

White Paper

Data-Centric Security

DATA-CENTRIC SECURITY

Author

Gerald D. Trites, FCA, CA•IT, CA•CISA

Project Director

Malik Datardina, CA, CISA

Information Technology Advisory Committee

Chair

Ray Henrickson, CA•IT, CA•CISA, Scotiabank, Toronto

Members

Efrim Boritz, FCA, CA•IT/CISA, PhD, University of Waterloo, Toronto

Nancy Y. Cheng, FCA, Office of the Auditor General of Canada, Ottawa

Malik Datardina, CA, CISA, Data Sync Consulting Inc., Mississauga
(also technical consultant for the Committee)

Mario Durigon, CA, KPMG LLP, Toronto

Henry Grunberg, CA•IT, Ernst & Young LLP, Toronto

Andrew Kwong, CA, Deloitte & Touche LLP, Toronto

Carole Le Néal, CISA, CISSP, CIA, Mouvement des caisses Desjardins, Montreal

James R. Murray, CA•CISA, CA•CIA, Grant Thornton LLP, Halifax

Robert G. Parker, FCA, CA•CISA, Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•IT, CA•CISA, CISM, PricewaterhouseCoopers LLP, Winnipeg

Douglas G. Timmins, CA, Office of the Auditor General of Canada, Ottawa


Gerald D. Trites, FCA, CA•IT, CA•CISA, Zorba Research Inc., Heatherton
(also technical consultant for the Committee)

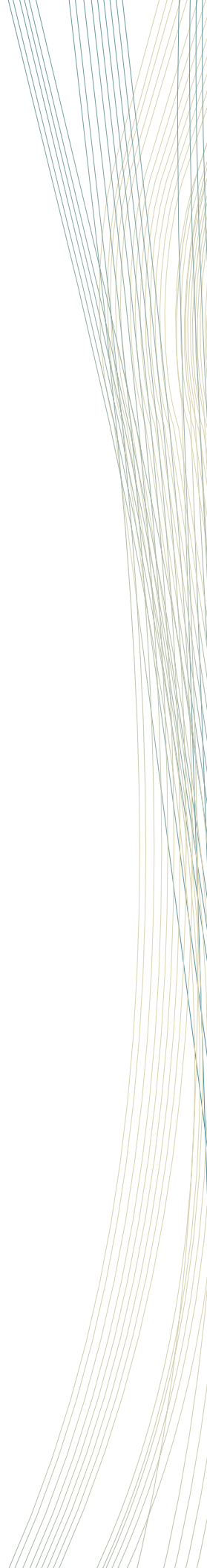
Bryan C. Walker, CA, The Canadian Institute of Chartered Accountants, Toronto

CICA Staff

Dave Pollard, CA, Vice President, Knowledge Development

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 to the CA profession and the business community.







INTRODUCTION

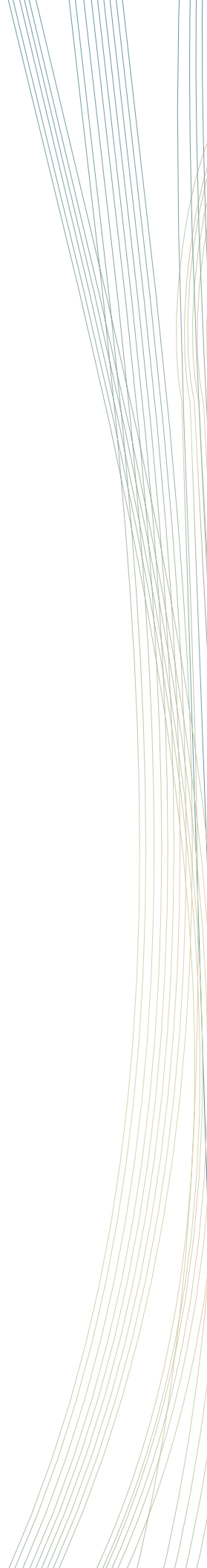
In most organizations, data that was once static and stored in one place now moves freely from platform to platform throughout the organization and beyond. Because data is now often generated and modified by users and is resident in different forms and versions in different places simultaneously, maintaining a secure environment is a growing challenge.

This paper suggests that a data-centric policy should be the focus for management, auditors and others involved in securing data in this new mobile environment. As used below, the term “security” is taken in its broadest sense to include confidentiality, integrity (accuracy, completeness and validity) and availability.

The proliferation of small portable devices with large capacities for handling data is the primary reason why data has become so mobile. Laptops are a prime example, but far from the only one. Personal Digital Devices (PDA's), such as the Blackberry, have a considerable capacity for storing and transmitting data. Email and Instant Messaging (IM) have become the common means of transmitting data. Smart cell phones, such as the iPhone, are becoming more capable and ubiquitous; the iPod, which used to be identified only with music storage, now stores other forms of data. Finally, many organizations use dedicated hand-held units to capture and maintain customer data, take orders, process payments in the field and keep inventory records.

Sensitive data about customers, employees, contracts, pricing tables, research data, etc., can now reside in a unit of any of these devices at any time. In addition, this data can now move from one device to another and one unit to another wirelessly. Therefore “data at rest” and “data in motion” are key concepts to be considered in developing an effective data-centric security policy.

Since these units are portable and subject to loss or theft, the first step in developing a data-centric security policy must include the design of a process for determining the location of the data at any given moment and for tracking its movement from one unit to another.



DEVELOPING A DATA-CENTRIC SECURITY POLICY

Phase 1: Following the Data

The most useful way to record the storage and movement of data is through the use of data-flow diagrams detailed enough to locate data at any time in the course of its travels.

Exhibit A: Data-Flow Diagram Sample

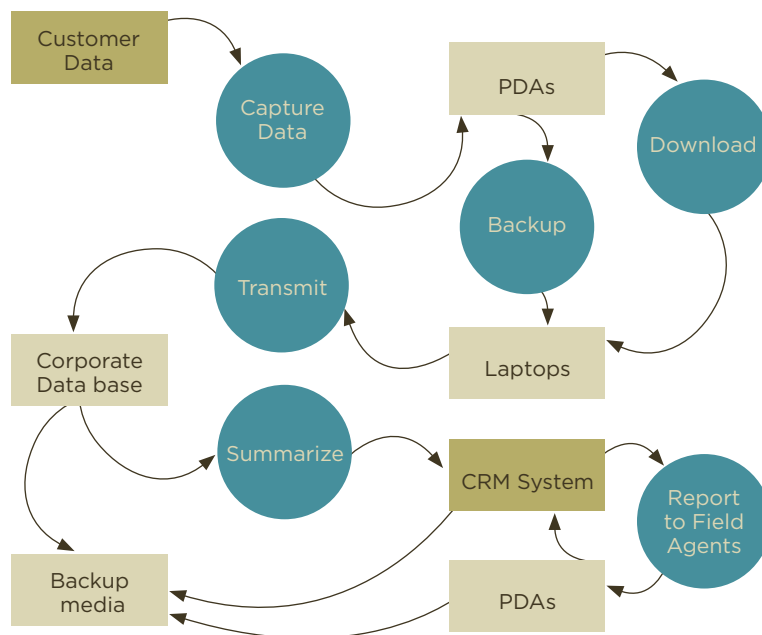


Exhibit A shows how data might flow in an organization. Data is first resident in the customer files, then captured by a company representative and stored in a PDA. That evening the representative downloads the PDA to a laptop and transmits it to the corporate database. The data is summarized in a CRM system and then made available to field agents, who capture it on their PDAs. Other ways to handle the data are also possible; for example, data might be captured directly by a laptop, or transmitted directly from the PDA to the corporate database.

Each circle in the diagram represents data in motion and each box represents data at rest. Data is moving when captured, downloaded, transmitted, summarized and retrieved by field agents. During this process, the data is at rest twice in PDAs, in a laptop and within corporate databases. The backup media are at rest, but they need to be located offsite and therefore must be transported to that site.

To continue the example, each step presents a different set of risks:

- *Capture of data:* This step could involve manual input with its inherent risk of human error, or it could involve the use of short-range frequencies such as Bluetooth, which run their own risk of detection by other nearby electronic devices.

- *Download:* A download through a wired connection should be relatively risk free, except for the possibility of human error. A wireless download risks detection by another nearby electronic device.
- *Transmission:* Data will most likely be transmitted over the Internet. The degree of security for such transmissions varies among organizations. Some use VPN to enhance security; others allow standard email messaging. Unless a very effective security system is in place, the risk of the data being read by the wrong people is relatively high.
- *Summarization:* Summarization requires the data to be moved into an application of some kind. Security then depends on the controls in place for that application and for the environment in which the application functions.
- *Retrieval by field staff:* When the field staff retrieve the data, they likely use some Internet-based method, perhaps similar to that which was used initially to transmit the data. Accordingly, similar risks apply. In addition, the risk of unauthorized persons accessing the data transmissions by field staff depends on the strength of those data-transmitting capabilities.

The power of these devices to copy or modify captured data raises the additional issues of controlling the ability of users to perform these actions, as well as ensuring the security and integrity of new copies or versions and their storage location(s).

As noted, the data is at rest at various points in this example:

- *PDA:* These small hand-held units are, of course, very vulnerable to loss or theft. While they usually have some security features (such as passwords), such features can be ineffective, especially if the unit is stolen. Some newer versions also have Wi-Fi connectivity, which increases the risk of transmitting data over unsecured networks.
- *Laptops:* As noted in Appendix B, there have been numerous incidents of sensitive private data being compromised when a laptop was lost or stolen. Many laptops have very good security features, particularly those based on encryption. However, one survey revealed that 46% of organizations do not use encryption.¹
- *Corporate Database/ERP/CRM:* Data resident inside the firewall of a corporate system should be easily controlled because it falls directly under the core system's security procedures. Of course, all the traditional elements of good security systems must be in place, such as segregation of duties, access control, physical control and monitoring.

Phase 2: Data Loss Risk Assessment

A data loss risk assessment should be carried out on each system to determine the controls appropriate to each one's risk of data disclosure or corruption, and the risk the organization is willing to assume. It is not reasonable to assume that all data in the organization needs to be controlled to the maximum degree; such an approach would be expensive and result in unnecessary controls. For example, some customer information gathered by the field staff may be considered public and need not be controlled; other data may be private and sensitive and therefore needs to be controlled.

Guidance contained in the following is useful in carrying out risk assessments: COBIT 4.1 *Risk and Control Objectives*, and the CICA publications,² *Information Integrity Guidelines* (to be published by the CICA in 2010). and *Secure IT Infrastructure for E-commerce*.

The data loss risk assessment must take into account the sensitivity of the data and its locations throughout the organization, whether at rest or in motion.

Classifying the Data

A first step in the assessment is to classify the data according to risk factors, such as:

- *Public*: Data whose release would have little or no negative impact on the organization.
- *Internal Operational*: Data needed by company personnel in the course of their work and not intended for public dissemination.
- *Confidential*: Data regulated by privacy legislation (or deemed confidential by contractual obligations) whose release could cause legal difficulties and/or embarrassment.

Management must also consider the possible loss of reputation or competitive advantage, regulatory and legal sanctions, and breach of contract if data falls into the wrong hands.

Even after inherent risks have been identified, residual risks remain. After installing the mitigating controls for the inherent risks, additional compensating controls can reduce the residual risks to an acceptable level.

Phase 3: Applying Controls in a Data-Centric Policy

Controls must be applied to those parts of the system where the data is most susceptible to unauthorized access, whether residing on a device or moving from one device or unit to another.

Encryption: A Key Data-Centric Security Control

Encryption is a key control in a data-centric system because the data is moving across different systems and is often open to attack from various sources along the way. Encryption is the most effective way to protect data in motion. This does not mean that encryption needs to be applied in all cases, but it does mean that it is normally appropriate to develop an encryption strategy as a subset of the overall control strategy. Therefore the direct result of the risk analysis is the identification of which data needs to be encrypted. In some cases, it is simply not possible to encrypt data; for example, many mobile devices do not have effective security capabilities. In these cases, alternative controls need to be developed.

In those recent cases where the loss of a computer hard drive or back-up media in transit has put private data at risk, the risk would have been substantially reduced if the data had been encrypted.

Role of Encryption

The power of encryption to protect data at rest or in motion makes it one of the most powerful controls to consider if strong protection is needed. Wherever possible, a single encryption methodology, such as one based on the PGP (Pretty Good Privacy) standard, should be used throughout the organization so that data can be easily recovered if the encryption keys are lost or corrupted. It is normally not sufficient to make use of the encryption technologies that exist in the various repositories of information, such as laptops, PDAs or cell phones, or technologies such as Wi-Fi or Bluetooth.

A single encryption methodology must be used throughout the organization because:

- files that have been encrypted must remain accessible in future years for business, audit, tax and other regulatory purposes. Therefore the organization must control the decryption technologies and keep the cryptography keys;
- since the systems within which the data may be travelling are likely to be of different sizes, the encryption process must be scaleable in order to operate as effectively on a single small computer as it does on several large systems;
- as data moves from platform to platform, the encryption solution must work on any significant platform in the system;
- without a single encryption technology in place, any data will have to be decrypted for use and then re-encrypted after use.

Encryption Standard

Different levels of encryption require the use of encryption keys of varying lengths. The most common lengths are 64 and 128 bits, although lower and higher levels are available. The 64-bit encryption level is generally inadequate for the protection of corporate data. The 64-bit DES algorithm has been broken many times in the past and is now broken routinely. Encryption policy should therefore specify at least the 128-bit level, which should be adequate for most purposes.

Key Management

The management of public and private keys is an important part of any encryption policy. As noted in ISO/IEC 17799:2005, key management includes:

- generating keys
- obtaining public key certificates
- distributing keys
- storing keys
- updating/changing keys
- procedures to manage compromised keys
- procedures to revoke keys
- recovering lost or corrupted keys
- managing keys that decrypt backups
- audit trails associated with key management processes and procedures.³

If keys are unprotected or poorly managed, the risk is increased that the encryption will be violated.

Although all organizations need basic key management controls, they vary in rigour and expense from organization to organization. For example, it is usually appropriate for key management to be fully automated and for private keys to be kept confidential; all keys, however, must be encrypted. Keys used to encrypt other keys must be different from the keys used to decrypt data. Short-life keys should, wherever possible, carry activation and deactivation dates. It is important that keys be chosen randomly. A detailed list of key-management procedures is available from VISA entitled *Payment Card Industry PIN Security Requirements*.⁴

Controlling Data Removal Points

Another technique to help control data risk is to control data removal points. These include USB ports and recordable CD/DVD drives. Data may be extracted through these points and used in an unauthorized manner. Control over data removal points can be achieved through:

- *Endpoint management solutions:* Technology-enabled controls can manage the connection and use of devices. For example, such technologies can monitor file transfers through the USB port/disc drive and limit the use of “copy and paste”. These tools can be purchased as part of a comprehensive data loss prevention solution.
- *Disabling USB ports, CD/DVD drives:* Where the ports and drives are not required for operational reasons, such as back-up, these controls can disable them. For example, USB ports on computers in a call centre could be rendered non-operational to prevent unauthorized employee use.

Portable Electronic Device Controls

Laptop thefts and losses are common. Consequently, hardware controls are particularly relevant to a data-centric policy because portability and other characteristics of this type of hardware are inherent risks. Data can also be exposed in ways other than theft or loss; for example, laptops can be subject to search and seizure when crossing international borders. These risks can be mitigated in the following ways:

- *Multi-factor authentication:* Because encryption on laptops can be bypassed by sophisticated users, organizations should investigate the use of multi-factor authentication, such as the combination of passwords with biometrics or with USB-based token-access devices.
- *Installation of tracking software:* Tracking software allows the laptop to transmit a signal when connected to the Internet. This software can also disable the laptop and/or delete all the data. Laptops using this software should carry a label warning potential thieves the laptop will be tracked if stolen.
- *Use of laptop as a terminal instead of a storage device:* A laptop used as a terminal requires centralized data storage, the use of terminal services, secure connection (e.g., VPN) and controls to prevent users from intentionally or unintentionally storing data on their laptops. More companies are using the Internet or their own servers to store data and allow no storage on the laptops. Some companies are beginning to use “Netbooks” to store data on the Internet.

Data Loss Prevention (DLP) Monitoring Tools

Some organizations have begun to use the relatively new “data loss prevention” (DLP) monitoring tools to identify any data leaks. More information on DLP can be obtained from the sites of the various vendors.

Information Release Procedures

To help control data leakage, management should review how data is passed to external parties. Strict standards of authentication should be in place before any external party is given private information. For example, employees should have a procedure for verifying the identity of couriers.

Contracts with third parties or other independent entities should contain terms including penalty provisions to protect shared data. Management should be allowed

to audit data-centric security controls or be entitled to receive a CICA *Handbook* Section 5970 audit, a SAS 70 report, or a Trust Services engagement attesting to the operating effectiveness of data-centric security controls. Management should also require the third party to give notification of any breach.

Phase 4: Formalizing the Data-Centric Security Policy

Once Phases 1 to 3 are complete, management can formalize and approve a formal data-centric security policy and release it to users. The policy should be a reference point for data management throughout the organization. Elements of a sample data-centric security policy are provided in Appendix A.

CONCLUSIONS

The use of different communication and storage devices by employees and external third parties requires modern corporations to develop data-centric security policies that allow data to be tracked throughout the system because most systems are connected with various types of hardware. This operating environment exposes the organization to data leakage through loss or theft of portable units and/or violation of the security available for specific units and/or loss of data resident in an abnormal place or while being transmitted over insecure media.

Only a coordinated security policy that can locate the data at any moment and identify and counter the risk of unauthorized access will be effective. Even a well-designed policy that meets these criteria can only produce results if it is communicated to employees who believe in its value and are trained in its use.

APPENDIX A: SAMPLE DATA-CENTRIC SECURITY POLICIES

[Note: These samples can be customized to meet the needs of a particular organization.]

Data is the lifeblood of the organization and must be protected. However, it is at risk of unauthorized access because it is constantly moving between devices and units both inside and outside the organization. The most effective means of protection is encryption. This policy sets out the design principles for a data security policy using 128-bit encryption as a standard. An annual risk analysis should follow the data flow to evaluate the adequacy of the controls.

Data at rest and data in motion present two different control problems. Data at rest is usually contained in systems that are (or should be) protected with standing security systems. Data in motion passes through other systems, some of which might require additional precautions because they are not under the control of the data owner.

DATA AT REST

Fixed Media

- Protect corporate data at rest in fixed media such as corporate servers located in a secure area by a firewall having strict access controls.
- Connect the controls to a Virtual Private Network (VPN) so that any data moved from one server to another will be encrypted.
- Secure systems storing or transmitting data by antivirus software or other such protection. Turn off unneeded services or ports and have properly configured applications.

Removable Media

Removable media include CD-ROMs, floppy disks, backup tapes, USB memory drives and any other portable units that can contain data.

- Encrypt all removable media containing corporate data and store in a secure, locked location, i.e., do not use passwords.

DATA IN MOTION

Transmission Security

- Encrypt all email messages containing corporate data.
- Encrypt all corporate data to be transmitted through a public network such as the Internet or use an encrypted tunnel.
- Encrypt the tunnels with 128-bit public-key encryption such as is used in the corporate Virtual Private Network (VPN) or in point-to-point tunnel protocols (PPTP) like Secure Shells (SSH) and secure socket layers (SSL).
- Encrypt wireless (Wi-Fi) transmissions with WPA or higher.

Removable Media

- Identify, authenticate and prove the authority of any recipient before removable media are transported.

- Transport media in a secure manner with an approved and documented transportation company using an approved packaging method, means of transportation and tracking capability.

Portable Devices

- Encrypt corporate data stored on portable devices such as laptops and personal digital assistants (PDAs).
- Do not use portable devices for long-term storage of corporate data.
- Install antivirus software, firewall software and encryption in all portable devices that store or transmit corporate data.
- Turn off unneeded services and ports.

KEY MANAGEMENT

- Use the corporate PKI wherever possible. Users must be expressly forbidden from using non-corporate encryption standards or tools.
- Automate key management.
- Encrypt all keys and keep private keys confidential.
- Separate and distinguish keys for encrypting keys from keys for decrypting data.
- Use short-life keys with activation and deactivation dates wherever possible.
- Choose keys randomly.
- Load keys using two individuals.⁵
- Divide key's knowledge between two individuals. No single individual should have complete knowledge of the key.⁶

APPENDIX B: EXAMPLES OF DATA LEAKAGE

Data leakage through loss or theft of laptops, mobile phones and PDAs has become commonplace. For example, ComputerWeekly.com reported on September 19, 2008: "A survey of London taxi drivers, carried out by Credant Technologies, indicates that 55,843 mobile phones and 6,193 other devices, such as laptops, have been left in the back of black cabs over the past six months. This is consistent with a survey carried out a few years ago by Pointsec, which showed that in the last half of 2004, 63,135 mobiles, 5,838 PDAs and 4,973 laptops were left behind in London taxis."

According to a 2007 survey of UK companies conducted by PricewaterhouseCoopers, 72% of large companies experienced a security breach that exposed the company to the "loss of confidential data".⁷ In another survey, the Poneman Institute found that 85% of "C-level executives" interviewed had experienced a data breach.⁸ The most common risks causing such breaches were inadequate control of:

- portable electronic devices
- storage media/devices
- the disposal process for records and data-storage devices
- access to strategically sensitive information, and
- the procedure for releasing information.

Specific incidents within each of these areas are discussed below.

Portable Electronic Devices

One study determined that, within the U.S., 1,000 laptops go missing daily and only 3% of these laptops are recovered.⁹ PDAs (Blackberrys, etc.) also face similar risks. Examples of such incidents include:

- February 2008: National Institutes of Health had a laptop stolen containing unencrypted data on approximately 2,500 patients in a research project.¹⁰
- May 2006: U.S. Department of Veteran Affairs (VA) had a laptop stolen containing 26.5 million records including birthdates and social security numbers.¹¹
- February 2006: A laptop belonging to Hotel.com containing 243,000 customer records including "names, addresses and credit- or debit-card information" was stolen from the car of an Ernst & Young auditor.¹²
- May 2005: A laptop was stolen containing the credit card information of 80,000 U.S. Justice Department employees.¹³

Storage Media and Devices

Back-up tapes, drives, and other storage devices are also susceptible to loss or theft. For example:

- April 2008: HSBC lost a disc containing 370,000 records including names, birthdates and other personal information.¹⁴
- November 2007: HM Revenue and Customs in the UK lost discs containing information on child benefit claimants affecting 25 million people.¹⁵
- May 2007: Alcatel-Lucent could not locate a disc containing personal information including "name, address, date of birth, social security number and salary date"¹⁶ of more than 200,000 employees, retirees and their dependants.¹⁷

- February 2007: the Canadian Imperial Bank of Commerce's mutual fund subsidiary, Talvest, lost a backup drive containing the personal information of 470,000 clients.¹⁸

Disposal of Files and Storage Devices

Another category of concern is the insecure disposal of data. For example, the Bank of Montreal accidentally sold servers containing “names, addresses and phone numbers of several hundred clients, along with their account information, including account type and number, balances and, in some cases, balances on GICs, RRSPs, lines of credit, credit cards and insurance”.¹⁹ In another incident, Select Physical Therapy was charged by the Texas attorney general with “violating identity theft protection laws”²⁰ for dumping “4,000 pieces of sensitive customer information in garbage containers”.²¹

Strategically sensitive information: Although the theft of data by competitors is not a well-publicized issue,²² it is nevertheless a risk that needs to be managed. For example, Thomas Stemberg, co-founder of Staples Inc., openly admitted that he sent his wife as a new hire into Office Depot to determine how their new delivery system worked.²³ From the perspective of data-centric security, mass storage devices can be connected by malicious users to uncontrolled USB ports to illicitly obtain trade secrets or other sensitive data.²⁴ Employees can also use webmail (e.g., Gmail, Hotmail, etc.) to email sensitive files offsite. For example, Shin-Guo Tsai used his personal email account to obtain strategically sensitive product information sold by Volterra, the company he worked for. After being questioned by law enforcement, he allegedly admitted that he obtained this information for the purposes of giving it to a Taiwanese start-up that was recruiting him for a job.^{25,26} In another incident, an executive of an IT security company had his laptop containing unencrypted blueprints for the company's key products stolen at gunpoint.^{27,28}

Release of Data to Unauthorized Parties

Another cause of data leakage is poorly designed controls that accidentally grant unauthorized access to data. The extent of this problem was demonstrated by a contest where contestants found sensitive information (e.g., names, credit card numbers, etc.) for approximately 25 million people — solely by using the Google search engine.²⁹ In December 2007, Passport Canada reported a security breach that allowed individuals applying for passports to access the records of other applicants by editing the Internet address in the web browser.³⁰ In 2004, Choicepoint Inc. suffered a widely publicized breach where the company divulged the personal information (e.g., credit histories) of 163,000 customers to fraudsters because it had failed to perform due diligence on the companies receiving the information.³¹ Choicepoint was fined \$10 million by the FTC and required to pay \$5 million in consumer redress to the 800 affected individuals for violating consumers' privacy rights and federal laws.³²

Email, Instant Messaging (IM), and Other Electronic Communication Channels

In a survey conducted in 2007, respondents felt on average that 20% of their out-bound email was a “legal, regulatory or financial risk to their organizations”.³³ The survey also found that nearly 40% of companies (with more than 20,000 employees) hire employees to analyze the contents of outgoing email.³⁴

According to Gartner, IM applications impose risks on the organization because there is no standard encryption mechanism to protect messages sent. The absence of “universal naming conventions” prevents the resolution of disputes over what was communicated to whom, and employees are able to circumvent acceptable-use policies because these communication channels cannot be monitored.³⁵

Endnotes

- 1 Dubie, Denise: "Data breaches plague U.S. companies", *Network World*, Vol. 24, Issue 20, p. 25 (Southborough: May 15, 2007). See www.networkworld.com/news/2007/051507-data-breaches.html [Accessed August 15, 2008.]
- 2 Available from www.cica.ca.
- 3 International Standards Organization, *Information technology – Security techniques – Code of practice for information security management (ISO/IEC 17799:2005)*, 2nd ed. (Geneva, Switzerland: June 15, 2005).
- 4 Visa International, *Payment Card Industry PIN Security Requirements (Visa Public 40026-02) (2004)*. See https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=95 [Accessed August 6, 2008.]
- 5 Visa International, *Payment Card Industry PIN Security Requirements (Visa Public 40026-02) (2004)*. See https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=95 [Accessed August 6, 2008.]
- 6 *Ibid.*
- 7 "Large company" was defined as employing more than 250 people; Kieran Poynter, "Good data security is not just a matter of technology", *Financial Times*, (London, UK: July 16, 2008), p. 13.
- 8 Denise Dubie: "Data breaches plague U.S. companies", *Network World*, Vol. 24, Issue 20, p. 25 (Southborough: May 15, 2007). See www.networkworld.com/news/2007/051507-data-breaches.html [Accessed August 15, 2008.]
- 9 Andy Dornan, "It's audit time. Do you know where your private data is?" *IT Architect* (Manhasset: September, 2005), Vol. 20, Issue 9, pp. 35-41.
- 10 Mary Mosquera, "Stolen laptop reveals security gap", *Federal Computer Week* (Falls Church: March 31, 2008), Vol. 22, Issue 7, p. 9.
- 11 Larry Greenemeier, "No More Excuses", *InformationWeek* (Manhasset: May 29, 2006), Issue 1091, pp. 23-25.
- 12 Reuters News Service, "Hotels.com: Credit-Card Data Is Lost In Stolen Laptop Computer", *Wall Street Journal*, Eastern edition (New York, NY: June 6, 2006).
- 13 Gary Fields, "Stolen PC Had Credit-Card Data For 80,000 Government Workers", *Wall Street Journal*, Eastern edition, (New York, NY: May 31, 2005), p. A.4.
- 14 Jane Croft, "HSBC apologizes for loss of customer data", *Financial Times* (London, UK: April 8, 2008), p. 4.
- 15 *Ibid.*
- 16 Anonymous, "Alcatel-Lucent unable to locate disk containing personal employee information", *Telecomworldwire* (Coventry: May 18, 2007), p. 1.
- 17 Nikki Swartz, "Losses Highlight Need for Physical Data Security", *Information Management Journal* (Lenexa: July/August 2007), Vol. 41, Issue, 4; p. 17.
- 18 Darren Charters, "Addressing privacy breaches", *CMA Management* (Hamilton: February 2008), Vol. 81, Issue 9, p. 34.
- 19 "BMO computer hard drives with sensitive info were on EBay auction site", *Canadian Press* (September 15, 2003).
- 20 "Texas AG accuses rehab center of dumping sensitive customer info", *Associated Press* (January 10, 2008). See www.kxan.com/global/story.asp?s=7606095 [Accessed August 4, 2008.]
- 21 *Ibid.*
- 22 Shane W. Robinson, "Corporate Espionage 201", *Information Security Reading Room* (SANS Institute: 2007). [Accessed July 31, 2008]
- 23 Richard B. Elsberry, "The spying game: How safe are your secrets?" *Office Systems* (Mt. Airy: September 1999), Vol. 16, Issue 9, pp. 42-46.

- 24 *Ibid.*
- 25 *Ibid.*
- 26 Birgitta Forsberg, "The spies in the next cube", *The San Francisco Chronicle* (April 25, 2005). See <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/25/BUGGLCDPUJ1.DTL> [Accessed August 4, 2008.]
- 27 Andy Dornan, "It's audit time. Do you know where your private data is?" *IT Architect* (Manhasset: September, 2005), Vol. 20, Issue 9, pp. 35-41.
- 28 *Ibid.*
- 29 Raymond J. Elson and Rey LeClerc, "Customer Information: Protecting the Organization's Most Critical Asset from Misappropriation and Identity Theft", *Journal of Information Privacy & Security* (Marietta: 2006), Vol. 2, Issue, 1, p. 3.
- 30 Kenyon Wallace, "Passport applicant finds massive privacy breach," *The Globe and Mail* (December 4, 2007), p. A1.
- 31 Christopher Conkey and Ann Carrns, "ChoicePoint to Pay \$15 Million to Settle Consumer-Privacy Case", *Wall Street Journal*, Eastern edition (New York, NY: January 27, 2006), p. A.3.
- 32 *Ibid.*
- 33 Ben Murray, E-mail: "Source of Risk to Companies", *Strategic Communication Management* (Chicago: August/September 2007), Vol. 11, Issue, 5, p. 9.
- 34 *Ibid.*
- 35 John Ginovsky, "An Emerging Corporate Threat: Instant Messaging", *ABA Bankers News* (Washington: July 4, 2006), Vol. 14, Issue 14; p. 8.

