Data Leakage: Affordable Data Leakage Risk Management

By Joseph A. Rivela
Senior Security Consultant

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

The Problem

In recent years, the hardship of preventing and containing the loss of sensitive data has done nothing but increase for many organizations. Incident rates are on the rise, organizational liability is high, and the risk of identity theft is pervasive.[1] Particularly vulnerable are industries and organizations bound by work processes and procedures that involve the acquisition, processing, retention, transmission and destruction of what information security professionals have dubbed *Personally Identifiable Financial Information* (PIFI) and *Personally Identifiable Health Information* (PIHI). More generally, this data is referred to collectively as *Personally Identifiable Information* (PII).

PII is all of the sensitive and nonpublic customer information an organization possesses. Some examples include: Social Security numbers, credit card information, insurance numbers, driver's license numbers and medical information specific to an organization's employees or the consumers to whom it provides service.

As consumer bases and organizational services expand, the amount of data and PII retained increases. And as an organization processes and/or maintains more PII data, the more at-risk it becomes for incidents of *data leakage*. Data leakage refers to situations in which sensitive or otherwise confidential data escapes organizational infrastructures, making that data vulnerable to potential unauthorized disclosure or malicious use. Mitigating the risks of handling such data and leakage can be an expensive undertaking.

Compliance and Data Leakage

Fortunately, due to industrial or governmental compliance requirements, many enterprises, organizations and institutions are forced to resolve risks associated with data leakage.

Payment Card Industry (PCI) compliance,[2] a well-known collection of requirements initially passed down by major credit companies, requires entities that process card transactions to comply with 12 data security rules in order to protect themselves from financial penalties. These requirements mandate the existence of controls, such as firewalls protecting organizational web applications that restrict access to warehoused credit card data; the encryption of such data while "at rest," rendering it finitely illegible to an attacker; and the regular review of organizational security to ensure compliance with current security standards. Such requirements facilitate the mitigation of data leakage risk and organizational liability.

More traditional governmental compliance also provides for rules and regulations directly or indirectly aimed at the prevention of data leakage. Provisions of the Sarbanes-Oxley Act of 2002 require that organizations focus on the information security best practice known as "least privilege access." Least privilege access exists to limit the exposure of sensitive data to only those individuals who have exhibited the appropriate need-to-know or need-to-have access, while allowing for the accomplishment of their specific job functions. Additionally, the Sarbanes-Oxley Act provides for individual accountability and change management procedures that assist in the identification of data leakage liabilities and occurrences.

[1] As described in Symantec's Internet Security Threat Report Volume XI with respect to data collected by Symantec from July 1, 2006 to December 31, 2006.

[2] The PCI data security standard (DSS) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

However, there are a multitude of organizations not bound by industrial or governmental compliance regulations. This type of organization may not maintain transactional data, could exist as a private entity absent of external stakeholders or may not be subject to other industry-driven compliance initiatives, such as Health Insurance Portability and Accountability Act (HIPAA) regulations. However, despite their potential absence of mandatory compliance responsibilities, these organizations still strive to maintain the confidentiality of consumer data in an effort to sustain their organizational reputation, demonstrate their ethical responsibility, maintain consumer confidence, and avoid any legal repercussions associated with data loss or the costs of data breach reporting.

This self-driven practice is commendable. Security professionals can learn much from organizations that have approached security for the sake of being secure and not compliant and, thus, have implemented security controls to mitigate data leakage.

Often, organizations operating outside the jurisdiction of federal regulation and industry-mandated compliance are relatively small operations with few employees and low revenue streams. However, despite their size, mandatory security requirements or specific business processes, there are several points of failure at which small organizations may have data leakage vulnerabilities similar to those exhibited by larger entities. Further, when such vulnerabilities are present, they may expand throughout an organization, rather than being specific to an individual unit, division or location. It is because of these commonalities that the following affordable solutions, successfully implemented in smaller scale organizations, most likely also will be effective in larger business environments.

Affordable Solutions

The affordable steps to be outlined exist as tactical, low-cost, security advancements that organizations may elect to implement to decrease the vulnerabilities that contribute to data leakage. These processes are affordable, and easily scaled and implemented. Such measures exist to complement a more comprehensive security plan, which may include the implementation of security technologies, the acquisition of experienced security personnel or the retention of security services firms; together they will have a positive impact on an organization's overall information security posture.

Such steps may be implemented to achieve security and accomplish data leakage prevention by way of deterrence, detection and defense (Figure 1-1).

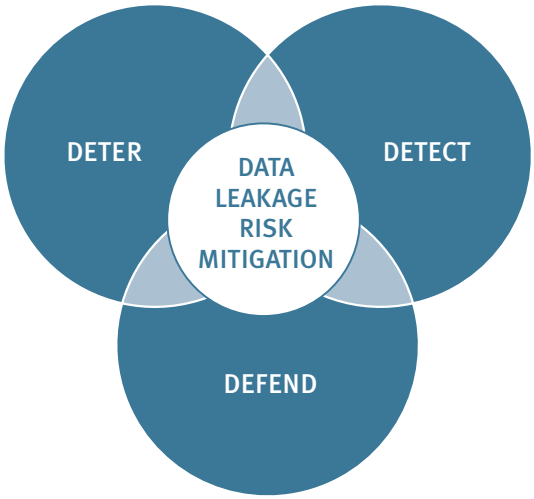

Figure 1-1

Deterrence measures are designed to prevent a less casual or opportunistic attacker from attempting to circumvent security in an effort to achieve a noncompliant end. Controls that allow for deterrence – such as an overarching security policy – are primarily administrative in nature. Deterrence can be considered the prevention of an attack prior to an occurrence. Deterrence leverages predictive analysis to create proactive controls.

Detection allows for the identification of potential attack situations executed by a more casual attacker. As illustrated in Figure 1-2, examples of such attack activity may include network reconnaissance or the excessive duplication of sensitive documentation. Either activity may be indicative of more malicious behavior. Controls allowing for detection are primarily technical and physical in nature. Technical examples include system logs, intrusion detection systems or failed log-in attempts. However, physical examples may include the identification of potentially malicious activity by informed and aware personnel.[3] Detection leverages an organization's reactive capability to preserve the security of sensitive data.

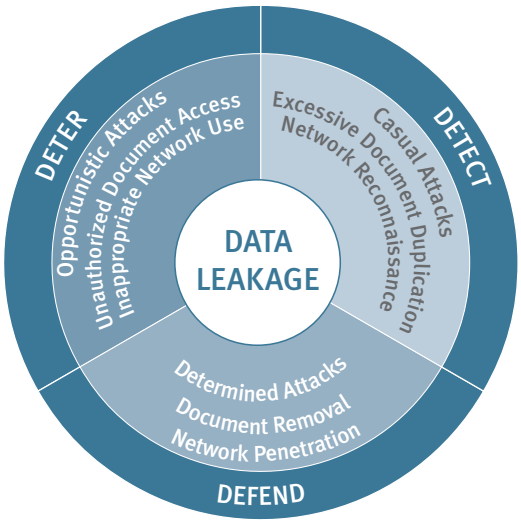

Figure 1-2

Defense is the prevention or suppression of attacks already in progress and commissioned by a determined attacker. Examples of attacks may include the attempted penetration of an organization's internal network via password-guessing or the removal of sensitive documentation from the organization's facilities. Factors contributing to defense can be administrative, technical or physical in nature. Defense capabilities are enhanced greatly by the existence of administrative controls, such as a developed "Incident Response Plan" and a trained and diversified "Incident Response Team," as well as the existence of developed vulnerability, patch and change management programs. Additional technical controls allowing for defense include regularly monitored and updated firewalls and the use of proven cryptographic solutions with respect to all sensitive data.

Sun Tzu, whose wisdom regarding military strategy and martial art remains timeless, and is applicable to many aspects of the modern business world, wrote that *"... the rule of military operations is not to count on opponents not coming, but to rely on having ways of dealing with them."*[4] Thus, it is essential for businesses to anticipate that their "opponents" will – if provided the opportunity[5] – either intentionally *or* unknowingly put organizationally maintained PII at risk.

Following are affordable solutions for deterrence, detection and defense.

Policy, Standards, Procedures and Guidelines

Seasoned security professionals should be familiar with the benefits of strong documentation, specifically, the benefits of complete and effective policies and standards. These documents are regarded as "must-haves" in the security arena due to requirements under a variety of compliance directives. Unfortunately, some organizations maintain such documents simply so they may "check off another box" with respect to an audit, instead of driving secure procedures and standards. This is not a new phenomenon.

Problems that might arise from adopting a policy for the sake of compliance may include:

- **Extravagant Policy:** Excessive requirements outside an organization's capabilities
- **Incomplete Policy:** Focus is on compliance rather than security; lacks direction
- **Conflicting Policy:** Results from disorganization or a lack of centralization

[3] Ongoing awareness programs are described by Kevin Mitnick and William Simon as "vital" in *The Art of Deception: Controlling the Human Element of Security*.

[4] As translated by Thomas Cleary in *The Art of War: Complete Texts and Commentaries*.

[5] One-third of the key contributory factors to fraud, as explained by Steve Albrecht et al. in *Fraud Examination*.

While extravagance might not greatly impact data leakage, it often makes it difficult for organizations to be compliant with their own policies. Incomplete and conflicting policies are more challenging to data leakage prevention. To achieve security success, it is important for an organization to provide a clear and complete vision and approach, which must resonate throughout all policies and standards and, also, be reinforced. Each of the aforementioned policy shortcomings will only create confusion and lead to noncompliance with respect to organizational goals.

Almost as important as policy (from a security perspective) are organizational procedures and guidelines. The completeness, let alone the existence, of these types of documents often is overlooked by regulatory directives, but they are arguably the strongest drivers of compliance. Procedures and guidelines aid both security and nonsecurity personnel in accomplishment of goals set forth in policies and procedures. An organization's senior management, process owners and security personnel should work together to establish and maintain processes and guidelines that facilitate the secure accomplishment of organizational activities, as well as foster compliance with an overarching policy. Participation in development, enforcement and maintenance of such documentation is a testament to an organization's dedication to performing due care and diligence with respect to the protection of PII.

Organizations also should abide by security best practices, both general and industry-specific, and include them in the development of organizational documentation (policies, standards, procedures and guidelines). Documentation should be controlled centrally and made readily available to all applicable personnel and management. Also, internal audit or information security units should monitor such administrative controls regularly to ensure compliance.

In 2007, the IT Policy Compliance Group[6] released the results of a study that documented 16 leading causes of data loss. The second highest contributor, averaging one in every four incidents, was identified as "violation of policies." Considering the negative impact of policy violations, management should include policy provisions describing the repercussions of noncompliance; implement administrative, physical and technical mechanisms to detect violations; and enforce those provisions of policy regularly.

Locking It Down

Securing sensitive data or the means to accessing that data is often the first step toward an environment less susceptible to data leakage.

Hard copies of documentation are often the most susceptible to either physical theft or unauthorized duplication and removal from business premises. There are several means by which an organization can ensure the protection of hard copy documentation. A very common – and severely underutilized – means of accomplishing this usually is readily available: locks. Most workplaces are filled with cabinets and drawers for storing hard copy documentation. Thus, security personnel should champion the maximum utilization of this available storage space, as well as secure locking mechanisms.

As with any security precaution or measure, personnel may associate the implementation of such security measures with a loss of productivity. Provided that security staff can demonstrate their ability to accomplish the following tasks quickly and with little disruption, personnel usually can be persuaded to implement such precautions:

- Identify appropriate personnel who require access to specific documentation
- Control the distribution of keys
- Maintain readily available backup or master keys

In an article titled the "Security Expert's Top 5 Tips to Combat Identity Theft," Todd Faro of Compliance Cabinets offered tips for securing physical documentation and limiting the accessibility to and availability of sensitive PII from determined attackers seeking to commit identity theft and other fraud. Among his suggestions, Faro reminds readers that even though locking mechanisms may have been integrated into an

[6] ITpolicycompliance.com (www.itpolicycompliance.com) is dedicated to providing public and private organizations with the latest research focused on best practices for IT policy and compliance.

organization, users should avoid specific activities that would diminish the effectiveness of such devices and allow users to circumvent security controls. As an elaboration to the article, users and security personnel should:

- Avoid leaving their keys (or combinations) in common storage areas such as:
  - Unlocked desk drawers
  - Underneath keyboards and monitors
  - Affixed to desk bottom surfaces
- Refrain from displaying any information specific to the locking mechanism that might allow an attacker to learn any information about that mechanism's operations (e.g., brand, model)
- Research locks and ensure that those implemented have been subjected to testing and given an acceptable designation (Grade 1) by the American National Standards Institute
- Subject locking mechanisms to organizational testing and ensure documented security "enhancements" are not bypassed easily

Finally, regardless of their maker's advertisements, locks are only "pick proof" or defensible for a certain amount of time. If a lock is able to withstand only one week of attack, then it would not be effective to monitor it only once a month. Locking mechanisms would be best complemented by monitoring mechanisms, such as roving security patrols or the implementation of closed-circuit security cameras.

Data Classification

A common cause for the misappropriation of data is a general lack of understanding about the data's significance, relevance to other materials or overall sensitivity. Therefore, organizations should implement a structured and uniform data classification standard that prompts data handlers to treat sensitive data with the level of respect and security required.

Data classification is often considered a cornerstone or prerequisite to successful risk management practices.[7] In addition to driving data handling, classification provides senior management with information vital to making decisions specific to the security of sensitive information or assets. Assets subject to data classification may consist of file servers, web servers, databases or SANs. Other assets that often evade formal classification are CDs and USB drives.

Data or asset classification may be determined in one of several ways. When considering PII, an organization may designate its highest classification to those pieces of information that are most sensitive to its consumer (e.g., Social Security numbers and credit card numbers). Loss of this information in an unencrypted format is normally associated with breach disclosure requirements, reporting costs, and damage to brand or reputation.

A different approach might be to assign classifications following a formal Business Impact Analysis (BIA). This process will aid in the identification of data and assets that are most critical to an organization, drive the prioritized recovery of computing systems and ultimately recover critical business processes as part of broader contingency planning strategies.[8]

Naming conventions for both government and nongovernment entities are well-known when it comes to data classification. To prevent data leakage, organizations should adopt a model of classifying data conducive to their operations. All data maintained should be identified, and the level of damage that could occur if data is compromised or lost should be anticipated.

Classifications also should be marked clearly, and policies and standards regarding data classification should be audited and enforced regularly.

---

[7] Himanshu Dwivedi describes the process of risk management starting with data classification in *Securing Storage: A Practical Guide to SAN and NAS Security*.

[8] Defined as the "Entire planning conducted by the organization to prepare for, react to and recover from events that threaten the security of information and information assets in the organization …" in *Principles of Information Security* by Michael E. Whitman and Herbert J. Mattord.

Network Use Restrictions

Securely storing and classifying documentation is only one of many ways for an organization to prevent the unauthorized removal of data and PII, and is just one step toward the protection of such information residing in tangible forms. Data existing in a logical format and residing in databases or systems still could be at risk, regardless of the implementation of physical security controls.

Without dedicating mass amounts of man-hours and/or finances to the mitigation of operating system and application-related vulnerabilities, there are some controls that a budget-bound IT organization might implement to reduce the risk or opportunity for data leakage stemming from poor machine or access configurations. Such controls may include the restriction of:

- Outbound e-mail (including e-mail forwarding)
- Internet accessibility:
  - Blogging
  - Access to personal e-mail (e.g., Yahoo!, Hotmail, G-mail)
  - Messaging services (AIM, Windows Messenger, Yahoo! Messenger)
  - Internet Relay Chat (IRC)
- Use of USB devices
- Command line access
- FTP/SFTP functionality
- eFax

If the aforementioned privileges are not limited or restricted, they may empower a malicious user to export sensitive data from the confines of where it was intended to be used. Initially, users should be restricted from all such privileges and must justify their business need and obtain the appropriate approvals. Security personnel should elect to discuss network restrictions with senior management prior to implementation, as such activity may have been approved previously under acceptable use policy or may negatively impact the performance of network maintenance. However, excessive network permissions should be recognized as highly probable avenues of data leakage and should be monitored closely.

Manage Vendor Relationships

Concerns about data leakage should not be limited to data processed, stored and managed within the confines of an organization, but rather, should include all data for which the organization can be held responsible. In an effort to protect such data, organizations should review their contractual arrangements with third parties regularly to ensure those parties are contractually bound to the provision of secure services. Organizations also should further ensure the safety of their data by participating in an assessment or audit of their vendors, so they can make sure documented controls are implemented in accordance with negotiated agreements.

Of the security controls that vendors might be asked to implement, organizations should require restricted access to their data, both logical and physical. This might mean the implementation of securely locked cabinets, drawers and doors, with tightly monitored access to sensitive materials, the use of key cards, and required use of “strong” passwords or phrases. These are just a few suggestions for creating a more secure

environment for data storage. The aim of secure storage is, of course, to accomplish and maintain the integrity, availability and, with respect to data leakage, confidentiality of sensitive information. An example of an "expensive" method for accomplishing secure storage might be the implementation of biometric access controls or the adoption of an inline encryption solution.

But access to sensitive data is only a small piece of the data leakage problem. Organizations need to be cognizant of the issues surrounding data leakage in all aspects of the data life cycle. It is not enough to secure the data while it is maintained; a good security practitioner will ensure the data is created in a sound and secure manner; outfitted with the appropriate data classification, per data classification standards; and maintained and destroyed in accordance with that classification.

Organizations must not only ensure that all phases of data management are accomplished in accordance with security best practices within their own walls, but also that vendors and other affiliates are meeting these requirements as well. Contractual agreements must be renewed and assessments conducted to ensure good security controls are implemented appropriately and practiced in a regular fashion.

Traffic Analysis

There are a number of proven commercial technologies that will provide organizational IT and security divisions with the tools they need to assess traffic patterns, monitor access, report breaches of organizational policy, and detect and prevent instances of data leakage. Leaders in the data leakage prevention[9] market include Vericept and Vontu. Implementation of these solutions offers organizations the ability to drastically impact their potential to detect and prevent data leakage. However, if the purchase of commercial products exceeds the reaches of an organization's budget, there are a number of freely available network tools that will allow for the detection of data leakage, albeit to a lesser degree of expediency and without all of the bells and whistles.

Certainly, there are several downsides to using freeware or open source products. Compared to commercially available tools, freely available tools may not receive the same support, from both a development and troubleshooting perspective. Often, open source tools lack the graphical user interface (GUI) that many IT professionals expect and have come to rely on for their convenience. Commercial tools allow IT and security professionals to spend less time at the command line and more time resolving the issues at hand.

However, for an organization with a limited budget, these freely available tools are a good alternative solution. Tools, such as sniffers,[10] have the ability to detect many indicators of data leakage, such as those network activities previously addressed in this document (e.g., instant messaging, blogging). In addition, these freely available tools can detect other malicious behaviors, such as outbound unencrypted PII (e.g., Social Security numbers), malformed packet attacks, password attacks or denial of service (DOS) activities. They also are capable of detecting uninitiated (by the user) outbound connections to nontrusted parties, often indicative of spyware or root kits.[11]

The determination of whether an open source solution is appropriate for an organization is left entirely up to the individual entity, its personnel and its defined policies. The benefits and drawbacks of commercially available and open source tools are commonly debated; however, for an organization with a limited IT or security budget, the choice to implement open source technology may be made easily.

---

[9] Forrester evaluated and reported in *The Forrester Wave™: Information Leak Prevention, Q4 2006* the leading information leak prevention (ILP) vendors and concluded that Vericept and Vontu had established early information leak prevention leadership because of their "rich analysis capabilities."

[10] Sniffers are defined in *Hacking Exposed,* Fifth Edition, as having the ability to capture, interpret and store for later analysis packets traversing a network.

[11] Root kits are defined in *Malware: Fighting Malicious Code* by Ed Skoudis as "… Trojan horse backdoor tools that modify existing operating system software so that an attacker can keep access to and hide on a machine."

Use of "Honey" Data

An inexpensive and emerging method of data leakage identification that organizations of varying sizes can implement is the population of organizational databases or information repositories with "honey" data. Honey data exists as nonspecific, nondescript data resident among legitimate organizational information. An example of honey data might be the addition of an e-mail address that is not associated with an organizational employee or customer among a database of legitimate e-mail addresses. As this address would not be provisioned for use or distribution, the receipt of e-mail or the publication of the honey data would be indicative of data loss.

But use of honey data does not have to be limited to e-mail addresses. Development team administrators may elect to populate their databases or file directories with threads of source code that serve no purpose other than to identify leakage instances. Such code might be made available in user-accessible directories or within file shares requiring privileged access. In this case, the use of such code would not only indicate the leakage and inappropriate use of sensitive information, but also, perhaps, the unauthorized escalation of privileges or shortcomings of an organization's identity management practices.

As one might suspect, there are several means by which an administrator or manager might investigate the leakage of honey data. One method would be to employ continuous or periodic monitoring of web resources. This might involve the most simplistic of search engine hacking or the use of automated scripts to crawl web resources. Whichever research method is employed, it is important that the individual(s) responsible for research activities remember to search not only the World Wide Web, but also cached publications and covert or less commonly leveraged channels of communication, such as IRC. Of course, this method also can be employed to detect the use or publication of legitimate data.

The second method of investigation would be to either monitor or configure alerting functionality surrounding the use of honey data. Using the example of an e-mail address mentioned earlier, an administrator would be responsible for the periodic access of the honey account and would ensure that the inbox is absent of any third-party materials. If the account has received e-mail from a headhunter or competitor, this may be evidence that the organizational e-mail directory has been compromised. To continue monitoring efforts and increase the likelihood of honey data detection, more developed security organizations also may elect to configure their intrusion detection/prevention systems to identify specific signatures associated with honey data. Facilitating early warning may be best accomplished either by using the Host-Based Intrusion Detection System (HIDS) resident on the system storing target honey data or positioning a Network-Based Intrusion Detection System (NIDS) sensor within close proximity of that same system.

While source code and e-mail directories are important to an organization, if that organization is responsible for the maintenance and storage of PII, the security of such data should be the administration's and executive management's primary concern. As such, the honey data organizations may wish to employ might be credit card numbers or other account numbers not associated with a consumer.

Following the detection of exposed honey data, responsibility for investigating the leakage might fall to the organization's forensic or incident response team. Given the nature of the honey data's usage, the organization also may elect to outsource the investigation of data leakage to a third party or even law enforcement.

As a caveat, senior management should have a plan in place for the management of honey data, as well as a response plan or approach to dealing with leakage of that data, as its release may cause confusion throughout an organization and among outsiders who may obtain such data.

Organizational Impact

The implementation of the affordable solutions addressed previously in this document is a good start to limiting the risks of data leakage and making organizational strides toward privacy; however, by no means will organizational data be kept safe by their implementation alone. An organization will have to make

investments in order to preserve the privacy and overall security of its data. Investments should include but certainly not be limited to:

- Acquisition of experienced security professionals
- Security training for existing security staff
- Basic security and awareness training for all personnel
- Access controls
- Identity access management
- Purchase and implementation of proven security technologies:
  - Data leakage
  - Policy enforcement
  - Intrusion detection/prevention system
  - Antivirus
  - Cryptographic solutions
- Physical security enhancements

As several of these potentially "costly" measures might not be fully adoptable considering an organization's IT or security budget, one alternative allowing for more gradual implementation is the use of a trusted third party to assess periodically the "vulnerability landscape."[12] A third-party assessment is generally not the long-term solution for an organization on an already stretched budget; however, organizational experience, dedication to information security, and the ability to be independent and subjective often are factors contributing to a more complete, thorough and unbiased assessment of an organization's current security posture.

Protiviti has been performing data leakage assessments for its clients since its inception. Although the following descriptions and diagrams describe Protiviti's approach and methodology at a high level, organizations may leverage such an approach when conducting their own assessments.

Prioritization and Measurement

While effective methods of deterrence, detection and defense may be implemented, organizations should have a structure in place to document and track data leakage deficiencies, as well as their progress toward remediation. Additionally, data leakage assessments might encapsulate a variety of vulnerability exposure techniques. Given the need for such a structure and the nature of the assessment, organizations may elect to take an approach that allows for the measurement and prioritization of vulnerabilities based on their technical focus, as well as the cost/resource utilization associated with remediation of each one. In Figure 1-3, resources and cost are measured as one variable, represented as "Effort," and compared against technicality ("Coverage") to rank initiatives geared toward successful cryptographic solution implementation.

Rarely will an organization's measurement illustrate such a clear and concise representation of cost versus coverage. As a result, senior management may find it difficult

Figure 1-3

[12] The term coined by Bruce Schneier in *Secrets and Lies: Digital Security in a Networked World* to limn the imaginary complicated world of attacks and countermeasures.

to conceptualize the benefits and value of certain security initiatives when compared to others. However, successful communication to senior management will be impacted greatly, provided an organization has (1) an established methodology and approach to vulnerability assessment, (2) a centralized repository for the storage and maintenance of leakage vulnerability data, (3) established models for the communication of data leakage information, and (4) the basis for associating cost of exploitation versus vulnerability acceptance.

Following the decision to implement initiatives geared toward the remediation of data leakage vulnerabilities, the success of such initiatives will be significantly enhanced by the continued support of senior management. For this reason, it is vital that organizations provide continuous and appropriate metrics to management so they might recognize the milestones achieved by security personnel or allocate resources to support the tactical completion of such initiatives.

As data leakage vulnerabilities vary with respect to their technicality and nature, it is important that a metric reporting structure be put in place to guide and govern data leakage initiatives while maximizing and efficiently leveraging the time of senior management. To accomplish this, and specifically address the concerns of interested parties, data leakage metrics can be condensed and consolidated as they escalate through the echelons of senior management. In Figure 1-4, the progress reporting of recommended data leakage initiatives is associated with a hierarchical structure of metric reporting.

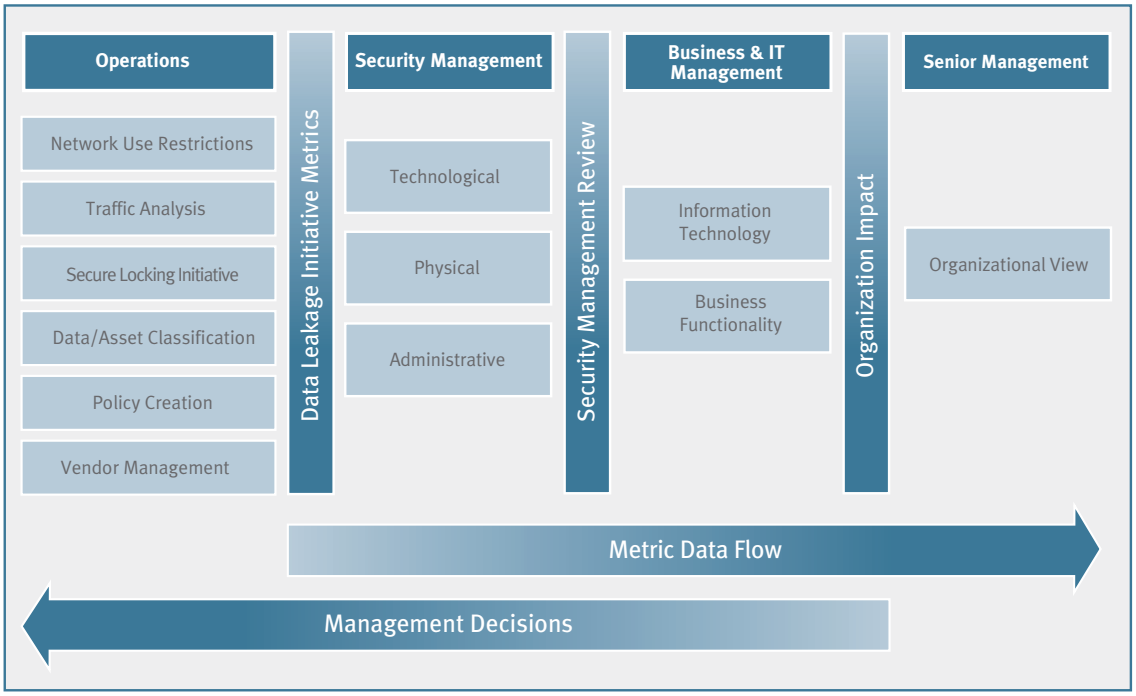

Figure 1-4

Considerations

"Affordable" is defined by Merriam–Webster's Online Dictionary as follows: "to manage to bear without serious detriment." An important aspect of that definition is that it lacks direct association or ties to finance or to specific monetary amounts. So, when discussing whether data leakage prevention is "affordable" or not, organizations should consider these questions:

Can we manage to bear data leakage risks without serious detriment to our customers?

Can we manage to bear data leakage loss without serious detriment to our reputation?

Can we manage to bear data leakage risks without serious detriment to our employees?

Can we manage to bear data leakage risks without serious detriment to our bottom line?

The ability to afford any of the solutions discussed previously in this document obviously will vary by organization, and unfortunately, even the resources associated with the most inexpensive risk mitigation activities may be viewed by some senior executives as too costly.

Too often, security initiatives such as these are viewed as "sprints." Senior management believes the solution will be effective only if it is implemented fully and quickly through maximum resource dedication. But instead, security initiatives and the implementation of secure practices, processes and technology should be viewed as part of a process better compared to a marathon. Gradual strides are taken to accomplish the same objectives, ensure quality, and provide for milestones of accomplishment and a continuous pattern of improvement.

Knowing some of the affordable methods to mitigate the risk of data leakage, developing an approach to measurement, and prioritizing, reporting and combining that knowledge with an understanding that security is a process will greatly improve an organization's ability to rationalize funding, better utilize and allocate its security budget, and dramatically improve its security posture.

Protiviti's Approach to a Data Leakage Assessment

The benefits of a data leakage assessment are great considering they exist as a culmination of a variety of beneficial security assessment services. The following diagram illustrates the primary aspects or characteristics of a core data leakage assessment (Figure 1-5).

The factors illustrated in Figure 1-5 enable Protiviti to gain a thorough and complete understanding of an organization's security posture. Policy review allows for the identification and gap analysis of administrative controls put in place to inform and deter employees, contractors or other parties from acting in a manner that would prove detrimental to the organization or its customers.

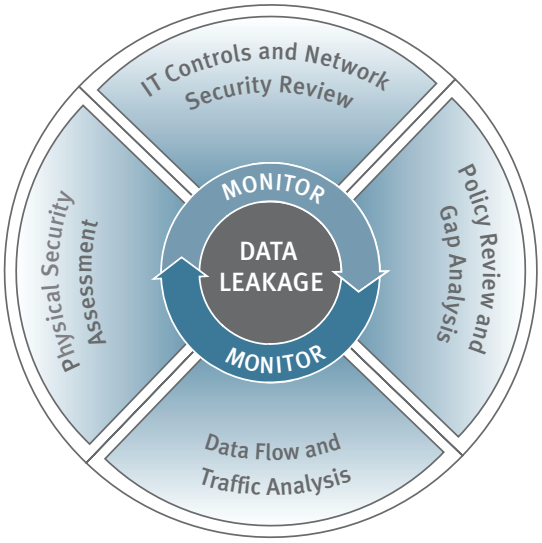

Figure 1-5

As administrative controls are assessed in review of policy, technical controls are assessed by way of an IT control and network security review. This particular aspect of a data leakage assessment allows for the identification of more traditional technical vulnerabilities (applicable to data leakage) such as:

- Poor password parameters
- Weak authentication protocols
- Insecure (plain text) data transmission
- Insecure data storage
- Failures in "least privilege access" and permissions
- Inappropriate site visitation
- Use of P2P software
- Use of chat protocols (IM, IRC)
- Rogue nodes

Offered in conjunction with a technical assessment, Protiviti professionals are experienced in assessing physical vulnerabilities. Often, those areas subject to scrutiny in a physical assessment include secure physical data storage, "turnstile" implementation, surveillance implementation, lock strength, key card implementation, access log management and organizational susceptibility to social engineering attacks.

Finally, Protiviti can perform a data flow and traffic analysis. While the description of the service can be interpreted as an examination of network data and traffic, it is actually a combined examination of electronically transmitted data and physically distributed data to parties within and outside the organization. This assessment is driven primarily through close observation and interviews in which experienced professionals trail data from source to destination while analyzing potential risks and inherent vulnerabilities associated with data distribution. Often, such an assessment leads to other organizational third parties who may require their own assessment to ensure organizational data is being handled appropriately and in accordance with organizational policy and contractual agreements.

Following the assessment phase, Protiviti will provide an overall gap analysis of an organization's security posture based on several security standards, including those applicable to the organization's industry, personnel knowledge of industry best practices, and Protiviti's experience and knowledge of information security. As in a traditional security assessment, recommendations will be made in an effort to minimize risks and close gaps. However, unlike in a traditional assessment, Protiviti can develop a road map for organizational activities in a way that allows for strategic planning and budgeting in cooperation with relevant staff. Additionally, while Protiviti does maintain alliances with proven and reliable technology vendors, recommendations of technologies are made only in the best interest of the organization being provided security services; this often leads to the recommendation of nonaffiliated products or solutions.

While in some instances a data leakage assessment may conclude following the presentation of assessment recommendations, Protiviti offers additional services for successfully implementing data leakage mitigating controls, as well as continuing services for maintenance and operation of data leakage activities.

The structure of a complete data leakage assessment is documented below (Figure 1-6).

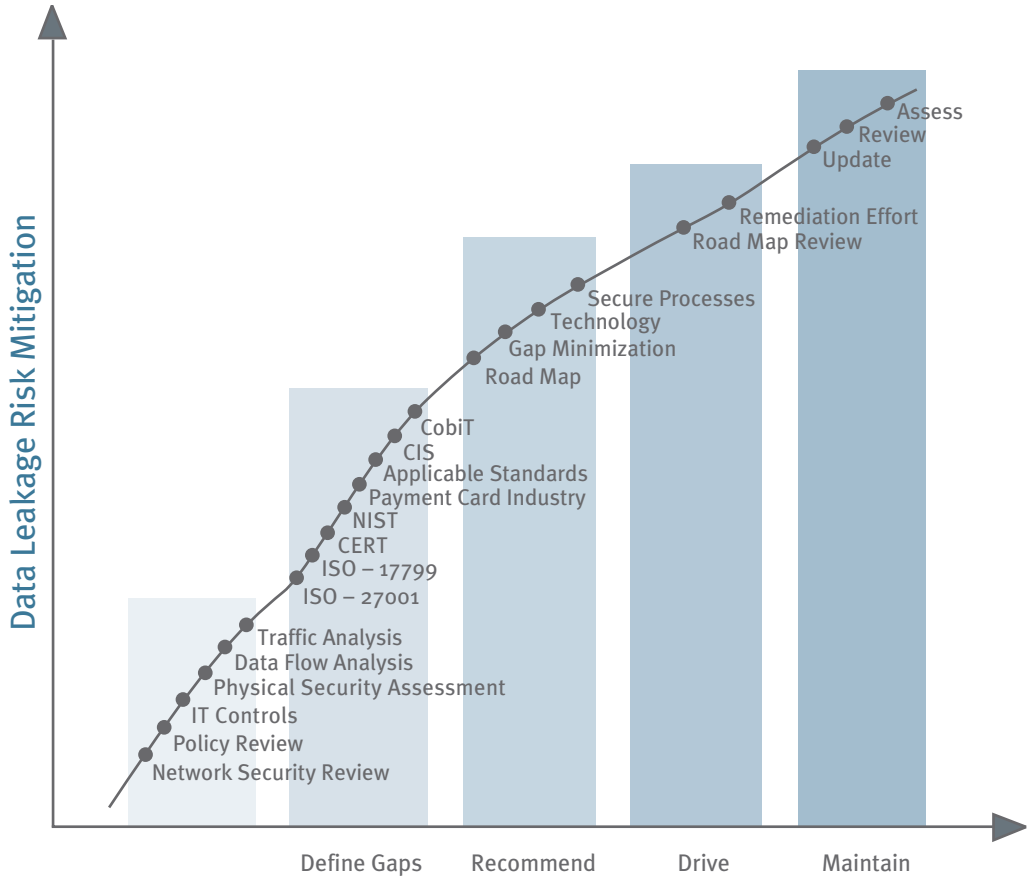

Figure 1-6

References

1. "Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain," 2007, retrieved from http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01.
2. PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard*, Security Audit Procedures Version 1.1, 2006, retrieved from https://www.pcisecuritystandards.org/tech/index.htm.
3. Mitnick, K. D. and Simon, W. L., *The Art of Deception: Controlling the Human Element of Security*, 2002, Indianapolis, Wiley.
4. Cleary, T. and Sun Tzu, *The Art of War: Complete Texts and Commentaries*, 2003, Boston, Shambhala.
5. Albrecht, S., Albrecht, C. C. and Albrecht, C. O., *Fraud Examination*, 2005, Cincinnati, South-Western Pub.
6. *Taking Action to Protect Sensitive Data*, 2006, retrieved from www.itpolicycompliance.com.
7. Dwivedi, H., *Securing Storage: A Practical Guide to SAN and NAS Security*, 2006, Westford, Pearson Educational, Inc.
8. Mattord, H. J. and Whitman, M. E., *Principles of Information Security*, 2003, Boston, Thompson.
9. Penn, J. and Raschke, T., *The Forrester Wave™: Information Leak Prevention, Q4 2006*, 2006, retrieved from www.forrester.com/go?docid=38929.
10. Kurtz, G., McClure, S. and Scambray, J., *Hacking Exposed (5th ed.)*, 2005, New York, McGraw Hill.
11. Skoudis, E., *Malware: Fighting Malicious Code*, 2004, Upper Saddle River, Prentice Hall.
12. Schneier, B., *Secrets and Lies: Digital Security in a Networked World,* 2004, New York, John Wiley & Sons.

About Protiviti

Protiviti (**www.protiviti.com**) is a leading provider of independent risk consulting and internal audit services. We provide consulting and advisory services to help clients identify, assess, measure and manage financial, operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services to assist management and directors with their internal audit functions, including full outsourcing, co-sourcing, technology and tool implementation, and quality assessment and readiness reviews.

Protiviti, which has more than 60 locations in the Americas, Asia-Pacific and Europe, is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Our Security and Privacy Solutions

The business world grows rapidly more connected each day. Opportunities for increased efficiency and productivity are great and varied. But the push for faster and more universal connectivity focuses on functionality, not the resident risk: whether it is granting access to users, blocking entry from would-be hackers, maintaining the privacy of your customers or protecting your intellectual property. You need to know your vulnerabilities. To protect you and your customers, security must be pervasive across the entire computing platform.

Protiviti approaches enterprise security and privacy from a business perspective. We understand your core business processes, your industry, and the technology that supports your current and future business strategies. We then implement sustainable solutions using our expertise and a structured approach that includes proven methodologies and tools. Our approach allows us to:

- Assess vulnerabilities and risk:
  - Focused on the root cause
  - Skilled in identification of both internal and external risks
- Develop policies:
  - Automated policy management processes
  - Aligned with key industry standards and regulatory requirements
- Design architecture
- Deploy solutions
- Create awareness
- Monitor compliance

For more information about the topics covered in this white paper or our security and privacy solutions, please contact:

Rocco F. Grillo, CISSP
Managing Director
212.603.8381
rocco.grillo@protiviti.com

Joseph A. Rivela, CISSP
Senior Security Consultant
212.399.8657
joseph.rivela@protiviti.com

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti.com 1.888.556.7420