GTAG

GLOBAL TECHNOLOGY AUDIT GUIDE

Managing and Auditing IT Vulnerabilities

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG) 6: Managing and Auditing IT Vulnerabilities

Authors:

Sasha Romanosky, Heinz School of Public Policy and Management, Carnegie Mellon University

Gene Kim, Tripwire Inc. and IT Process Institute

Bridget Kravchenko, General Motors Corp.

October 2006

GTAG — Table of Contents

The authors would like to thank Julia Allen, Lily Bi, Ron Gula, George Spafford and the many other reviewers who provided valuable feedback. Special thanks to Peter Mell of the U.S. National Institute of Standards and Technology (NIST) for his invaluable contributions.

Among their responsibilities, information technology (IT) management and IT security are responsible for ensuring that technology risks are managed appropriately. These risks originate from the deployment and use of IT assets in various ways, such as configuring systems incorrectly or gaining access to restricted software. However, these risks can be identified and remediated by detecting vulnerabilities, assessing their potential impact, and when warranted, deploying corrective measures.

Vulnerability management is the processes and technologies that an organization employs to identify, assess, and remediate IT vulnerabilities — weaknesses or exposures in IT assets or processes that may lead to a business risk[1] or security risk.[2] According to the U.S. National Vulnerability Database[3], approximately 5,000 new vulnerabilities are discovered every year, and 40 percent of those vulnerabilities have a "high severity" (i.e., they could cause major disruptions to organizations).

You may be wondering why you should read a guide on vulnerability management. After all, isn't this something you can completely delegate to your IT audit staff? The answer is "no." Often, the potential impact of an IT-related risk remains ill-defined and misunderstood until a worm, such as SQL Slammer, shuts down business operations. Knowing how to educate and inform executive management on the importance of vulnerability management will help drive support and create a call for action. Executive management must understand that to have an effective vulnerability management program, they must design a process to detect, assess, and mitigate vulnerabilities continually by integrating these tasks into the overall IT process framework. The issues surrounding vulnerability management aren't all technical in nature. In fact, many of the greatest challenges will lie with motivating individuals and driving effective processes.

This guide was developed to help chief audit executives (CAEs) pose the correct questions to their IT security staff when assessing the effectiveness of their vulnerability management processes. The guide recommends specific management practices to help an organization achieve and sustain higher levels of effectiveness and efficiency and illustrates the differences between high- and low-performing vulnerability management efforts.

After reading this guide, you will:

- Have a working knowledge of vulnerability management processes.
- Have the ability to differentiate between high- and low-performing vulnerability management organizations.
- Be familiar with the typical progression of capability — from a technology-based approach to a risk-based approach to an IT process-based approach.
- Provide useful guidance to IT management on best practices for vulnerability management.
- Be able to sell your recommendations more effectively to your chief information officer (CIO), chief information security officer (CISO), chief executive officer (CEO), and chief financial officer (CFO).

[1] Such as failure to maintain integrity of financial reporting or a loss of revenue or productivity.
[2] Such as violations of confidentiality, integrity, or availability of data.
[3] http://nvd.nist.gov

IT vulnerabilities have become an epidemic, exposing networks to attackers, viruses, and worms. In fact, more than 12 vulnerabilities are discovered every day in hardware and software products.[4] Other types of IT vulnerabilities include inadequate password management, inappropriate access to files, weak cryptography, and misconfigured applications. Keeping up with the latest announcements and patches has become a nonstop job for IT managers and security professionals. However, some are more successful than others.

2.1 Identifying Poor Vulnerability Management

The top six indicators of poor vulnerability management processes are:

- A higher than acceptable[5] number of security incidents during a given period of time.
- An inability to identify IT vulnerabilities systematically, resulting in exposures to critical assets.
- An inability to assess risks associated with each vulnerability and to prioritize vulnerability mitigation activities.
- Poor working relationships between IT management and IT security, leading to an inability to control and make changes to computer assets.
- Lack of an asset management system.
- Lack of a configuration management process that is integrated with vulnerability mitigation efforts.

2.2 Improving Vulnerability Management

The six prescriptive steps that can be taken to improve vulnerability management processes are:

- Obtain executive management support for identifying and remediating IT vulnerabilities consistent with the organization's tolerance for risk.
- Acquire a complete inventory of all IT assets and their vulnerabilities.
- Prioritize remediation efforts according to business risks.
- Remediate vulnerabilities by delivering planned work projects to IT management.
- Continually update asset discovery[6], vulnerability testing, and remediation processes.
- Use automated patch management and vulnerability discovery technologies to the greatest extent possible.

2.3 The Internal Auditor's Role

Vulnerability management has become a high priority, because IT controls are considered part of the internal control structure over financial reporting and regulatory compliance requirements in regulations such as the U.S. Sarbanes-Oxley Act of 2002, the U.S. Federal Financial Institution Examination Council (FFIEC)[7], and Canadian and Japanese version SOX acts. Therefore, there is an increasing requirement for IT management to provide mission-critical services to businesses. IT management and IT security are accountable for implementing and demonstrating that sufficient security controls exist and operate effectively to meet internal control and regulatory requirements.

Internal auditors provide guidance and value to the business in many ways. They can assess the effectiveness of preventive, detective, and mitigation measures against past attacks, as deemed appropriate, and future attempts or incidents deemed likely to occur. Internal auditors should confirm that the board of directors has been appropriately informed of threats, incidents, vulnerabilities exploited, and corrective measures.

Internal auditors also provide recommendations to executive management regarding compliance with internal and regulatory requirements and raise their awareness concerning likely vulnerabilities and impacts. In this way, internal auditors assist executive management by identifying possible sources of risk to enterprise, thus helping to avoid security incidents or regulatory violations. In particular, internal auditors identify where IT security has failed to implement effective vulnerability management processes and validate existing vulnerability remediation efforts.

One question auditors might ask is, "What would a vulnerability audit scope look like?" Table 1 provides a brief introduction to the activities auditors may consider in scope. More details of each section are provided in Section 3.

2.4 How Vulnerability Management Drives Changes to the IT Infrastructure

Scanning for and discovering vulnerabilities initiates the risk assessment process, possibly requiring changes to IT assets. With the increasing proliferation of vulnerabilities, the successful execution from discovery to expeditious remediation is important to ensure minimal impact to the business. This means that vulnerability management must be integrated with an organization's change and patch management activities. As will be discussed, prioritizing and executing changes to IT assets is always a challenge, but there are ways to determine if you have an effective vulnerability management process that is fully integrated with your organization's change management practices. Change management processes are discussed fully in *GTAG 2: Change and Patch Management Controls*. [5]

[4] Source: U.S. National Vulnerability Database

[5] An "acceptable" number of incidents can be determined by comparing one's tolerance for loss with the loss from past incidents. Then, one can adjust vulnerability management efforts by balancing the costs of implementing controls and remediating vulnerabilities with the benefits of these activities, possibly as a function of loss avoided.

[6] This will be discussed in Section 3.1.

[7] http://www.ffiec.gov

Identification and Validation	Risk Assessment and Prioritization	Remediation	Maintenance and Improvement
Asset Inventory Ensure an inventory of all IT systems is maintained. Ensure IT systems identified are grouped and prioritized according to their corresponding business risks. Ensure process dependencies exist between configuration management and change management.	**Risk Assessments** Identify the criteria used to assign risk as vulnerabilities are detected. Ensure criteria are used consistently across the organization.	**Monitoring** Identify automated and manual processes for vulnerability announcements. Develop contingency plans in the event an identified vulnerability is not patched timely.	**Configuration Management** Ensure IT assets are maintained in a standardized format to help track logical and physical elements of the IT asset such as model, applications installed, and patches. Ensure change and incident management are integrated with configuration management.
Vulnerability Detection Identify automated tools used to scan and monitor the network and host devices. Ensure IT assets are scanned periodically. Identify resources used for timely vulnerability information (e.g., third parties, software providers, CERT.).	**Vulnerability Priorities** Analyze how significance is quantified based on impact to and criticality of the system. Ensure business impact is included as a measurable priority identifier.	**Incident Management** Procedures for remediation should be consistent across the organization. Impact and urgency assigned to the incident ticket should be aligned with the business risk of the asset. Incident metrics, such as mean time to recover, should be defined and tracked to ensure operation-level agreements (OLAs) are met.	**Operation-level Agreements** Identify that OLAs are in place to ensure vulnerability management timing and process handoffs are measured and accountable.
Validation of Findings Ensure a process is in place to identify false positives and negatives during detection. Ensure vulnerabilities are analyzed as applicable to the native environment.		**Change Management** Analyze whether changes are reactive to identified vulnerabilities. Patches should be planned and tested prior to implementation. Changes that are a result of vulnerabilities should cause minimal disruptions to the business.	**Policies and Requirements** Ensure roles and responsibilities are defined for identification, communication, and remediation. Identify policies and procedures to ensure appropriate strategy and decisions have been defined.
		Patch Testing Determine how centralized patches are deployed to ensure efficiencies and eliminate duplicated efforts for the same vulnerability. Ensure patches are tested and checked for viruses. Ensure patches are tested in a pre-production environment to ensure that no unexpected risks or service-impacting problems will result from the patch [5]. Identify automated and manual patch procedures to ensure deployment efficiency.	

Table 1: Vulnerability management audit scope

This section illustrates only the critical components necessary for achieving an effective vulnerability management program. A more comprehensive discussion can be found in Creating a Patch and Vulnerability Management Program [3].

Figure 1 illustrates the dependencies between the relevant IT security and IT operations functions. For the purpose of this document, we consider the functions of an organization implementing the ITIL framework [8].

The Vulnerability Management Lifecycle begins by identifying IT assets and then scanning or monitoring them for IT weaknesses. The vulnerability data is then validated to confirm that vulnerabilities do exist. They are then prioritized based on the risk to the organization.

Critical vulnerabilities are handled by Incident Management which coordinates remediation efforts with Change Management using emergency change procedures that expedite the implementation into production. Non-critical vulnerabilities are reviewed via the standard Change Management process. Once approved, Release Management then prepares, tests, and facilitates the change. Again, Change Management reviews the change to ensure it met all requirements and finally, the Configuration Management database is updated to reflect these improved (i.e., more secure) modifications.

Note that regardless of whether the remediation work is an emergency or not, all changes are routed through Change Management. They act in a marshalling role to move the change through the IT machinery to a successful completion.

3.1 Identification and Validation

Scoping Systems

To scope systems properly, the auditor should acquire a complete list of all network segments used throughout the organization, such as corporate wired and wireless networks, production networks, backup or administration networks, transit networks, laboratories and testing networks, and remote offices. Each of these networks must be identified and documented.

The networks also should be included in a network architecture diagram that shows network interconnections as well as perimeter security devices, such as routers, firewalls, and intrusion detection systems. This diagram will allow management to understand how vulnerabilities found in one network may impact the security of assets in another network.

Detecting Vulnerabilities

Once a network inventory is obtained, all IT assets connected to each network segment should be scanned or monitored periodically for vulnerabilities. These assets include devices such as business application servers (e.g., database, e-mail, Web, and customer relationship management servers),

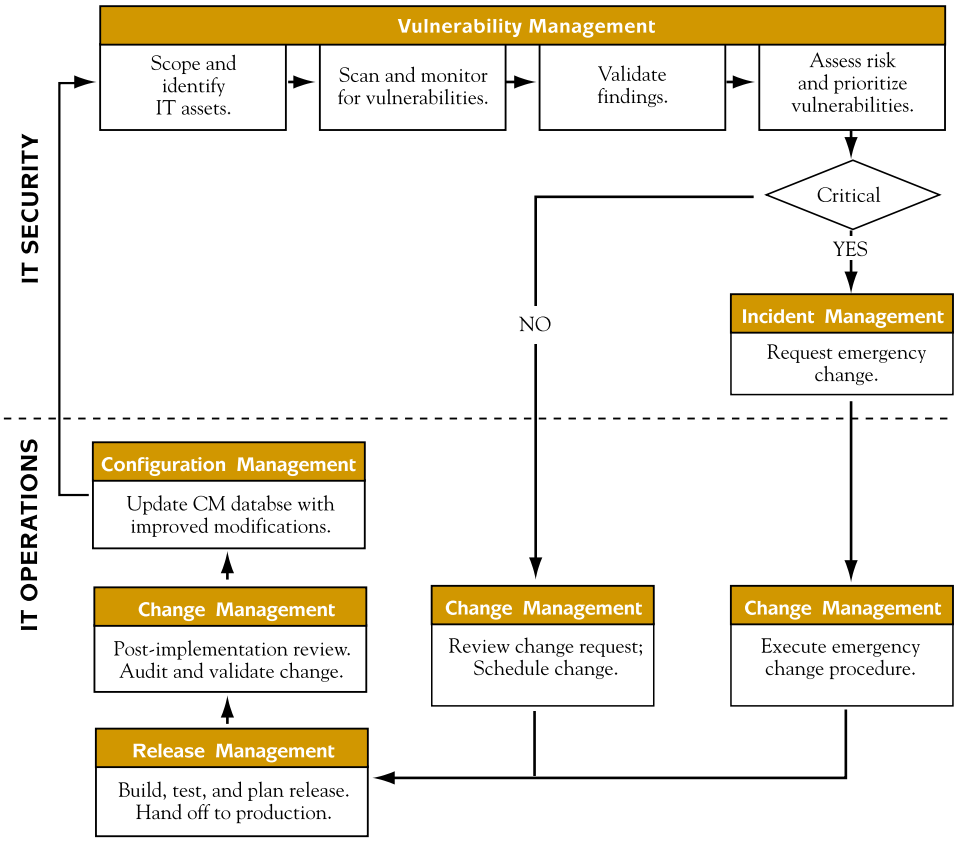

Figure 1: Vulnerability management and IT dependencies

security devices, telecommunication and networking devices, and printers.

Scanning refers to network devices or specialized applications that actively probe other applications and IT assets for weaknesses[8]. These devices should be scheduled to run daily, monthly, or quarterly based on the needs, risks, or capability of the organization[9].

Monitoring refers to software agents installed on IT assets that report host configuration information. It also refers to network devices that continuously listen to network traffic and report, or optionally block, malicious traffic that may exploit a vulnerability. These devices also are useful for identifying rogue or previously unknown IT assets. They are considered a preventive security control because of their ability to block attacks before they cause loss.

Validating Findings

Finally, companies should validate the results from the vulnerability monitoring and scanning process. Although the sophistication and accuracy of vulnerability scanning and monitoring devices are generally good, they always have limitations. Errors can occur in the form of false positives or false negatives. A false positive is a vulnerability that has been reported but does not exist, because the detection mechanism was in error. A false negative occurs when a vulnerability exists, but the detection system failed to identify it.

3.2 Risk Assessment and Prioritization

Assessing Risks

Once vulnerability data have been acquired, the organization must be able to determine the actual risk they pose. While a full risk management project generally is not necessary, a basic risk assessment is necessary.[10] Given the large number of vulnerabilities discovered with each scan, it is likely an organization will be performing a large number of mini-risk assessments. Therefore, organizations must have a well-defined procedure to measure risks that can be applied quickly and accurately.[11] Note that the presence of a vulnerability does not always warrant remediation, and the organization may choose to accept the risk posed by the vulnerability [2], for example, when existing security controls sufficiently reduce the likelihood of a successful attack or when the asset targeted is of little or no value. In these cases, the risk acceptance should be documented and approved to avoid reassessing the same finding later.

Prioritizing Vulnerabilities

The organization should prioritize the remediation of vulnerabilities according to the criticality of the vulnerable asset, the likelihood or frequency that an attack will occur (e.g., Internet-accessible devices are more likely to be attacked than backend devices), and the effort required to implement the fix. Thus, auditors will compare the actual risk posed to the organization[12] with the cost to implement the fix, and prioritize the risk based on its cost-effectiveness. The organization also may want to examine the causes of past security incidents and prioritize accordingly. For example, perhaps past incidents were due to breaches initiated from third-party connections or were caused by malicious software introduced by employees.

3.3 Remediation

Mitigating Critical Vulnerabilities

Often the best way to fix the most critical vulnerabilities is for IT security staff to use the existing incident or trouble ticketing system.[13] This system is probably part of a standard IT operating procedure, which ensures fixes are addressed in a timely manner by the appropriate personnel.

Creating a Vulnerability Mitigation Process

Fixing the most critical vulnerabilities removes obvious dangers. This should be a quick process to execute, because there may be only a couple of vulnerabilities. However, different challenges arise when trying to remediate hundreds or thousands of vulnerabilities at a time. The most efficient way to execute these fixes is to create an IT project that includes a project manager, process deliverables, and deadlines. The project must then have the authority to integrate with the organization's configuration management process and deploy the necessary patches. Implementing a well-designed vulnerability management project with a configuration management process is the best way to achieve repeatable and effective vulnerability management.

By way of analogy, consider the development team of a software application firm. The applications development lifecycle is built to produce quality software. Development teams understand that new features are identified and requested for product development. They take these features; prioritize them based on effort and value to the business; and develop, test, and roll out the product. This is done using a mature and proven process where every stakeholder recognizes their motivations, roles, and responsibilities. For example, a develop-

[8] IT Infrastructure Library (ITIL) is a framework that describes best practices for high-performing IT service organizations.

[9] Ideally, device information should exist within a Configuration Management Database (CMDB), but practically, the database may not always reflect what is actually connected to the network.

[10] Sample of a vulnerability scan report can be found in Section 5.4.

[11] The organization should schedule these scans according to their capability of processing the vulnerability information that is collected. Scheduling scans more frequently than this serves no purpose.

[12] Refer to Section 5.3 in the Appendix for a brief discussion of risk management.

[13] One such quantitative metric is the Common Vulnerability Scoring System (www.first.org/cvss).

ment team may request additional infrastructure from IT staff to support a business application. Naturally, IT may be resistant in terms of cost, delivery date, or configuration, but the goals and expectations are clear.

The success of an effective vulnerability management program lies with IT security staff having a similar relationship with IT management. The program's success also depends on formulating the vulnerability management work and delivering it to IT management as just another stock of planned work[14] to be added to their workload. The details of the project, including delivery date, responsibilities, and vulnerability validation, become part of the larger machinery of day-to-day IT processes and operations.

3.4 Continually Improve

Stopping the Spread

With vulnerabilities being addressed through standard IT business processes, IT Security should notify Change Management of any permanent system or application modification to ensure future builds are released with more secure configurations. This notification is critical and is one of the few proactive steps involved in vulnerability management. To ensure this communication takes place, the security organization should have a direct relationship with Change Management or whichever groups manage desktop, server, and application builds.

Setting Expectations With OLAs

Effective vulnerability remediation often is made more complex and difficult, because the group that is detecting the vulnerabilities (i.e., IT Security) is not generally the group that manages the IT asset (i.e., IT Management).

Often, IT Security may track business-critical vulnerabilities adequately, but may not be able to mobilize IT operations to address them timely. Therefore, an OLA[15] should be established to manage the expectations of both groups — those issuing the requests and those providing the service. The OLA may define separate procedures for each vulnerability category. Table 2 identifies one possible agreement.

Vulnerability Severity	Remediation Time Frame
1	2 business days
2	5 business days
3	15 business days

Table 2: Sample remediation agreement

Achieving Efficiency Through Automation

The efficiency of a vulnerability management group is improved vastly through automation. The more the organization can automate processes, such as scanning for vulnerabilities, creating tickets with operational groups, updating status reports, and reporting, the more it will be able to focus on further improving and scaling its efforts — or, indeed, spending fewer resources on IT security. Whoever is responsible for actually deploying the patches should use automated patching solutions, as it is rarely cost effective to apply them manually.

Using Past Experience to Guide Future Actions

The metrics of Section 5.1 can be used to determine the extent to which vulnerability management is improving. Organizations also can use many of these indicators — such as patch failure or change success rates — to rate the risk of changes. For example, if a specific type of change has been historically problematic, the risk of deploying future patches of that type can be decreased by increasing pre-deployment testing practices.

[14] The concept of planned versus unplanned work is discussed thoroughly in the GTAG 2: *Change and Patch Management Controls* [5].
[15] In the ITIL context, this may be referred to as an operational level agreement.

This section describes the characteristics of high- and low-performing IT vulnerability management organizations. These descriptions, and those in Table 4 in Section 5.2, will help organizations determine their vulnerability management maturity.

4.1 Low Performers

Not surprisingly, a low-performing organization will have inefficient vulnerability detection and management processes. Low-performing organizations don't detect vulnerabilities often enough and don't keep track of their IT assets. When the organization performs a vulnerability detection, the amount of change that has occurred since the last scan is so vast, it expends a huge amount of energy just tracking new hosts, applications, and system owners. In addition, the number of vulnerabilities discovered may be so high that the organization becomes overwhelmed when dealing with them.

When low-performing organizations attempt to remediate vulnerabilities, their effort is generally not effective and only a portion of the vulnerabilities are addressed. This is often because the organization hasn't integrated its vulnerability and configuration management processes or, in many cases, because it doesn't even have such a process. Other problems may arise from inefficiencies in network management or in communication between IT security and IT management, such that IT management ignores IT security's recommendations. In addition, the organization may rely on security devices to protect unpatched computers (e.g., virus proxies, firewalls, and intrusion prevention technologies). Security software cannot replace a solid patch management program, but must complement it to achieve greater security. Finally, the networks of low-performing organizations often are designed to be "open" — that is, anyone can connect and gain access to the entire corporate or production network.

The characteristics of low-performing organizations — or those in the early stages of vulnerability management — are easy to spot and include:

Identification and Validation

- The organization is scanning nonproduction IT assets or a small fraction of production IT assets where business risks may be the greatest.
- The network architecture diagram showing the location of IT assets and perimeter security devices protecting those assets is incomplete or limited.
- The organization attempts to increase the scope of IT asset scanning or monitoring, but is impeded by limited visibility to the network or resistance from asset owners (e.g., "you cannot deploy instrumentation on my mission-critical systems").
- Vulnerability pilot programs fail due to "too much noise," often indicating that the production environment defies control (e.g., IT administrators or users are installing new software and hardware frequently, resulting in a wildly chaotic environment with no accountability or traceability to authorized projects).
- The organization is unable to validate results of the vulnerability scans due to the volume of data, lack of resources, or lack of technical expertise.
- Scanning is performed rarely, and there is no follow-up activity to ensure that vulnerabilities are mitigated.
- The organization has no asset management system.
- The organization has no record of the baseline configuration of its systems — or has outdated records — and, therefore, cannot measure easily the impact of an exploit that impacts a system.
- The organization has a high level of configuration variance, resulting in unpredictable results when a patch is deployed across a group of systems in the environment.

Risk Assessment and Prioritization

- The organization is unable to distinguish between critical and noncritical IT assets and prioritize vulnerability management actions accordingly.
- The organization is overwhelmed by the number of vulnerabilities that need to be fixed. The number of vulnerabilities is growing too quickly for the organization to address them as needed.

Remediation

- The organization has too many unmanaged systems, and doesn't have a widely deployed automated patching solution. Therefore, users are allowed to re-configure their systems as they like.
- The IT department is unable to adequately test patches to ensure a successful deployment within the organization.
- The vulnerability management program generates a work queue that far exceeds the organization's ability to address it. Remember, it is not enough to demonstrate that a risk exists; the organization also must be able to remedy problems without creating business disruptions that are worse than the originating risk.
- The organization either has no configuration management program or the configuration management program is not integrated with the vulnerability management program.
- The organization has a high variance in its IT asset configuration and operation activities due to the absence of standardization or ineffective production controls.
- The organization spends a large amount of time performing unplanned work by servicing IT assets (e.g., patching servers, or break or fix cycles).

Continually Improve

- The organization has few automated processes to help with the vulnerability management effort.

- There are unreasonable or nonexistent OLAs between IT security and IT management or IT management and the business owners of the computing assets.
- The organization is constantly in a reactive mode, battling attempted and successful attacks.
- The organization becomes aware of security incidents only by mistake, chance, or after a loss has occurred.
- The organization has no record of its patch or change success rate.

4.2 High Performers

In contrast, consider the case of high-performing organizations that have effective vulnerability management processes. Such organizations exhibit the following characteristics:

Identification and Validation

- The organization has an effective asset management system that maintains a complete inventory of business owners for all IT assets.
- The organization knows exactly what percentage of critical assets is managed fully.
- The organization performs vulnerability scans on all third parties and business partners, virtual private network clients, and any temporary user who connects to the network.
- The organization is able to verify results accurately that are returned from vulnerability scans and ignore those that are misidentified.
- The organization uses practices consistent with those of high performers, as described in the GTAG 2: *Change and Patch Management Controls* [5].

Risk Assessment and Prioritization

- The organization constantly is assessing the risk to IT assets and implementing appropriate security controls to protect them.
- The organization is able to evaluate the cost of remediation and, therefore, is better able to prioritize remediation efforts.
- The organization uses previous data on patch and change successes as metrics to determine which changes and patches are of a high risk as well as uses extra rigor when dealing with high-risk patches.

Remediation

- The organization standardizes system configurations, significantly reducing the number of unique vulnerabilities — and unique fixes required — throughout the enterprise.
- The organization knows exactly which group to engage to address each vulnerability and provides the appropriate amount of information.
- The organization uses an automated patching solution and effectively tests patches to ensure compatibility before deployment.
- When necessary, the organization creates and executes business projects with asset owners to remediate large numbers of vulnerabilities.
- The organization is able to track the remediation process from initiation to fix and validate the result.
- The organization is able to verify that compromised systems have been returned to their known, good state.

Continually Improve

High-performing organizations have efficient processes that detect vulnerabilities almost in real time and promote secure configurations. They achieve this by:

- Providing security recommendations back to configuration management to build a next generation of more secure systems.
- Increasing scanning frequency and coverage.
- Installing host agents that monitor all applications and assist with patch and antivirus updates.
- Requiring hosts to be analyzed for vulnerabilities before they can be added or authenticated to the network.
- Building systems using secure configuration guidance to minimize the number of vulnerabilities that may exist.
- Deploying standard IT asset configurations to simplify patch deployment.
- Using previous patch and change successes as metrics to rate the risk of patches and determine whether or not the organization is improving its ability to mitigate patch implementation risks.

Because the vulnerability management sampling is so frequent, changes that may indicate larger trends, such as incorrect network management procedures, new classes of vulnerabilities, or groups of misconfigured systems, can be detected quickly.

The networks of high performers are appropriately segmented throughout the organization, with the realistic expectation that there will always be vulnerabilities in the services and clients running on the network. High performers, therefore, enforce a variety of design requirements such that if a compromise occurs, it will be detected at and quarantined to the local network.

High-performing organizations exhibit effective control of their networks when:

- They can identify every IT asset deployed on the network.
- They have a network architecture diagram that shows the location of IT assets and perimeter security devices protecting those assets.
- Employees are not allowed to reconfigure their IT systems arbitrarily and install software.
- Vulnerability scans are scheduled on a regular basis as necessary (e.g., in real time, daily, monthly, or quarterly).

- They quickly and effectively engage the necessary IT groups to fix any vulnerability, and those groups have the authority to deploy patches timely.
- They automate processes for gathering vulnerability information, communicating remediation steps with owners, deploying remediations, and updating remediation status.

High-performing IT organizations may not be the quickest to deploy patches in response to vulnerabilities, but they are better able to accept and accommodate planned work.[16] They treat requests from IT security in the same way as they treat any new business need and are better able to fulfill the request. These organizations understand that untested patches can impact operations negatively and may create higher risks than a known vulnerability.

High-performing IT organizations also have established formal OLAs between IT management and the business owners that govern how quickly prioritized vulnerabilities must be fixed. They have operational agreements on how and when operational changes can be made to remedy vulnerabilities.

Research has shown that high performers will have fewer incidents relative to organizations of equivalent size.[17] Their preventive controls detect and avert many potentially damaging events. When an event does occur, detection controls make them immediately aware. Their corrective and recovery controls respond immediately to an incident, preventing or limiting any significant damage. High-performing organizations will not feel overwhelmed by the constant flood of new vulnerabilities being discovered, but will, instead, have a repeatable, consistent, and verifiable process to manage and mitigate them.

[16] "High performers tend to apply patches less frequently than low performers" [5]

[17] *IT Controls Performance Study — Identification of Foundational Controls That Have the Greatest Impact on IT Operations, Security, and Audit Performance Measures*, IT Process Institute, 2006.

5.1 Metrics

This section contains example metrics that can be used to measure vulnerability management practices within an organization. Different types and sizes of organizations are likely to have different metric results. Thus, the best way to use these metrics is to trend them over time to demonstrate improvement within the organization.

When using metrics to compare the performance of multiple units within an organization, the metrics that do not deal with percentages or averages should be converted into ratios so that metric results are calculated based on the number of systems in the organization (e.g., number of vulnerabilities per computer). Example metrics are listed in Table 2. Additional metrics are available in the NIST's *Creating a Patch and Vulnerability Management Program* publication [3] and the American Institute of Certified Public Accountant's (AICPA) *Report of the Best Practices and Metrics Teams* [7].

Metric	Description
Percent of total systems monitored or scanned.	This measures the completeness of an organization's vulnerability management solution, whether it has awareness of all or some of its systems, and whether it is monitoring them.
Number of unique vulnerabilities.	This measures the amount of variance and risk [1] that exists among systems.
Percent of total systems that are subject to a configuration management process.	This measures the degree to which an organization has control over devices that are placed on its network. For instance, is the organization aware of every new device? Is each device configured with appropriate patch management and security controls?
Percent of all detected vulnerabilities that have been validated.	This metric measures the percentage of all vulnerabilities that have been validated or prioritized. This metric serves to highlight the difference between organizations that simply gather data and those that act on data.
Mean time to remediate a vulnerability.	This measures the efficiency of an organization in remediating vulnerabilities.
Percentage of actionable vulnerabilities fixed within a predetermined time period.	This metric measures the organization's ability to remediate the vulnerabilities it deems worthy of fixing. "Actionable" refers to the difference between all vulnerabilities and those that need to be fixed.
Percentage of OLAs where performance targets have been achieved.	This metric measures the effectiveness of the OLAs the organization has set for itself and for other groups.
Percentage of the IT Security organization's time spent on unplanned work.	This is a measure of how effective the organization is at implementing quality changes to IT assets, and how little time it spends reacting to failed changes or security incidents.
Number of security incidents.	This metric measures the number of compromises to the confidentiality, integrity, or availability of an organization's IT assets.
Impact of security incidents.	This metric measures, to the best extent possible, total dollar losses due to security incidents. This includes time and costs involved in investigating and correcting the incident and the impact to the business.

Table 2: Vulnerability management metrics

5.2 Top 10 Questions CAEs Should Ask About Vulnerability Management

Table 3 provides 10 questions a CAE should ask to determine the maturity of the organization's vulnerability management practice. These responses are meant to illustrate and compare answers one might hear from organizations of a similar size.

Question	Low Performer	Manager in Denial	High Performer
1) What percent of total systems are monitored or scanned?	We're not sure. We've started scanning, but we're discovering new networks all the time. Or: Zero. We are barred from scanning. Or: Probably about 2 percent. We're still testing the vulnerability scanners.	Definitely 100 percent. We asked many groups what networks they use, and we're scanning all of them. Or: We are only scanning 35 percent of our enterprise. After all, these are critical networks and the only thing we need to scan.	We believe 100 percent. We use a combination of human interviews and technical processes to discover new hosts and audit all known hosts for vulnerabilities. We use host agents, as well as passive and active vulnerability scanning to discover anything we might have missed. Or: 100 percent and we can prove it. We are plugged into change management and can determine efficiently if we are scanning the entire network or not.
2) How many unique vulnerabilities exist in your enterprise?	Probably a lot, but we haven't looked. Or: We ran a vulnerability scan and didn't find any vulnerabilities. Or: Wow, there are a lot of them. What do we do now?	Last month, we discovered more than 400, but it's difficult to tell for sure because the network keeps changing. Or: Because we were only scanning a few networks, we only found 15 unique vulnerabilities.	We have fewer than 50 unique vulnerabilities, but our network is designed with the expectation that each service will have vulnerabilities. However, we compensate for this with other mitigating factors, such as firewalls, network systems, and host intrusion prevention systems, and by running our applications with least privilege. Or: There are only 15 unique vulnerabilities across our production systems, but there are 45 in our corporate networks. We know exactly what causes the variance, and we are committed to cutting this number in half by next quarter.
3) What percent of systems are managed?[18]	Only the production machines are managed. We let people do what they want in the corporate network.	All of them ... we're pretty sure. At least all of the important ones.	We currently manage 100 percent of all critical and production devices and 80 percent of all other devices on the network. We will complete a project by the end of the quarter to have the remaining 20 percent of machines either managed by us or pulled from the network. Or: 100 percent of IP devices are managed. Nothing gets connected without authorization, and that requires IT to fully support the machine.

Table 3: Top 10 auditor questions

Continued on page 12

[18] The term, "managed" refers to having a dedicated custodian who is responsible for maintaining the availability of the hardware and software of the IT asset.

Question	Low Performer	Manager in Denial	High Performer
4) What percent of vulnerabilities have you validated?	There are so many that we can only check about 10 percent right now.	We employ a full-time staff that validates every vulnerability.	About 85 percent. We have prioritized about 40 percent of the vulnerabilities based on critical severity to our three most popular applications and two most common platforms. We have validated the remaining 45 percent.
5) What is the mean time to remediate a vulnerability?	Sorry, we don't track that. Or: It takes about two weeks to fix the most critical stuff in production, and close to a month to get anything else done.	Everything is getting fixed quickly. We know this because we haven't heard of any security incidents at all.	Our most critical vulnerabilities are being fixed within the day, which matches our OLA.
6) What percentage of actionable vulnerabilities was remediated in the past quarter?	We don't track that; we just do the scanning. We send our scan results to the business owners, and it's up to them to determine risk. Or: We're getting all kinds of results back from the scanners, but we're still trying to validate the results.	It always costs too much to remediate vulnerabilities, so we rely on firewalls, and intrusion detection and prevention systems. Or: We require all vulnerabilities to be patched.	We have prioritized vulnerabilities into five categories: 100 percent of our top two category vulnerabilities were fixed, and we have a commitment from IT and the asset owners to fix 100 percent of the vulnerabilities in the next two categories by next quarter.
7) What percent of your OLAs are met?	We haven't established any formal OLAs at this time.	All of the groups are committed to addressing vulnerabilities right away. This is an effective process that has worked for us for many years, and I don't think we need to change it.	We are always meeting the OLAs related to the most critical vulnerabilities. For those that are less severe, we do very well, but the reality is that business processes sometimes prevent us from meeting all of them.
8) What percent of IT Security work is unplanned?	It seems like all of it. We are constantly reacting to outages and repairing systems that failed a patch or update.	Oh, not that much at all. We have a few fires here and there, but overall we're always on top of things.	Only a small percentage of our IT Security work is unplanned. With our well-tested patch and change management procedures, as well as our layered security controls, we are rarely reacting to outages.
9) How many security incidents have you experienced during the past quarter?	Ninety-five; we're not sure where they're coming from or how to stop them. Please help.	We only had 35 incidents in the past quarter. Luckily, this was down from last year, so I know we're getting better at this.	We only had three significant security incidents. We were able to detect and quarantine them quickly, and we have established controls to help prevent similar events in the future.
10) What was the average cost of your last five security incidents?	We don't really know; we haven't evaluated them.	It's not that much. After all, we're still a profitable company.	We have performed a root-cause analysis on five incidents from the past year and evaluated their cost. Three impacted the business for one hour each and cost us $X in FTE to investigate, repair, and recover.

Table 3: Top 10 auditor questions

5.3 A Word on Vulnerability and Risk Management

Risk management has been defined as "the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level," and typically involves the following steps [3, 4, and 6]:

- **Asset evaluation:** Identifying the overall value an organization places on an asset.
- **Threat assessment:** Identifying the likelihood of harmful events that could affect an asset.
- **Vulnerability assessment:** Identifying all the weaknesses of an asset and their severity.
- **Risk determination:** Evaluating and prioritizing the risks posed to an asset.
- **Risk decision:** Deciding whether to accept, transfer, or mitigate the risk posed to an asset.

The reader will notice that many of the risk management tasks match those of vulnerability management. The authors recognize that others will have differing perspectives and definitions for the terminology used in this publication and that these differences are healthy and useful. Within the context of this document, we consider vulnerability management to be a tactical and short-term effort that may take days or weeks, whereas risk management is generally a more complex and strategic process that may take many months. Ultimately, of course, the goals are similar in that both processes reduce the possibility of harmful events and improve the overall security posture of the organization.

5.4 Vulnerability Resources for the Internal Auditor

The following is a list of resources for internal auditors to help them understand the risk and likelihood of impact that vulnerabilities may bring to the organization.

Common Vulnerability Scoring System (CVSS)[19]: CVSS is an open framework for scoring computer vulnerabilities. It provides users with a method for standardizing vulnerability severity across disparate vendors and helps them prioritize the vulnerabilities according to the risk they pose to their organization. More information can be found at www.first.org/cvss.

ISO/IEC 17799: This standard is a collection of industry best practices to help ensure an organization employs and manages proper security controls. Further information can be found at www.iso.org.

The Laws of Vulnerabilities [9]: This paper describes The Laws of Vulnerabilities, which are six axioms about the behavior of vulnerabilities gleaned from a continuous long-term research project.

National Vulnerability Database (NVD): NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. government vulnerability resources and provides references to industry resources. It is based on and synchronized with the Common Vulnerability and Exposure (CVE)[20] vulnerability naming standard and provides a severity score using CVSS. More information can be found at http://nvd.nist.gov.

SANS Top 20: The "Twenty Most Critical Internet Security Vulnerabilities" is a living document and includes step-by-step instructions and pointers to additional information useful for correcting these security vulnerabilities. This list includes sections for Windows, Cross-Platform, UNIX, and networking vulnerabilities and can be found at www.sans.org/top20/.

Vulnerability Scanners: Examples of commercial and open-source network and application vulnerability scanners are shown below in Table 4.

Network Scanners	Application (Web) Scanners
nCircle (www.ncircle.com)	AppScan (www.watchfire.com)
Nessus (www.nessus.org)*	Nikto (www.cirt.net/code/nikto.shtml)*
Tenable (www.tenablesecurity.com)	Spi Dynamics (www.spidynamics.com)
Qualys (www.qualys.com)	

Table 4: Vulnerability scanners

* Open-source tools

[19] The CVE Identification is an industry-standard identification name given by the Mitre organization (http://cve.mitre.org/). It is very common for vulnerability reports to cross reference the vulnerabilities with the CVE id because different security organizations may describe a vulnerability differently, but they may all refer to the same CVE ID.

[20] CVSS (Common Vulnerability Scoring System) attempts to address these disparate scoring systems by creating a common scheme that all vendors can use to score computer vulnerabilities. CVSS also attempts to prioritize vulnerabilities based on the risk they pose to any given organization. See www.first.org/cvss for more information.

Sample of Vulnerability Scan Report

Figure 2 shows a summary report from a vulnerability scan[21]. This view displays the particular vulnerability that was discovered, the CVE for that vulnerability, and the number of hosts that are affected. Because these vulnerabilities refer to Microsoft products, the official Microsoft vulnerability ID also is listed. Finally, a severity level for each vulnerability is provided. Note that each security vendor will have their own scale for scoring vulnerabilities[23]. Nevertheless, this score communicates an approximate level of severity for the auditor.

Vulnerability	CVE	Hosts	Score
MS01-023: Microsoft IIS printer ISAPI Available	CVE-2001-0241	1	31548
MS01-026: Microsoft IIS CGI Filename Decode Error	CVE-2001-0333	1	31433
MS01-033: Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow	CVE-2001-0500	1	31151
MS02-056: Microsoft SQL Server User Authentication Remote Buffer Overflow Vulnerability	CVE-2002-1123	1	26939
MS03-007: Microsoft Windows ntdll.dll Buffer Overflow Vulnerability - WebDAV	CVE-2003-0109	1	25302
MS03-026: Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability	CVE-2003-0352	5	24031
MS04-011: Microsoft Windows LSASS Buffer Overrun Vulnerability	CVE-2003-0533	5	20892
MS04-011: Microsoft Windows Private Communications Transport Protocol Buffer Overrun	CVE-2003-0719	5	20892
Apple QuickTime Sample-to-Chunk Integer Overflow Vulnerability	CVE-2004-0431	1	20680
MS04-029: Microsoft RPC Runtime Library Remote Denial Of Service And Information	CVE-2004-0569	1	18497
MS05-011: Microsoft Windows Server Message Block Vulnerability	CVE-2005-0045	7	16746
MS05-019: Microsoft Windows IP Validation Vulnerability	CVE-2005-0048	7	15741

Figure 2: Vulnerability scan report

[21] This sample scan was provided by nCircle.

5.5 Glossary

Business owners: Those responsible for an asset's business function.

Change Management: The goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently, to improve the day-to-day operations of the organization.

Configuration Management: The process responsible for maintaining information about Configuration Items (CIs) required in information systems, including their relationships. The primary objective of Configuration Management is to provide accurate data to all information systems and IT operation processes when and where it is needed.

Configuration Item: Generally, any data regarding, or request for change concerning, a software or hardware asset.

High-performing organization: These organizations know precisely which devices exist, who owns them, and how they are managed. They have automated and effective processes for identifying new machines and their vulnerabilities, as well as formal processes for remediation of any business-impacting vulnerability. All of their assets are appropriately classified and protected.

Incident Management: The process responsible for managing the lifecycle of all security incidents. The primary objective of incident management is to return the IT services to customers as quickly as possible.

IT asset: Any software application or hardware device that is used within the organization to support the organization's business services.

ITIL (IT Infrastructure Library): ITIL is a framework that describes best practices for high-performing IT service organizations and an increasingly globally accepted reference model for IT management.

IT security (security management, information security management): Generally, the group who performs the vulnerability scans and provides recommendations to IT about what to remediate and how to do it.

Low-performing organization: These organizations are just beginning their vulnerability management process. They have little idea of what systems exist, who owns them, and how they are managed. They have few processes for identifying and remediating vulnerabilities. They have not yet begun to track their effectiveness.

Managed system: A fully managed system is one for which the asset owner follows a strict process for change and patch management. The owner knows exactly how the device is configured, who is applying what changes, and when changes are made.

Release Management: Release Management is the process responsible for planning, scheduling, and controlling the movement of releases to the test and production environments. The primary objective of Release Management is to ensure that the integrity of the production environment is protected and that the correct components are released. Release Management works closely with Configuration Management and Change Management.

Remediate (a vulnerability): To patch, block, or otherwise neutralize a vulnerability.

Security incident: Any event, malicious or accidental, that exploits a vulnerability, causing a business loss of revenue, productivity, or life.

Unique vulnerabilities: These are simply the number of different vulnerabilities reported by a vulnerability scan. They are representative of the variance — in system configuration and platform diversity — across a collection of IT assets.

Vulnerability: Any weakness or exposure of an IT asset that could lead to a compromise of the asset's confidentiality, integrity, or availability.

Vulnerability management: All of the processes and technologies an organization employs to identify, track, and remediate IT vulnerabilities.

[1] Kevin Behr, Gene Kim, George Spafford, *The Visible Ops Handbook: Starting ITIL In 4 Practical Steps*, IT Process Institute, 2004.

[2] Jennifer Bayuk, Productive Intrusion Detection, *Computer Security Journal*, Volume XVIII, 3-4, 2002, pp. 23-33.

[3] Peter Mell, Tiffany Bergeron, David Henning, *Creating a Patch and Vulnerability Management Program*, Special Publication 800-40 v2.0, NIST, 2005.

[4] Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad (editors), *Security Patterns: Integrating Security and Systems Engineering*, Wiley & Sons, 2006.

[5] Jay R. Taylor, Julia Allen, Glenn Hyatt, Gene Kim, *Change and Patch Management Controls: Critical for Organizational Success*, The IIA, 2005.

[6] Gary Stoneburner, Alice Goguen, and Alexis Feringa, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, NIST 2002.

[7] Corporate Information Security Working Group, *Report of the Best Practices and Metrics Teams*, the American Institute of Certified Public Accountants, http://ftp.aicpa.org/CSC/infotech/Security/CISWG2_Final_Report.pdf, 2004.

[8] Office of Government Commerce, IT Infrastructure Library, www.itil.co.uk.

[9] Gerhard Eschelbeck,*The Laws of Vulnerabilities: Which security vulnerabilities really matter?*, Information Security Technical Report, Volume 10, Issue 4, pages 213-219, http://dx.doi.org/10.1016/j.istr.2005.09.005, 2005.

Sasha Romanosky, CISSP, holds a Bachelor of Science in electrical engineering from the University of Calgary, Canada. He has been working with internet and security technologies for more than 10 years, predominantly within the financial and e-commerce industries at companies such as Morgan Stanley and eBay. Romanosky is co-author of *J2EE Design Patterns Applied and Security Patterns: Integrating Security and Systems Engineering* and has published other works on information security. He developed the FoxTor tool for anonymous web browsing and is co-developer of the common vulnerability scoring system (CVSS), an open framework for scoring computer vulnerabilities. Romanosky is currently enrolled in the Master of Science, Information Security Policy and Management Program at the Heinz School of Public Policy and Management at Carnegie Mellon University. He can be reached at sromanos@cmu.edu.

Gene H. Kim, CISA, is the chief technology officer (CTO) and founder of Tripwire Inc. In 1992, he co-founded Tripwire while at Purdue University with Dr. Gene Spafford. In 2004, Kim wrote the *Visible Ops Handbook* and co-founded the IT Process Institute, dedicated to research, benchmarking, and developing prescriptive guidance for IT operations, IT security, and auditors. Kim currently serves on The IIA Advanced Technology Committee.

Kim holds a masters degree in computer science from University of Arizona and a bachelors degree in computer sciences from Purdue University. Most recently, Kim was honored as one of the "Top 4 CTOs to Watch" by *InfoWorld* magazine due to his "forward-thinking and leading-edge activities." He also served as co-chair of the April 2003 SANS technical workshop, Auditable Security Controls That Work, hailed by SANS as one of their top five gifts back to the community and one of their top initiatives for 2003. Kim co-chaired the Best In Class Security And Operations Roundtable with the Software Engineering Institute in October 2003. Kim is certified on both IT Management and audit processes and holds an ITIL Foundations certification. He can be reached at genek@tripwire.com.

Bridget Kravchenko, CISSP, is an IT audit manager for General Motors Corp. and is responsible for developing and executing the infrastructure technology audit plans, as well as supporting the financial services processes for integrated audit support. General Motors operates in a highly-leveraged environment using numerous third-party IT providers from around the world. Kravchenko has more than 10 years of IT consulting experience and holds an ITIL Foundations certificate. She can be reached at bridget.kravchenko@gm.com.

Reviewers

The IIA Advanced Technology Committee, IIA global affiliates, AICPA, Center for Internet Security, Carnegie Mellon University Software Engineering Institute, Information System Security Association, IT Process Institute, National Association of Corporate Directors, and SANS Institute joined the review process. The IIA thanks the following individuals and organizations for their valuable comments to this guide.

The IIA, UK and Ireland

Rohit S. Antao, PricewaterhouseCoopers LLP, USA

Ken Askelson, JCPenney, USA

Christine Bellino, Jefferson Wells, USA

Larry Brown, The Options Clearing Corp., USA

Alfred Dahlmann, WestLB AG, Germany

David T. Flynn, Horn Murdock Cole, USA

Nelson Gibbs, Deloitte & Touche, LLP, USA

Michael S. Hines, Purdue University, USA

Dwayne Melancon, Tripwire, Inc., USA

Fernando Nikitin, Inter American Development Bank, USA

Jay Schulman, KPMG, LLP, USA

Jay R. Taylor, General Motors Corp., USA

Hajime Yoshitake, Nihon Unisys, Ltd., Japan

GTAG

Managing and Auditing IT Vulnerabilities

"Vulnerability management is a set of processes, supported by technology, that an organization employs to identify, assess, and mitigate business risks arising from the deployment and use of IT assets and processes. This guide was developed to help Chief Audit Executives assess the effectiveness of their organization's vulnerability management processes. It recommends specific practices to guide an organization toward achieving and sustaining higher levels of effectiveness and efficiency. After reading this guide, you will have a working knowledge of vulnerability management processes, and the ability to quickly differentiate between high- and low-performing vulnerability management organizations."

Jay R. Taylor, General Director-Global IT Audit, General Motors Corp.

What is GTAG?

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

Guide 1: Information Technology Controls

Guide 2: Change and Patch Management Controls: Critical for Organizational Success

Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment

Guide 4: Management of IT Auditing

Guide 5: Managing and Auditing Privacy Risks

Check The IIA technology Web site at www.theiia.org/technology

Order Number: 1021
IIA Member US $25
Nonmember US $30
IIA Event US $22.50

ISBN 0-89413-597-X

06634

www.theiia.org