined with a

proactive security posture. The most common fields of use are intrusion detection systems, malware, botnets, spam, phishing, wireless and web [2,1,16].

To better understand the benefits of honeypots for web application risk awareness we made an experiment with a high interaction honeynet, which was reported elsewhere [8]. We executed 10 virtual honeypots with different web applications during 3 months. The main results of the experiment were:

- We observed 8858 attacks during that period of time, which shows the risk to which web applications are exposed.
- The most targeted web applications were: PhpMyadmin (81% of the attacks), TomcatManager (8%), Zencart (6%) and Roundcube (3%).
- The most common attacks were: URL bruteforce (73%), command execution (22%), authentication bruteforce (2%).
- The source of attacks were diverse as it can be seen in Figure 1 with the United States (35%) and China (16%) as the major attackers.


**Fig. 1.** Worldwide attack origin distribution

## 3 ISO/IEC 27001

### 3.1 Description

The ISO/IEC 27001 is an international standard that provides a model for establishing an Information Security Management System (ISMS) as a strategic organization decision [6]. The word system does not imply a real asset, but a defined and monitored methodology or security program. The ISMS is formed by tools, processes, templates, documents and best practices. The ISMS can be defined as an overall management system from a business risk perspective that has to be established, implemented, operated, monitored, and maintained. It mandates that the organization systematically examines its risks taking into account

threats and vulnerabilities, implements control procedures to deal with those risks and adopts a continuous improvement information security management process that continuously responds to business security needs.

The ISO/IEC 27001 is used in conjunction with ISO/IEC 27002, formerly known as ISO/IEC 17799 [5], that establishes the code of practice for information security management. This code of practice contains specific controls for dealing with most requirements of ISO/IEC 27001 including technical security, but ISO/IEC 27001 expects that these measures are already taken care of and focuses on the mandatory requirements of an Information Security Management System. ISO 27001 focuses on these control objectives from ISO/IEC 27002 in annex A.

### 3.2 Benefit Analysis

In the general requirements of the ISO/IEC 27001 standard (Section 4.2) it is stated that it is necessary to assess the realistic likelihood of a security failure occurring in the light of prevailing threats and vulnerabilities and impacts associated with the assets and the controls currently implemented. This realistic likelihood can be measured effectively using real honeypots with the same vulnerabilities as production systems. This approach mimics the production systems behaviour exposing the decoys to the same threat level. The ISO/IEC 27001 standard mandates that is crucial to monitor and review the ISMS to identify attempted and successful security breaches and incidents. The honeypots could bring to this requirement increased added value when compared to traditional intrusion detection systems, because of the detailed information gathered about an attack, which enables gaining real know-how and situational awareness of the risk that the asset faces.

In ISO/IEC 27002, the code of practice for ISO/IEC 27001, there are some controls that can be adapted to the added value of honeypots. The control for protection against malicious code (27001 Annex A.10.4.1) can be complemented with a honeypot by performing evaluation of malicious code using client honeypots and by having a honeypot infrastructure capable of monitoring malicious code spreading mechanisms. The use of multiple different malware analysis is suggested in the standard as a vector to improve the effectiveness of malicious code protection.

The ISO/IEC 27002 standard states that is necessary to reduce risks from exploitation of technical vulnerabilities (27001 Annex A.12.6). The control defines that timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. This is the main focus of the honeypot technology and by adequate use of honeypots it is possible to accomplish this goal of establishing an effective management process for technical vulnerabilities that responds to the requirements.

The ISO/IEC 27002 standard details the need to ensure a consistent and effective approach to the management of information security incidents (27001 Annex A.13.2.2). It suggests defining the responsibilities and procedures to deal with the incidents collecting forensic evidence for internal problem analysis. This

collection of evidence can be gathered using honeypots or honeypot data gathering mechanisms. Maintaining the chain of custody has multiple requirements, so training how to collect and preserve the evidence should be an exercise first performed on decoy systems such as honeypots, to prepare for a real incident on production systems. The ISO/IEC 27002 standard states that there should be a learning experience from information security incidents allowing the incidents to be monitored and quantified. The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents. This learning can be developed with the risk and threat awareness delivered with the continuous use and analysis of honeypots. Honeypots were founded as a unique possibility of learning about the modus operandi of attackers developing situational awareness about the security status of the infrastructure, allowing investigators to develop the know-how to recognize and treat these incidents with appropriate procedures when they happen in the real critical systems.

In the ISO/IEC 27002 standard there is a section concerning the correct processing in applications (27001 Annex A.12.2) detailing components such as input and output data validation that are the cause of multiple web attacks. Although the honeypots are no direct defense against those attacks, they provide the necessary learning and research capabilities necessary for secure programming and correct evaluation of the risk that results with the lack of validation in applications. The attacked decoy web applications can measure the threat level and serve as case studies for future applications developed.

The protection of organizational records is also a subject detailed in the ISO/IEC 27002 standard regarding its loss, destruction or manipulation (27001 Annex A.12.5.4). Organization information disclosure attacks happen frequently in an enterprise and they are difficult to prevent or even to detect. The concept of honeytokens can help in the detection of disclosure of critical data by placing careful bogus monitored records in such datastores and track those records while they travel through the network serving as a warning that the data is being disclosed. These detection mechanisms can be complemented with intrusion prevention solutions that limit data losses by identifying the bogus records and block further data travel or tear down the connection.

The summary of the honeypots concepts and their relation to the ISO/IEC 27701 standard can be found in Table 1.

| **Honeypot Concept** | **ISO/IEC 27001** |
|---|---|
| Risk Awareness | 4.2 Establishing and managing the ISMS |
| Secure Coding | A.12.2 Correct processing in applications |
| Malicious Code Detection | A.10.4.1 Controls against malicious code |
| Information Disclosure Detection | A.12.5.4 Information leakage |
| Vulnerability Management | A.12.6 Technical vulnerability management |
| Incident Response | A.13.2.2 Learning from information security incidents |

**Table 1.** Honeypot benefits to ISO/IEC 27001

# 4 COBIT

## 4.1 Description

Nowadays information technology (IT) processes are key activities of any organization and the dependence of the business operations from IT becomes impossible to dissociate. This close dependence can have drastic consequences if not carefully controlled and measured, as business requirements tend not to be shared with IT. It is crucial to understand that the business drives the investment in IT resources and those resources are used by IT processes to deliver the information necessary back to business. The Information Systems Audit and Control Association (ISACA) published the Control Objectives for Information and Related Technology (COBIT) to help information technology governance professionals to align technology, business requirements and risk management [4]. The Committee of Sponsoring Organizations (COSO) is an internal control framework for organizations to deal with financial, operational and compliance-related internal controls and COBIT provides those controls for information technologies.

COBIT may be positioned at the higher business management level dealing with a broad range of IT activities and focuses on how to achieve effective management, governance and control. Being maintained by a non-profit independent group with continuous research improvement, it integrates seamlessly with other standard and best practices as it forms a set of principles that can be adapted to business needs. It covers five areas of IT Governance: Strategic Alignment, Value Delivery, Resource Management, Risk Management, Performance Measurement. COBIT deals with effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability as business requirements and applications, information, infrastructure and people as resources while adopting the necessary processes for supporting activities. COBIT is illustrated by a process model with 34 processes distributed among four distinct domains:

- Plan and Organise (PO): This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organization as well as technological infrastructure must be put in place.
- Acquire and Implement (AI): To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition changes in existing systems and their maintenance are covered by this domain to make sure that the systems life cycle is continued.
- Delivery and Support (DS): This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.
- Monitor and Evaluate (ME): All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This

domain addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

### 4.2 Benefit Analysis

The COBIT plan and organise domain has a process that deals specifically with assessing and managing IT risks (Control PO9). Among its control objectives there is the requirement of risk event identification, where an event is an important realistic threat that exploits a significant applicable vulnerability causing a negative impact to business. These events deal with multiple aspects: business, regulatory, legal, technology, trading partner, human resources and operational. Under the technology events, honeypots can play the role of accessing the threats to the assets, determining the severity of the impact when dealing with vulnerabilities and developing risk awareness in the organization. This enables to determine the nature of the impact and adds value to the risk registry by detailing real relevant risks that might pass unnoticed without using decoy systems. Another control objective inside this process is conducting risk assessments on a recurrent basis being able to determine the likelihood and impact of all identified risks, using qualitative and quantitative methods, where honeypots can gather the necessary information to qualify and quantify the risk impact on technological assets. Honeypots can also contribute to the risk response control objective being able to prepare the personnel for real responses due to training gathered from honeypot detailed attack information analysis.

The COBIT acquire and implement domain has one process that deals with acquiring and maintaining application software (Control AI2) where honeypots also present an adequate measure when regarding risk awareness. Honeypots bring benefits to the application security and availability control objective by feeding the know-how regarding application attacks and how to code adequate security safeguards. Being honeypots most of the time compromised to install distributed denial of service zombies, they create the necessary awareness regarding threats against availability and show how common denial of service proliferates. Regarding the development of application software control objective, honeypots promote secure coding by showing developers how the attacks work and how they can be suppressed. This is performed with detailed information gathered from decoy systems enabling the research without harming critical production systems. The acquire and maintain technology infrastructure process has the control objective of infrastructure maintenance that mandates that there should be a strategy and plan for the infrastructure maintenance that includes periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerability assessment and security requirements. Honeypots contribute to risk awareness that help to identify and quantify risks, they also show new methods and tools to exploit known vulnerabilities, uncover unknown vulnerabilities and provide information to respond to the security requirements that mitigate the risk caused by them.

The deliver and support domain has a specific process that deals with ensuring systems security. The security testing, surveillance and monitoring control objective (Control DS5.5) has the task of ensuring that the enterprise security baseline

is maintained by testing and monitoring the IT implementation in a proactive way. It states that a logging and monitoring function will enable the early prevention and detection and subsequent timely reporting of unusual or abnormal activities that may need to be addressed. The honeypot technology promotes the proactivity by learning from attacked decoys and gathering the latest malicious tools used by attackers. It monitors the environment detecting unusual or abnormal activities while deviating the attention of the attacker from the critical systems. It tests the security baseline of enterprise systems by evaluating the robustness of the honeypots deployed using that security baseline.

Another control objective inside the systems security process (Control DS5.6) is to define security incidents communicating its characteristics so they are properly classified and treated by the problem management process. The classification of security incidents needs specific training and awareness of threats and security risks. Although multiple courses exist on that matter, it is crucial to have live training on the organization's infrastructure to adapt to real incidents and this is where a research honeypot testbed will help. The honeypot testbed trains the personnel by dealing with attacks in research decoy systems that do not interfere with business critical systems and develop a risk awareness mindset that allows them to recognize characteristics of security incidents when they really happen in production systems.

Another control objective inside this process (Control DS5.9), where honeypots play a vital role, is malicious software prevention, detection and correction. Honeypots have measures to deal with malicious software such as viruses, worms, spyware and spam. Worms are detected, monitored and researched by compromising honeypot decoys, spyware is evaluated using client-side honeypots and spam is detected and mitigated using email honeypots in conjunction with honeytokens.

The delivery and support domain has a process that deals with data management and has one control objective of defining and implementing the policies and procedures (Control DS11.6) to identify and apply security requirements applicable to the receipt, processing and storage and output of data to meet business objectives. The requirement of data confidentiality must be maintained in order to preserve business secrets and assure the privacy of clients' records, so information disclosure should be detected. Honeytokens can be used to limit information disclosure by ensuring the detection of careful placed bogus records maintaining data security. The summary of the honeypots concepts and their relation to the COBIT Framework can be found in Table 2.

| **Honeypot Concept** | **COBIT** |
|---|---|
| Risk Awareness | PO9 Assess and manage IT risks |
| Secure Coding | AI2 Acquire and maintain application software |
| Malicious Code Detection | DS5.9 Malicious software prevention, detection and correction |
| Information Disclosure Detection | DS11.6 Security requirements for data management |
| Vulnerability Management | DS5.5 Security testing, surveillance and monitoring |
| Incident Response | DS5.6 Security incident definition |

**Table 2.** Honeypot benefits to COBIT

# 5 PCI-DSS

## 5.1 Description

The payment card industry data security standard (PCI-DSS) was developed to assure cardholder data security and unify consistent data security measures globally [9]. It was created by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to establish requirements for the security of the payment card industry affecting everyone that stores card payment data, including common online commercial transactions. It is guided by a continuous process to ensure adequate monitoring and improvement of requisites by assessing, remediating and reporting procedures. It has six control objectives and establishes twelve requirements for compliance.

## 5.2 Benefit Analysis

The Payment Card Industry Data Security Standard was build with the main requirement of protecting the cardholder data when dealing with online transactions. It has requirements dealing with storage of limited card information explaining what shouldn't be kept in the database and mandates that encryption is used during travel and storage to protect cardholder data from disclosure (Requirement 3.1). Here the honeytoken principle can be used to detect the disclosure of data by using decoy invalid cards and deviating the attention during an attack from the real encrypted cards.

The PCI-DSS mandates that a process must be established to identify newly discovered vulnerabilities responding to the requirement of developing and maintaining a secure system or application (Requirement 6.2). This requires a constant vulnerability awareness program that can be complemented by deploying decoy honeypot systems monitored to find new vulnerabilities. Only reading security disclosure information from outside sources might not be enough to catch new threats as the vulnerability disclosure time window is decreasing throughout the years, leaving no time for security administrators to act accordingly protecting critical systems.

This standard has detailed requirements of coding guidelines against specific web vulnerabilities such as Cross-site scripting (XSS), Injection flaws, Malicious file execution,Insecure direct object references, Cross-site request forgery, Information leakage and improper error handling, Broken authentication and session management, Insecure cryptographic storage, Insecure communications and Failure to restrict URL access. Secure coding best practices (Requirement 6.5) against these vulnerabilities can be achieved by learning from the attacks that web applications face everyday. Although attacks can be detected using intrusion detection systems, there is no detailed information available that can serve as a learning experience, which is why honeypots are better to learn how vulnerabilities work and how they are exploited by attackers in order to promote secure coding from the lessons learned. This vulnerability awareness and know-how becomes crucial in understanding the issues detected by vulnerability assessments as there is another requirement that states that is necessary to conduct them on an ongoing

basis. The know-how gained from honeypot analysis allows developers to address these issues with secure programming to safeguard for similar situations.

The standard mandates that anti-virus software is installed on all systems commonly affected by malicious software and that it should detect, remove and protect against those threats (Requirement 5.1.1). It should be updated, running and generating audit logs. The honeypot architecture can complement anti-virus software by testing unknown suspicious malware in a controlled environment that the anti-virus has not classified yet. It is capable of detecting web malware using client honeypots and monitors the consequent behaviour and provides implicit detection against worms by detecting its propagation to decoy systems. The concept of having available a honeypot test environment provides the necessary know-how to detect, remove and treat unknown malware threats.

PCI-DSS also requires that an incident response plan (Requirement 12.9) is documented along with providing the appropriate training to staff with security breach response responsibilities. This continuous training can be achieved with periodical external courses, but practical onsite training is also fundamental to get familiar with the infrastructure and issues encountered. Honeypots can perform this role providing staff with onsite non critical system training to develop the necessary incident awareness to respond to real situations. Humans learn better by practicing and making mistakes, so honeypots provide such a research infrastructure without affecting the critical assets.

The PCI-DSS explains that the information security policy should reference that there should be an annual process that identifies threats and vulnerabilities resulting in a formal risk assessment (Requirement 12.1.2). This formal risk assessment promotes the risk awareness capabilities of the organization annually, but this awareness should be maintained with continuous improvements to ease annual evaluation and there honeypots can play a vital part. Honeypots contribute to the identification of threats to business with decoy infrastructures, monitoring exploited vulnerabilities, gathering detailed information about intrusions and malicious actions performed by attackers.

The summary of the honeypots concepts and their relation to the PCI-DSS can be found in Table 3.

| **Honeypot Concept** | **PCI-DSS** |
|---|---|
| Risk Awareness | 12.1.2 Identify threats and vulnerabilities,conduct risk assessment |
| Secure Coding | 6.5 Develop all web applications with secure coding guidelines |
| Malicious Code Detection | 5.1.1 Detect, remove and protect against malicious software |
| Information Disclosure Detection | 3.1 Keep cardholder data storage to a minimum |
| Vulnerability Management | 6.2 Identify newly discovered security vulnerabilities |
| Incident Response | 12.9 Implement an incident response plan |

**Table 3.** Honeypot benefits to PCI-DSS

## 6 Discussion

It can be observed from the previous individual risk framework analysis that the honeypots can bring benefits to multiple requirements in each framework. The honeypot contribute is not constrained to benefit measures specific to each framework, because they all deal with the same basis requirements under different names and aggregated in different groups (Table 4). More generically, the major benefits of using honeypot concepts when dealing with risk frameworks are:

- The creation of a risk awareness culture being able to correctly identify the threats to IT and evaluate the impact to business of attacks;
- The promotion of secure coding by learning from the application attacks suffered, evaluating the coding vulnerabilities that were explored and developing the safeguards necessary to correct them;
- The detection of malicious code due to monitorization of propagation attempts and unusual activity, along with the testing of suspicious webpages and binaries in a test decoy environment;
- The detection of disclosure of information with the monitorization of decoy bogus items (honeytokens);
- The creation of an accurate and timely vulnerability management framework being able to identify, analyze and patch with a minimum time delay recently disclosed exploits and malicious tools used by attackers;
- The creation of an incident management and response system capable of identifying, classifying and addressing security problems;

| Honeypot Concept | ISO/IEC 27001 | COBIT | PCI-DSS | Benefit Impact |
|---|---|---|---|---|
| Risk Awareness | 4.2 | PO9 | 12.1.2 | High |
| Secure Coding | A.12.2 | AI2 | 6.5 | Low |
| Malicious Code Detection | A.10.4.1 | DS5.9 | 5.1.1 | High |
| Information Disclosure Detection | A.12.5.4 | DS11.6 | 3.1 | Medium |
| Vulnerability Management | A.12.6 | DS5.5 | 6.2 | High |
| Incident Response | A.13.2.2 | DS5.6 | 12.9 | Medium |

**Table 4.** Summary of the honeypot benefits to three frameworks studied

## 7 Conclusion

In this paper an analysis of the basic concepts of honeypots is performed in comparison with the control requirements of frameworks in order to infer the added value that this security mechanism can bring to enterprises. This research confirmed our previous belief that honeypots are useful for companies but underestimated by them, probably mainly because of a lack of knowledge regarding this technology, its uses and benefits.

The fear of challenging the attacker and being unable to control the consequences of the intrusion is also a deterrence factor in the use of honeypots by

companies. These issues are never balanced with the possibility of developing the necessary risk awareness within the company using these decoy systems to be able to defend the critical assets when a real attack emergency happens.

Companies have multiple risk and security frameworks already in place to be able to respond to compliance requirements. In these risk frameworks the demand of developing a risk awareness program is detailed with the deployment of multiple controls. In this research some of these frameworks were analysed and it can be concluded that the honeypot technology plays a vital part in responding to those needs by applying some of its basis concepts.

## References


1. Anagnostakis, K.G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E., Keromytis, A.D.: Detecting targeted attacks using shadow honeypots. In: Proceedings of the 14th USENIX Security Symposium. pp. 129–144 (August 2005)
2. Baecher, P., Koetter, M., Dornseif, M., Freiling, F.: The Nepenthes platform: An efficient approach to collect malware. In: Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection. vol. 4219, pp. 165–184. Springer (2006)
3. Baumann, R., Plattner, C.: Honeypots. White Paper, Swiss Federal Institute of Technology (2002)
4. ISACA: Cobit framework 4.1. http://www.isaca.org (2007)
5. ISO/IEC 17799: Information technology - security techniques - code of practice for information security management. http://www.iso.org (June 2005)
6. ISO/IEC 27001: Information technology - security techniques - information security management systems - requirements. http://www.iso.org (October 2005)
7. McRae, C.M., Vaughn, R.B.: Phighting the phisher: Using web bugs and honeytokens to investigate the source of phishing attacks. In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences (January 2007)
8. Nunes, S., Correia, M.: Web application risk awareness with high interaction honeypots. In: Actas do INForum Simposio de Informatica (September 2010)
9. PCI-DSS: Payment card industry data security standard version 1.2. http://www.pcisecuritystandards.org (October 2008)
10. Pouget, F., Dacier, M., Debar, H.: White paper: honeypot, honeynet, honeytoken: terminological issues. Research Report RR-03-081, Institut Eurecom, France (2003)
11. Provos, N.: A virtual honeypot framework. In: Proceedings of the 13th USENIX Security Symposium. pp. 1–14 (August 2004)
12. Provos, N., Holz, T.: Virtual honeypots: from botnet tracking to intrusion detection. Addison-Wesley, Boston, MA, USA (2007)
13. Spitzner, L.: Honeypots: Tracking Hackers. Addison-Wesley, Boston, MA, USA (2002)
14. Wicherski, G.: Medium interaction honeypots. German Honeynet Project (April 2006)
15. Yegneswaran, V., Barford, P., Paxson, V.: Using honeynets for internet situational awareness. In: Proceedings of the 4th ACM/USENIX Workshop on Hot Topics in Networks (November 2005)
16. Zou, C.C., Gong, W., Towsley, D., Gao, L.: The monitoring and early detection of internet worms. IEEE/ACM Transactions on Networking 13(5), 961–974 (2005)