CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Security

TECHNOLOGY SPOTLIGHT

Security encompasses the mechanisms that protect an organization's IT systems and data from unauthorized access, use, disclosure, manipulation or destruction.

Over the years, major vendors have made improvements in remediating identified software vulnerabilities and building more effective security into application and system software. New identity and access management products have come to market to improve access control through electronic authentication and permission management (granting, roll changes, revocation).

Organizations have benefited from this maturity so that some management groups feel confident they can maintain the security of their technology environments. The problem is that the technology environment is not stable. It is a dynamic environment that must evolve to meet the changes of technology, user expectations and business needs.

The security challenge today is how to define and enact effective security in a continuously changing technical, business and user environment. The media regularly reports large-scale thefts of data, breaches of privacy, alleged state-sponsored computer attacks and the role of organized crime in the execution of sophisticated malware.

Today's computer security practices must deal with these and other threats in order to protect the reputation and intellectual capital of organizations, the privacy of their customers and the integrity of their systems.

This publication was originally published by The Canadian Institute of Chartered Accountants in 2012.
It has been reissued by Chartered Professional Accountants of Canada.

Description

Mobile Technology

Security over mobile technology is an increasing concern as more and more mobile devices find their way into business environments. The risks of lost or stolen devices, malware contamination of a device and contagion to business technology infrastructure are increasing.

Personally Owned Technology

Secure use of personally owned technology for business purposes (i.e. bring your own device).

Cybercrime

Security threats with social engineering.

Advanced Threats

This is a new category of more sophisticated threats.

Economic Constraints of Security

Insufficient investment in securing the business's information assets

Importance

Mobile Technology

New technologies such as smartphones, tablets, Wi-Fi hotspots and downloadable apps are becoming mainstream. However, mobile technology is relatively recent and there has not been time for security to reach a satisfactory level of maturity. Users, particularly when they connect to various networks to exchange information and then access a business network, must be vigilant about the potential risks.

Personally Owned Technology

The usage and controls of personally owned devices and enterprise-owned devices tend to be very different.

Enterprise-owned devices are configured and maintained to perform business functions, are connected to an enterprise network and typically have controls over their Internet and email usage.

Personally owned devices generally lack these kinds of controls. In addition to being used for business purposes, they enable owners to connect to the Internet directly or through a home router and to use their computers for entertainment purposes, such as playing games, watching videos, shopping, and communicating with friends through social media. Owners freely download and install application software and transfer files between external sources. These different usage patterns mean that personally owned devices tend to be exposed to a different mix of computer threats than enterprise-owned devices.

Cybercrime

Cybercriminals have long used social engineering to deceive users into disclosing personal information or to install software that performs malicious actions in addition to or instead of the software's desired functions or that exploits vulnerabilities in already installed software.

Cybercrime, the use of malware, phishing and other techniques have seen cybercrime increase recently. Organizations and individuals are under increased threat from cyber-attacks.

Advanced Threats

This type of computer attack differs from the opportunistic attack for financial, political or other gain that typifies most computer attacks. Some call it cyber-espionage. The objective of this attack is to remain undetected in a system for a lengthy period of time in order to steal an organization's intellectual property to use or hand off to a competitor. Such an attack related to the proposed acquisition of the Potash Corp. of Saskatchewan by Australian company BHP Billiton Ltd. was reported in the December 6, 2011, edition of The Globe and Mail.

The operators of these attacks are highly skilled, well organized and well funded, allegedly by foreign states.

Economic Constraints of Security

The economic volatility of the past four years has resulted in budgetary restraint as organizations cut back expenditures and capital investment in almost all areas. On the other hand, cybercriminals are becoming increasingly sophisticated and better funded by organized crime elements or, as recently reported in the media, state funded.

Business Benefits

Business benefits from an effective security program are frequently difficult to measure: how many viruses did the business not get, how many intrusions were unsuccessful, or how many database rebuilds were not required? Industry statistics are either difficult to obtain or events may be underreported. However, the following will likely cast the business in an unfavourable light and cause stakeholders to assess their position and options:

- Negative publicity due to a security breach involving personal information;
- Lost or stolen customer information;
- Leaks of confidential business intellectual property of future plans.

Issues and Risks	Possible Mitigation
Mobile Technology	
Employees who use mobile technology to access sensitive business data are susceptible to hacks. **Organizations face increased risk of processing transactions from fraudulent sources using stolen credentials of valid employees or customers.** **Employees who are allowed "reasonable use" of mobile business technology for personal purposes may introduce malware into the business environment.** **With mobile payments looming in Canada, organizations have no choice but to address end-point device security risks. Mobile payments are just the beginning—down the road, transaction source documents will not be paper-based at all.**	Test and deploy security updates to mobile devices. Provide secure access to the enterprise's systems and data such as through VPN, encrypted channels and virtualization environments such as those available from VMware and Citrix. Require two-factor authentication for remote access to corporate systems. Implement procedures to disable use and delete data from lost or stolen mobile devices. Set policies to define expected behaviour as well as the consequences of not following the policy. Corporate applications should be encapsulated or compartmentalized, separate from user applications and data.

Issues and Risks	Possible Mitigation
Personally Owned Technology	
Employees may lack concern about security and privacy when using personally owned devices for business purposes. **Security and control procedures over the use and maintenance of personally owned devices do not meet the organization's standards.**	Develop and enforce a security strategy for employee use of personal devices, mobile devices and social media. Ensure personally owned technology is protected by approved enterprise security and passwords. Provide appropriate support and best practice security guidance to owners of personal technology to help them resolve problems with personal technology quickly. Enhance the organization's capacity to support the variety of non-standard user-owned technology. Provide secure methods, such as quarantined web addresses, by which owners of personal technology can interact with enterprise systems and data. Train employees to understand the threats of the use of personally owned technology, the organization's control standards, their responsibility for the protection of business data on those devices and the escalation procedures for when control breaches are identified. Corporate applications should be encapsulated or compartmentalized, separate from user applications and data. Set policies to define expected control standards and user behaviour as well as the consequences of not following the policy. Have employees trained and signed off on these policies. Connection to the corporate network should perform initial and/or regular/continuous checks on device configuration against corporate standard, and be able to fix settings to allow the session to continue.

Issues and Risks	Possible Mitigation
Cybercrime	
Employee is deceived into downloading fake antivirus software. **Employee provides personal credentials in response to an email hoax.** **Employee follows a hyperlink on a web page or in an email message that leads to a page that attempts to use browser vulnerabilities to install malware.**	Block Internet access to known phishing or attack sites. Implement website filtering capability that is provided through search engines or install additional filtering software to detect malicious sites. Limit users' ability to download and install software or software updates. Test and deploy security updates from all software vendors. Ensure development and maintenance teams follow formal system life-cycle methodology. Limit the number and access privileges of powerful user accounts in the organization. Provide them only to those who must have access and to the specific resources they need. Audit the ownership and use of powerful user accounts. Train employees to understand the threats of social engineering, the techniques employed for such attacks, how to resist these attacks and escalation procedures for when such attacks are identified. Set policies to define expected behaviour as well as the consequences of not following the policy.

Issues and Risks	Possible Mitigation
Advanced Threats	
Unexpected encrypted traffic leaving the organization. **Large outbound data transfers via HTTP/HTTPS.** **Login to a critical network device that is not attributable to an authorized employee.** **Unexplained remote access activity.** **Unusual web communications, DNS resolution and user agent strings.**	Test and deploy network security updates from all vendors. Carry out periodic penetration tests. Implement identity and access management technology. Provide employee security awareness training programs. Centralize security information management process. Unless the communicating device is a web server, any device that sends large volumes of data outbound via either HTTP or HTTPS should be examined for compromise. All login events, whether successful or unsuccessful, should be logged. The logs should be reviewed regularly. Hosts attempting to establish a communication channel using DNS requests to unknown DNS servers, trying to connect directly rather than using an enterprise web proxy, or using non-standard user agent strings such as one that includes the internal host name, may be signs of advanced persistent threat activity and should be investigated. Connection to the corporate network should perform initial and/or regular/continuous checks on device configuration against corporate standard, and be able to fix settings to allow the session to continue.
Security-Economic Constraints	
Insufficient investment in maintaining the organization's core capabilities of its information security function.	Develop a vision and strategy for maintaining an effective security function within the organization. Objectively assess the value of information to the business against the strength of the security initiatives, and close gaps that are too big to live with. Implement strategies that can build upon collaboration among key business areas such as compliance, audit, security and business management to gain additional synergies.