The Canadian Institute of Chartered Accountants

Information Technology Advisory Committee

Using an Ethical Hacking Technique to Assess Information Security Risk

Insights for a changing world

Notice to Reader

The objective of white papers issued by the CICA's Information Technology Advisory Committee (ITAC) is to increase the awareness of CAs and other interested parties on IT topics considered significant to the accounting profession and business community. They are not intended to provide detailed guidance.

The CICA expresses its appreciation to the principal authors of this white paper, Gary Baker, CA (an ITAC member) and Simon Tang, MSc, CPA(Michigan), CISSP of Deloitte & Touche. The advice and comments provided by other members of ITAC, who are listed at the back of this document, were also appreciated.

The views expressed in this paper are those of the principal authors, and have not been formally endorsed by the CICA or ITAC.

Comments on the paper are welcome and should be addressed to Andrée Lavigne, CA, Principal, Research Studies, CICA (andree.lavigne@cica.ca).

This white paper is available in PDF format at the CICA web site (www.cica.ca/itac).

Disponible en français
(www.icca.ca/ccti)

USING AN ETHICAL HACKING TECHNIQUE

TO ASSESS INFORMATION SECURITY RISK

CONTENTS

INTRODUCTION

Adequately protecting an organization's information assets is a business imperative – one that requires a comprehensive, structured approach to provide protection commensurate with the risks an organization might face. The purpose of this white paper is to explore an ethical hacking technique – referred to in the IT community as **Penetration Testing** – that organizations are increasingly using to evaluate the effectiveness of information security measures. This paper aims to provide them with information about penetration testing and help them evaluate penetration testing as a tool for their information security strategy.

WHAT IS PENETRATION TESTING?

As its name implies, penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. The idea is to find out how easy or difficult it might be for someone to "penetrate" an organization's security controls or to gain unauthorized access to its information and information systems.

A penetration test typically involves a small team of people sponsored by the organization asking for the test. This team attempts to exploit vulnerabilities in the organization's information security by simulating an unauthorized user (or "hacker")[1] attacking the system using similar tools and techniques. Penetration testing teams typically comprise people from an organization's Internal Audit department or IT department, or from consulting firms specializing in these types of services. Their goal is to attempt to identify security vulnerabilities under controlled circumstances, so that they can be eliminated before unauthorized users can exploit them. Because penetration testing is an authorized attempt to simulate hacker activities, it is often referred to as "ethical hacking."

[1] This paper uses the term "hacking" or "hacker" because the term is most commonly used to refer to someone who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously. It is recognized that, in the IT community, a "hacker" refers to an individual with specialized skills and expertise who attempts to identify and expose programming errors and security vulnerabilities. An individual whose intent is malicious is referred to as a "cracker."

It is important to point out that a penetration test cannot be expected to identify all possible security vulnerabilities, nor does it offer any guarantee that an organization's information is secure. Penetration testing is typically conducted at a point in time. New technology, new hacker tools and changes to an organization's information system can create exposures not anticipated during the penetration testing. In addition, penetration testing is normally completed with finite resources, focused on a particular area, over a finite period of time. Hackers determined to break into an organization's information systems are often not bound by similar constraints. Penetration testing is also typically focused on a system's security vulnerabilities that would enable unauthorized access. It is **not** necessarily focused on security vulnerabilities that could result in the accidental loss or disclosure of the organization's information and information systems.

WHY SHOULD AN ORGANIZATION CONSIDER PENETRATION TESTING?

By simulating the actions that a hacker might perform, an organization can gain valuable insights into the effectiveness of the security controls in place over its information systems. Penetration testing can identify vulnerabilities that unauthorized users could exploit. It can also identify more pervasive gaps and deficiencies in the organization's overall security processes including, for example, its ability to identify, escalate and respond to potential security breaches and incidents.

In deciding whether penetration testing is appropriate as a part of its overall information protection and security strategy, an organization should consider both the significance and the likelihood of individuals exploiting security vulnerabilities to gain unauthorized access to its information systems and, thereby, undermining the confidentiality or the integrity of both the information and the systems.

Assessing Significance

Security controls are the foundation for trust – the trust an organization's customers, employees, trading partners and stakeholders place in the organization that its data and intellectual property are adequately protected against unauthorized access, disclosure, use or loss. Therefore, in assessing the significance of the loss of the confidentiality or integrity of its information and systems, an organization must consider the importance that a breach in trust may have on its business operations, its customers, its employees or any of its key stakeholders.

A successful e-business environment enables business partners, customers, suppliers and visitors to quickly and directly access an organization's information systems. It, therefore, provides business with tremendous opportunities for improving operational efficiencies, strengthening customer relationships and driving revenue growth. At the same time, these technological advancements and innovations introduce exposures and vulnerabilities that, if exploited for malicious purposes, can have significant and, perhaps, even devastating consequences to an organization's reputation and, in extreme situations, ongoing viability. The challenge lies in balancing access requirements with robust protection against unauthorized usage.

Protecting an organization's information and systems is a business imperative — the price of entry for successful business in a networked economy. Increasingly, management, audit committees, boards of directors, customers, consumers and other stakeholders are requiring assurance that the organization is taking appropriate measures to protect its information and the information entrusted to it. Audit opinions on the adequacy of controls over information systems, such as SysTrust, WebTrust and Section 5900[2] opinions, are increasingly used to provide this assurance. Legislation such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA),[3] as well as the *Gramm-Leach-Bliley Act* and the *Sarbanes-Oxley Act* in the United States, are placing increased responsibility on organizations to implement procedures that ensure the privacy, confidentiality and integrity of their information and information systems. Penetration testing can help provide the assurance management and its auditors need on the information security components an organization uses to protect its information assets.

---

2 *CICA Handbook – Assurance*, Section 5900, "Opinions on Control Procedures at a Service Organization."

Assessing Likelihood

The likelihood of an organization suffering an unauthorized intrusion is increasing for two main reasons. First, all information technology components in use today have potential security vulnerabilities. Some vulnerabilities are a consequence of the inherent limitations in the performance or design of the particular technology. Other vulnerabilities arise from the way the technology is configured or programmed for use. Regardless, these inherent vulnerabilities are widely publicized by technology vendors, security organizations and the hacker community on the Internet, and are available to anyone with professional or malicious interest. Second, a proliferation of powerful computers and software tools, coupled with the growing number of people who are inclined to use such tools for fun, mischief or profit, leads many to believe that the number of potential attackers and the types of potential attacks is increasing faster than the improvement in security techniques.

The term "hacker" conjures up the image of an external person attempting to exploit security vulnerabilities to gain unauthorized access to an organization's information systems. Exposure to security vulnerabilities is not, however, limited to those external to the organization. Internal, "authorized" users of a system also present a significant security exposure. According to a recent survey,[4] 75% of respondents cited that disgruntled employees are the most likely source of attacks. Employees or other trusted parties were those most likely to be responsible for vandalism, theft of information and sabotage of data. When assessing the likelihood of someone attempting to exploit security vulnerabilities, organizations should consider the potential for both internal and external attack.

Hackers, both internal and external, identify targets through *choice* and *opportunity*. A "target of choice" is one that is specifically identified and selected. Hackers penetrate targets to achieve notoriety within their community or to reap more tangible benefits from, say, information theft and industrial espionage. Large, high-profile organizations, such as governments and financial institutions, are regular targets of choice. Employers and former employers often represent targets of choice for disgruntled employees, suppliers or contractors.

---

3 For further information, refer to *Privacy Compliance: A Guide for Organizations & Assurance Practitioners* (Toronto: CICA, 2002 (a CICA web-site publication – www.cica.ca/itac).

4 Computer Security Institute Survey 2002.

A "target of opportunity," on the other hand, has been selected because of fortuitous circumstances, such as relative ease of access, availability of insider information, or luck. As such, almost any organization can be a target of opportunity. Internal attacks also present a significant exposure, as employers and former employers often, perhaps unknowingly, provide ample opportunity for disgruntled employees, suppliers or contractors to attempt unauthorized access.

When assessing the likelihood of being subject to unauthorized access attempts, organizations should consider the potential of being identified both as a "target of choice" and a "target of opportunity." They should also consider their potential exposure to not only external threats but also the statistically more likely internal attacks.

ARE FIREWALLS AND INTRUSION DETECTION SYSTEMS (IDS) ENOUGH?

Many organizations have deployed sophisticated security mechanisms, such as firewalls or intrusion detection systems (IDS), to help protect their information assets and to quickly identify potential attacks. While these mechanisms are important, they are not foolproof. A firewall cannot protect against what is allowed through – such as online applications and allowed services. While an IDS can detect potential intrusions, it can detect only what it has been programmed to identify, and it will not be effective at all if the company does not monitor or respond to the alerts. As well, firewalls and intrusion detection systems must be continuously updated or they risk losing their effectiveness at preventing or detecting attacks. Penetration testing can help validate and confirm the effective configuration of an organization's firewalls and its intrusion detection systems.

WHAT'S INVOLVED IN PENETRATION TESTING?

The scope of a penetration testing project is subject to negotiation between the sponsor of the project and the testing team, and will vary depending on the particular objectives to be achieved. The principal objective of penetration testing is to determine whether an organization's security vulnerabilities can be exploited and its systems compromised. Conducting such a test involves gathering information about an organization's information systems and information security and then using this information to attempt to identify and exploit known or potential security vulnerabilities. Evidence to support the penetration testing team's ability to exploit security vulnerabilities can vary from gathering "computer screen shots" or copying sensitive information or files to being able to create new user accounts on the system or being able to create and/or delete particular files on the organization's servers.

Penetration testing can have a number of secondary objectives, including testing the organization's security incidents identification and response capability, testing employee security awareness or testing users' compliance with security policies. There are two areas that should be considered when determining the scope and objectives of a penetration testing exercise: testing strategies and testing activities to be executed.

Testing Strategies

Various strategies for penetration testing, based on specific objectives to be achieved, include:

- **External vs. internal testing.** External testing refers to attacks on the organization's network perimeter[5] using procedures performed from outside the organization's systems, that is, from the Internet or Extranet. To conduct the test, the testing team begins by targeting the company's externally visible servers or devices, such as the Domain Name Server (DNS), email server, web server or firewall. Internal testing is performed from within the organization's technology environment. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.

---

[5] The term "perimeter" is often used to describe the logical boundary of the information systems within the organization's control and the access points to and from other systems and networks not within its control.

- **Blind and double blind vs. targeted testing strategy**. In a blind testing strategy, the testing team is provided with only limited information concerning the organization's information systems configuration. The penetration testing team must use publicly available information (such as company web-site and domain name registry, Internet discussion board) to gather information about the target and conduct its penetration tests. Blind testing can provide information about the organization that may have been otherwise unknown, but it can also be more time consuming and expensive than other types of penetration testing (such as targeted testing) because of the effort required by the penetration testing team to research the target.

  Double-blind testing extends the blind testing strategy in that the organization's IT and security staff are not notified or informed beforehand and are "blind" to the planned testing activities. Double-blind testing can test the organization's security monitoring and incident identification, escalation and response procedures. Normally, in double-blind testing engagements, very few people within the organization are made aware of the testing, perhaps only the project sponsor. Double-blind penetration testing requires careful monitoring by the project sponsor to ensure that the testing procedures and the organization's incident response procedures can be terminated when the objectives of the test have been achieved.

  Targeted testing (often referred to as the "lights-turned-on" approach) involves both the organization's IT team and the penetration testing team being aware of the testing activities and being provided information concerning the target and the network design. A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, than on the organization's incident response and other operational procedures. A targeted test typically takes less time and effort to complete than blind testing, but may not provide as complete a picture of an organization's security vulnerabilities and response capabilities.

Types of Testing

In addition to the penetration testing strategies to be used, consideration should be given to the types of testing the testing team is to carry out. These could include:

- **Application security testing**. Many organizations offer access to core business functionality through web-based applications. This type of access introduces new security vulnerabilities because, even with a firewall and other monitoring systems, security can be compromised, since traffic must be allowed to pass through the firewall. The objective of application security testing is to evaluate the controls over the application and its process flow. Topics to be evaluated may include the application's usage of encryption to protect the confidentiality and integrity of information, how users are authenticated, integrity of the Internet user's session with the host application, and use of cookies – a block of data stored on a customer's computer that is used by the web server application.
- **Denial of Service (DoS) testing.** The goal of DoS testing is to evaluate the system's susceptibility to attacks that will render it inoperable so that it will "deny service," that is, drop or deny legitimate access attempts. Decisions regarding the extent of Denial of Service testing to be incorporated into a penetration testing exercise will depend on the relative importance of ongoing, continued availability of the information systems and related processing activities.
- **War Dialing.** War dialing is a technique for systematically calling a range of telephone numbers in an attempt to identify modems, remote access devices and maintenance connections of computers that may exist on an organization's network. Well-meaning users can inadvertently expose the organization to significant vulnerability by connecting a modem to the organization's information systems. Once a modem or other access device has been identified, analysis and exploitation techniques are performed to assess whether this connection can be used to penetrate the organization's information systems network.
- **Wireless network penetration testing.** The introduction of wireless networks, whether through formal, approved network configuration management or the inadvertent actions of well-meaning users, introduce additional security exposures. Sometimes referred to as "war-driving," hackers have become proficient in identifying wireless networks simply by "driving" or walking around office buildings with their wireless network equipment. The

goal of wireless network testing is to identify security gaps or flaws in the design, implementation or operation of the organization's wireless network.

- **Social Engineering.** Often used in conjunction with blind and double-blind testing, this refers to techniques using social interaction, typically with the organization's employees, suppliers and contractors, to gather information and penetrate the organization's systems. Such techniques could include:
    - posing as a representative of the IT department's help desk and asking users to divulge their user account and password information;
    - posing as an employee and gaining physical access to restricted areas that may house sensitive information;
    - intercepting mail, courier packages or even trash to search for sensitive information on printed materials.

  Social engineering activities can test a less technical, but equally important, security component: the ability of the organization's people to contribute to — or prevent — unauthorized access to information and information systems.

MANAGING THE RISKS ASSOCIATED WITH PENETRATION TESTING

While management sponsors the testing activities, those activities do, in themselves, represent some level of risk. Some of the key risks include the following:

- the penetration test team may fail to identify significant vulnerabilities;
- misunderstandings and miscommunications may result in the test objectives not being achieved;
- testing activities may inadvertently trigger events or responses that may not have been anticipated or planned for (such as notifying law enforcement authorities);
- sensitive security information may be disclosed, increasing the risk of the organization being vulnerable to external attacks.

The organization should take steps to appropriately manage these risks including:

- **Ensuring that the testing team is reliable and appropriately qualified.** To be effective — and to validate the legitimacy of the findings — it is important for the penetration testing team to have the appropriate qualifications and familiarity with both system construction and rapidly evolving hacker techniques. In deciding on the team to complete the penetration testing activities, consideration should be given to their qualifications, experience, knowledge and their reputation in the e-business community.

  Many information security consulting firms, including the major professional services firms, offer penetration testing as part of their risk management and consulting services. In addition to the qualifications and credentials of their team and reputation in the community, external service providers can be evaluated on the basis of their methodologies and their access to, and use of, state-of-the art tools to improve the efficiency and effectiveness of the testing activities.

  Those retained to perform penetration testing, whether employees or third-party service providers, will have access to extremely sensitive security information and, as such, hold a significant position of trust throughout the course of the testing. Organizations should ensure that these people can, in fact, be relied on to maintain this trust by carrying out background checks and reference checks, and by requiring non-disclosure agreements related to confidentiality of findings and observations.

- **Ensuring that the project scope, objectives, and terms of the engagement are in writing.** Because the potential significance of differences in understanding or expectations can leave an organization exposed to significant security vulnerabilities, it is important to have the scope, objectives and terms of the penetration testing engagement clearly and fully articulated in writing. The roles and responsibilities of each participant in the project should be clearly defined. Project management, activity monitoring, ongoing communication expectations and how incident management will be handled should be formally documented.

Depending on the nature of the organization's IT infrastructure participation, sign-offs and approvals may be required from its third-party hosting company (such as an Internet Service Provider). These sign-offs and approvals should describe appropriate details of the tests (time, target, source addresses, etc) and any appropriate liability considerations.

The terms of engagement should clearly identify the "rules" governing the testing activities. They should include provisions for confidentiality of findings and observations; conflict and dispute resolution procedures; representations, warranties and remedies; as well as defining liability if anything were to go wrong.

- **Defining the role of the observer.** It is important for the sponsor of the penetration testing activities to actively monitor the progress of the project. While particularly true of blind and double-blind testing strategies, where the organization's information security group may not be aware that a test is being conducted, an individual with the appropriate authority and decision-making capability should be permitted to intervene in the project, as appropriate. Such intervention could include halting the security escalation procedures (for example, to prevent notification of law enforcement authorities of what appears to be a security attack), or halting the penetration testing activities if, for example, it appears the objectives have been achieved, or in the event of a real attack occurring at the same time.

- **Protecting the confidentiality of findings and observations.** During the course of the penetration testing, significant security vulnerabilities can, and likely will be, identified. Such information must be adequately protected to minimize the risk that it does not create a further security exposure by falling into the wrong hands. Some questions to consider include:
    - Will activities be conducted over the Internet or other public network? If so, how is information protected while in transmission over such networks?
    - How and where will information that is collected, including working paper files, be stored? In electronic form? In physical form? Who has, or will have, custody of this information, including summaries of findings and observations?

- How much information will the final reports and executive summaries contain? How will content and distribution of findings, observations and reports be controlled?
- How will notes, working papers and other forms of information be retained or destroyed?
- Do the terms of engagement include appropriate provisions to protect the confidentiality of the information collected, as well as the findings, observations and recommendations?

- **Defining when testing activities end.** The activities or events that will trigger the conclusion of the penetration testing activities should be clearly described in the engagement scope definition. Such activities or events would, of course, depend on the specific objectives of the test, but could, for example, include collecting proof of the team's ability to exploit security vulnerabilities. This "proof" could take many forms, such as copying a target file, creating a file on a target server, adding a new user to a target system or capturing "screen shots" of a target application system. In some instances, it may be appropriate to define a time period within which the testing is to be completed.

HOW DOES PENETRATION TESTING COMPARE WITH OTHER KINDS OF SECURITY RELATED PROJECTS?

As noted earlier, penetration testing determines how easy or difficult it is for someone to penetrate or gain unauthorized access to an organization's information and information systems by exploiting security vulnerabilities. By contrast, other forms of security assessment include:

- **Vulnerability Identification/Assessments** (sometimes referred to as a Security Assessments). Typically diagnostic in nature, these types of projects focus on identifying and assessing weak spots within an organization's security architecture. These projects often employ automated tools specifically designed to identify if the organization has addressed, or remains exposed to, known security flaws and vulnerabilities in its particular computing environment. These engagements typically do not include activities to determine if the identified vulnerabilities could be exploited. These projects provide a broader coverage of

known security vulnerabilities, whereas penetration testing tends to be more narrowly focused on specific vulnerabilities, but more deeply in terms of ability to exploit those vulnerability.

- **Threat and Risk Assessments.** These types of projects tend to be the most comprehensive assessments, covering the broad range of threat and risks confronting an organization's IT operation. A threat and risk assessment will typically include risk and control areas such as backup, disaster recovery and contingency planning, incident response procedures, computer operations, IT policies and procedures, human resources, data classification and systems classification and prioritization. Threat and risk assessments tend not to delve deeply into the ability to exploit potential vulnerabilities in any particular area.
- **Security Breach Investigations.** Investigations are often conducted following a security breach or other incident. The focus of this type of project can be both diagnostic in nature – to identify the root cause of the incident and prescribe corrective actions to prevent recurrence – and investigative in nature – to identify the perpetrator and to preserve electronic evidence for potential prosecution. These types of projects are reactive and are initiated as a response to the occurrence of a particular event. Penetration testing, on the other hand, is an attempt to proactively simulate security incidents so that remedial action can be implemented before a real incident occurs.

SUMMARY AND CONCLUSIONS

As noted at the outset of this paper, adequately protecting an organization's information assets is a business imperative. Penetration testing can be an efficient and cost-effective part of an organization's overall security strategy to provide insights on how easy or difficult it is for someone to gain unauthorized access to its information and information systems and to "test" its information security and response capability.

CICA Information Technology Advisory Committee

Chair

Donald E. Sheehy, CA•CISA	Deloitte & Touche LLP, Toronto

Committee

Gary S. Baker, CA	Deloitte & Touche LLP, Toronto
David Chan, CA•CISA	Ontario Government Information Protection Centre, Toronto
Allan W.K. Cheung, CA•CISA	The Canadian Depository for Securities Limited, Toronto
Henry Grunberg, CA	Ernst & Young LLP, Toronto
Ray Henrickson, CA•CISA	Bank of Nova Scotia, Toronto
Robert G. Parker, FCA, CA•CISA	Deloitte & Touche LLP, Toronto
Robert Reimer, CA•CISA	PricewaterhouseCoopers LLP, Winnipeg
Douglas G. Timmins, CA	Office of the Auditor General of Canada, Ottawa
Gerald D. Trites, FCA, CA•CISA	St. Francis Xavier University, Antigonish, NS (also staff consultant for the Committee)

CICA Staff

David J.Moore, CA	Research Studies Director
Bryan C.Walker, CA	Principal, Assurance Services Development
Andrée Lavigne, CA	Principal, Research Studies

The Information Technology Advisory Committee (ITAC) is part of the Knowledge Development Group at the CICA. Its role is to provide support and advice on IT matters as they affect the CA profession and the business community.