

realtimepublishers.comtm

The Definitive Guidetm To

Security Inside the Perimeter

Apani

Rebecca Herold

Chapter 3: Multi-Dimensional Enterprise-Wide Security	52
Protection Strategies	52
Risk Analysis and Assessment.....	54
Risk Assessment and Analysis Methodologies.....	55
Define Risks.....	57
Risk Analysis and Assessment Challenges.....	59
Risk Analysis and Assessment Must Be Part of a Multi-Dimensional Security Strategy .	60
Security Policies, Procedures, and Standards	61
Information Security Policy	61
Information Security Procedures	61
Information Security Standards	62
Regulatory Requirements for Information Security Documents	62
The Goal of an Information Security Policy	63
Challenges of Policies, Procedures and Standards	64
Policies Are Viewed as Business Inhibitors	65
Education	65
Regulatory Requirements Compliance	66
Customer Trust and Satisfaction.....	66
Compliance with Published Policies.....	67
Due Diligence	67
Corporate Reputation	68
Accountability.....	69
Audit and Validation.....	69
Planning	71
Challenges of Audit and Validation.....	71
Legal Implications	71
Simplifying Complexity.....	72
Challenges in Simplifying Complexity.....	72
Divide and Conquer	73
Address Information Security Components Using an Enterprise-Wide Action Plan	73
Challenges to Simplifying Complexity.....	76
Summary	76

Copyright Statement

© 2005 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimerepublishers.com and the Realtimerepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimerepublishers.com, please contact us via e-mail at info@realtimerepublishers.com.

[**Editor's Note:** This eBook was downloaded from Content Central. To download other eBooks on this topic, please visit <http://www.realtimepublishers.com/contentcentral/>.]

Chapter 3: Multi-Dimensional Enterprise-Wide Security

Multi-dimensional security involves protecting the information assets and associated resources within all areas of an enterprise and in compliance with all regulatory, policy, and contractual requirements. It places protection at not only the perimeter, as has historically been the norm, but also wherever information is stored, processed, or transmitted. Multi-dimensional security involves more than just technology solutions; it also utilizes operational, administrative, and human forms of protection to help reduce the risks to information wherever information can be found.

At a high-level, a multi-dimensional security program includes the use of:

- Protection strategies
- Risk analysis and assessment
- Security policies, procedures, and standards
- Education
- Audit and validation
- Simplifying complexity

Using multi-dimensional security reduces the risk of a security breach, secures data flows throughout the transmission path, reduces the impact and cost of compliance audits, protects against insider attacks, and demonstrates due diligence.

Protection Strategies

There is no magic bullet solution that, in and of itself, will secure all enterprise information assets and systems in compliance with all contractual and legal requirements. Multiple protection strategies must be used to most effectively reduce and manage the risks that exist within today's highly decentralized and widely connected systems.

As a starting point, the strategies can be visualized as a combination of protecting connection points and processing and storage locations as well as educating the people who utilize them. Figure 3.1 represents these multi-dimensional topics and examples of the underlying components.

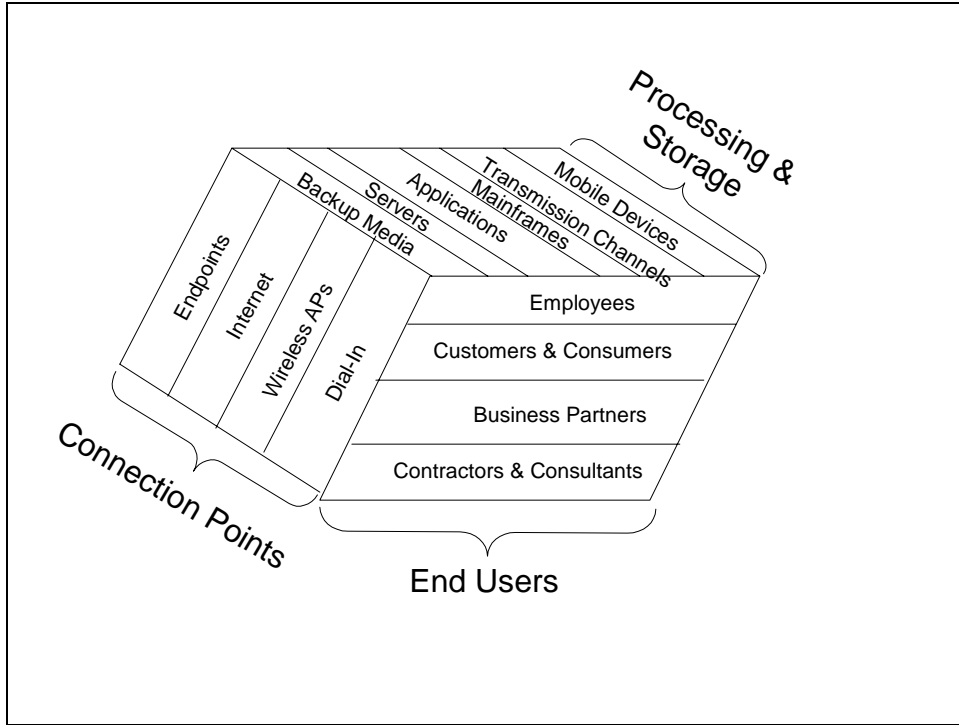


Figure 3.1: Illustration of multi-dimensional topics.

All these components are then working and handling information within the requirements outlined within policies, procedures, and standards, regulatory and legal requirements, education, and under the watch of audit and validation, as Figure 3.2 represents.

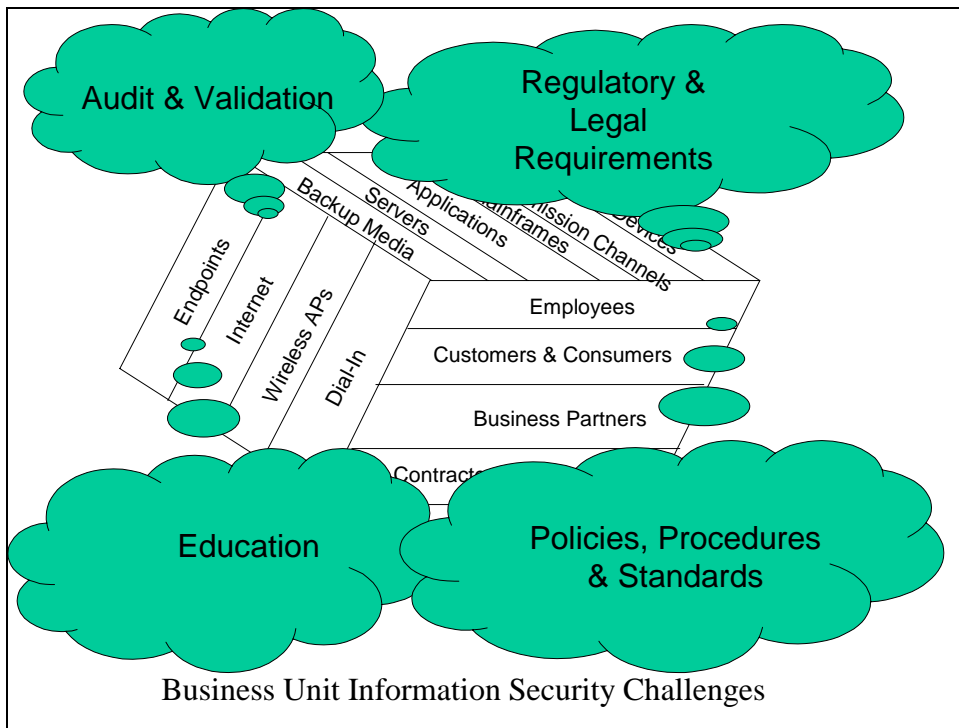


Figure 3.2: Multi-dimensional strategies within an organization's security requirements.

Each business unit must deal with these clouds of information security considerations. The typical organization will have many business unit information security clouds addressing these issues. Highly diverse multinational organizations will literally have information security considerations clouds covering significant areas of the earth, similar to the situation illustrated in Figure 3.3.

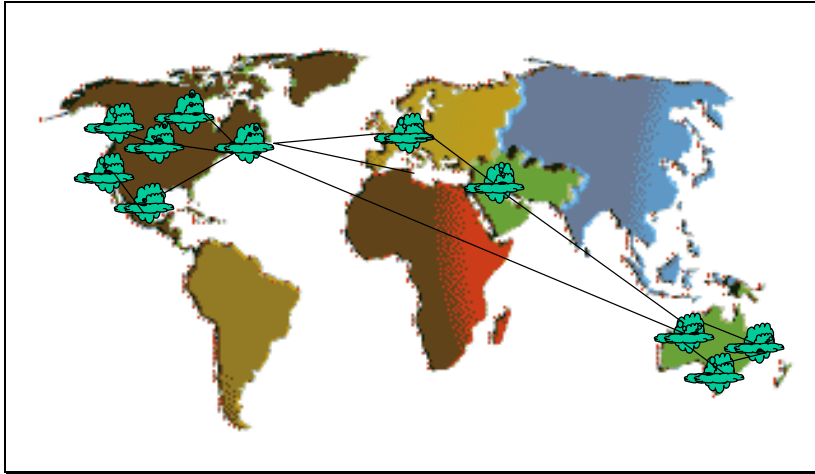


Figure 3.3: Worldwide processing locations and data flows.

The information components and issues within even the most seemingly simple organization can in actuality be quite complex. In a large organization, it can become almost overwhelming to information security practitioners to secure all these components and address all these issues. It is critical with so many components and issues to consider that organizations simplify the complexity as much as possible to be able to implement a successful information security program and subsequently help avoid dealing with information security incident storms that could result from all these volatile security considerations clouds crashing into each other. The first step in preventing your worldwide information security environment from experiencing destructive information security storms is to perform a risk analysis and assessment.

Risk Analysis and Assessment

It used to be that when businesses considered risks, they basically addressed the insurance coverage portfolio for the organization. Information security risk was not something at the top of business leaders' minds, or even in their thoughts, when the topic of risk management was mentioned.

As technology advanced, and as businesses became more decentralized and global, astute, forward-thinking business leaders realized that information was a cornerstone of successful business. As such, these leaders realized the need for appropriate protection to help reduce the risks to the confidentiality, integrity, and availability of the information.

Information security risk management evolved from the United States National Institute of Standards and Technology (NIST) Guidelines for Automatic Data Processing Physical Security and Risk Management (FIPSPUBs 31) and Guideline for Automatic Data Processing Risk Analysis (FIPSPUBs 65) in the mid-1970s. Because of the dramatic changes in the way information has been handled and processed since the introduction of what were then revolutionary documents, these FIPs were withdrawn in 2005 and 1995, respectively.

Risk Assessment and Analysis Methodologies

Since the introduction of risk analysis and assessment, there have been a wide range of methodologies and technologies developed for an even wider range of purposes. Some of the approaches are qualitative in nature, using metrics based upon information assets, threats, vulnerabilities, and safeguards and controls. Other methods are quantitative in nature, taking into consideration the monetary value of information assets, threat frequencies, threat exposure factors, and safeguard and control costs.

Risk Assessment and Risk Analysis...Defined?

First let us consider what is meant by the terms *risk assessment* and *risk analysis*. There has been much debate about these definitions over the years. NIST defines risk assessment and risk analysis within their Special Publication 800-30 as follows:

Risk assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

Note that NIST considers the terms to be one and the same in meaning. However, the International Organization for Standardization (ISO) defines these terms within ISO/IEC Guide 73:2002 as follows:

Risk analysis: Systematic use of information to identify sources and to estimate the risk

Risk assessment: Overall process of risk analysis and risk evaluation

Indeed there is room for interpretation. The goal of this guide is certainly not to argue for one term over another or to delineate the differences. For the purposes of this discussion, both terms will be used whenever discussing these types of risk management activities.

Most quantitative approaches are labor intensive and require the assessment/analysis facilitator to be a subject matter expert to most accurately determine the values of the risks. Unfortunately, a recurring weakness of risk assessments/analyses is that they usually fail to effectively communicate the discovered risks to business leaders, information owners, and decision-makers. Additionally, the accuracy of risk assessments/analyses is often in question, providing little value for business leaders and their decision-making process.

Automated tools can significantly reduce the labor and, to an extent, the inaccuracy of the monetary guesses associated with each risk. However, many businesses, frustrated with the cost and/or hard-to-use tools, have created their own in-house risk assessment/analysis methodologies and procedures. This process typically results in unstructured, uncoordinated methods for performing a risk assessment/analysis, and usually does not provide adequate consideration of all risks at all levels of the organization.


What Is Information Security Risk?

NIST defines risk in Special Publication 800-75 in the following two ways:

Security risk: The level of impact on agency operations (including mission functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Investment risk: Risks associated with the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints.

Reducing information security risks is a necessity in today's business environment. Any type of internal or external threat, risk, or vulnerability can quickly impact a well-running organization in many ways, such as losing a competitive advantage, losing customers, missing deadlines or orders, bad publicity, regulatory noncompliance resulting in fines and penalties, or costly civil suit judgments. Performing a risk assessment demonstrates your company is demonstrating due diligence for the decision-making processes throughout your organization.

 A well-constructed risk analysis provides the documentation you need to prove that due diligence is performed.

To perform a risk analysis and assessment that will be useful to your organization, you must first define the risks. There are many professional and industry associations and government agencies that have published risk management and analysis guidance. Groups that have published risk management and analysis guidance include:

- The American Institute of Certified Public Accountants (AICPA)
- The Institute of Internal Auditors (IIA)
- The Information Security Forum (ISF)
- The American Society of Industrial Security (ASIS)
- The Information Systems Audit and Control Association (ISACA)
- The Information Systems Security Association (ISSA)
- The International Information Security Foundation (IISF)
- The International Organization for Standardization (ISO)
- The National Association of Corporate Directors (NACD)
- The Organization for Economic Cooperation and Development OECD
- The United States Department of Homeland Security Critical Infrastructure Assurance Office (CIAO)
- The United States President's Commission on Critical Infrastructure Protection (PCCIP)

Define Risks

Define risks for your organization and within each of the business unit areas. What does legal consider as information risk? What do your privacy and compliance areas consider as information risk? What do your auditors consider as information security risk? What do information security leaders consider as risk? To be successful with a risk analysis and assessment, you need to first define organization-wide risks that exist within your environment and come to a consensus. The subsequent results of the risk analysis and assessment will then be more readily accepted as being applicable for your environment. When your coworkers participate in making security decisions, they feel ownership for the resulting actions that are implemented and are more likely to make a conscious effort for compliance.

The United States Office of Management and Budget (OMB) has identified 19 areas of information security risk, which are highlighted in the following list:

- Schedule—Risk associated with schedule slippages, either from lack of internal controls or from those associated with late delivery by vendors, resulting in missed milestones.
- Initial costs—Risk associated with “cost creep” or miscalculation of initial costs that result in an inaccurate baseline against which to estimate and compare future costs.
- Life cycle costs—Risk associated with misestimating life cycle costs, exceeding forecasts, and relying on a small number of vendors without sufficient cost controls.
- Technical obsolescence—Risk associated with technology that becomes obsolete before the completion of the life cycle and cannot provide the planned and desired functionality.
- Feasibility—Risk that the proposed alternative fails to result in the desired technological outcomes; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
- Reliability of systems—Risk associated with vulnerability/integrity of systems.
- Dependencies and interoperability between this investment and others—Risk associated with interoperability between other investments; risk that interoperable systems will not achieve desired outcomes; risk of increased vulnerabilities among systems.
- Surety (asset protection) considerations—Risk associated with the loss/misuse of data or information; risk of technical problems/failures with applications; risk associated with the security/vulnerability of systems.
- Risk of creating a monopoly for future procurements—Risk associated with choosing an investment that depends on other technologies or applications that require future procurements to be from a particular vendor or supplier.
- Capability of agency to manage the investment—Risk of financial management of investment, poor operational, and technical controls, or reliance on vendors without appropriate cost, technical, and operational controls; risk that business goals of the program or initiative will not be achieved; risk that the program effectiveness targeted by the project will not be achieved.
- Overall risk of project failure—Risk that the project/investment will not result in the desired outcomes.


- Project resources/financial—Risk associated with “cost creep,” miscalculation of life cycle costs, reliance on a small number of vendors without cost controls, or inadequate acquisition planning.
- Technical/technology—Risk associated with immaturity of commercially available technology and reliance on a small number of vendors; risk of technical problems/failures with applications and their inability to provide planned and desired technical functionality.
- Business/operational—Risk associated with business goals; risk that the proposed alternative fails to result in process efficiencies and streamlining; risk that business goals of the program or initiative will not be achieved; risk that the investment will not achieve operational goals; risk that the program effectiveness targeted by the project will not be achieved.
- Organizational and change management—Risk associated with organizational-, agency-, or government-wide cultural resistance to change and standardization; risk associated with bypassing, lack/improper use of, or non-adherence to new systems and processes because of organizational structure and culture; risk associated with inadequate training planning.
- Data/information—Risk associated with the loss or misuse of data or information; risk of compromise of citizen or corporate privacy information; risk of increased burdens on citizens and businesses because of data collection requirements if the associated business processes or project requires access to data from other sources (federal, state, and/or local agencies).
- Security—Risk associated with the security/vulnerability of systems, Web sites, and information and networks; risk of intrusions and connectivity to other (vulnerable) systems; risk associated with the evolution of credible threats; risk associated with the criminal/fraudulent misuse of information; must include level of risk (high, moderate, low) and what aspect of security determines the level of risk (for example, need for confidentiality of information associated with the project/system, availability of the information or system, or integrity of the information or system).
- Strategic—Risk associated with strategic- and government-wide goals; risk that the proposed alternative fails to result in achieving those goals or in making contributions to them.
- Privacy—Risk associated with the vulnerability of information collected on individuals or risk of vulnerability of proprietary information on businesses.

Risk Analysis and Assessment Challenges

Major problems exist with the language and use of risk analysis and risk assessment primarily because such activities did not evolve from academia or from a well-structured professional oversight body. Instead, information security practitioners have been forced to create their own risk analysis and assessment methodologies to meet their environments' needs. A significant number of information security professionals have performed what they label as risk assessments and skewed the results to meet their own agendas (for example, obtaining more budget or obtaining justification to remove systems they personally do not want to support). Such misuse of the risk assessment process has negatively impacted the perception of the usefulness of such risk review activities.

The language of results of the risk assessment/analysis is also typically vague or highly subjective. Such vagueness and subjectivity does not typically fit well within a business environment that is used to viewing risks in terms of dollars and cents. Unfortunately, most business leaders ask information security practitioners to quantify risks to determine budgets for information security expenditures. This requirement puts information security practitioners in the very difficult situation of losing the confidence of their management when they do not get the numbers exactly right.

Lacking a well-established taxonomy and terminology, even well-meaning, smart security practitioners discuss risk management in ways that can be misinterpreted or lead to poor business decisions. This misinterpretation results in confusion, frustration, and mistrust not only within an organization but also among the security professionals themselves. Inconsistent and misleading use of language results in inconsistent, misleading, and incorrect results of a risk assessment activity.

 Risk assessment and risk analysis are not the only misused terms in this area. *Threats* and *vulnerabilities* are often used interchangeably within risk assessment/analysis reports and by information security professionals, leading to confusion on the part of the readers, which are typically business organization leaders.

Most insightful risk and security leaders realize that security risks cannot be accurately and specifically calculated. The reason is that there is no body of complete and valid information covering information security upon which you can base calculations (unlike predicting financial investment risks based upon actuarial tables and significantly large and well-established bodies of incident information). However, performing risk assessment/analysis is still necessary for businesses to be able to adequately understand information risks and to determine which controls and tools to use to prevent the risks based upon how many times similar incidents have occurred elsewhere. The most realistic way to do so is through the use of qualitative risk analysis, based upon regulatory requirements and the potential impact from non-compliance fines and penalties. The assessment/analysis should then communicate what the financial impact experiences for each risk have been in other companies.


Organizations must meet the conditions of the various legal and regulatory requirements for performing a risk analysis and assessment. Smart organizational leaders will maximize the process of performing a risk assessment/analysis so that the requirements of as many applicable laws and regulations are met as possible to eliminate the need to do multiple assessments and end up duplicating work and effort.

Risk Analysis and Assessment Must Be Part of a Multi-Dimensional Security Strategy


Business leaders must recognize two givens:

- Each information system and process has its own risk environment
- Each information system and process has its own unique inputs, outputs, level of activity, and associated costs


Because of these differences, each information system and process will have unique security requirements that are determined by the associated risk environments.

 The risk environment determines the possibility of harm and loss, and the inputs, outputs, level of activity, and associated costs determine the magnitude of harm and loss resulting from the exploitation of the risks.


An effective risk assessment/analysis will document information about risk exposures. This risk information will be used to make the most optimal risk mitigation decisions to result in the best overall performance. An effective risk assessment/analysis will allow the business to invest enough, but not more than what is necessary, to appropriately address information security risks.

 It is bad business and bad information security management to spend \$10,000 to mitigate \$1000 of potential losses. Information security expenditures should not cost more than the value of the systems, assets, and processes being protected.

An effective risk assessment/analysis will produce a measure of risk so that risks can be consistently and reliably compared with one another, and the risk mitigation costs can be correlated to the risks they are addressing.

 A common mistake businesses make is assessing a risk as “high,” “unacceptable,” or some other qualitative term, then not providing the quantitative information (such as estimated lost time, money, customers, fines, and so on) necessary to support a decision to implement risk mitigation measures. Risk mitigation measures should always have quantitative implementation costs provided to make the assessment/analysis useful.

Security requirements are identified using a methodical assessment/analysis of security risks. Expenditures for risk mitigation controls must be balanced against the business harm estimated to result from security incidents and failures. The results of the risk assessment/analysis will help to guide and determine the appropriate management action and priorities for managing information security risks and for implementing the controls selected to protect against these risks.


 Risk assessment/analysis should be repeated periodically to address changes that might influence the risk assessment results.

Security Policies, Procedures, and Standards

Information security policies, procedures, and standards are all important considerations organizations must formally document and implement to have an effective information security program. Each type of document serves a different purpose.

Information Security Policy

An information security policy establishes the framework within which the business rules and regulations for handling information and reducing risk are described. Effective policies are created to help bring the organization into compliance with applicable laws and regulations as well as to address how to secure the business information processing environments within the organization. Management should set a clear policy direction in line with business objectives and visibly demonstrate support for, and commitment to, information security.

 Information security policies are mandatory; they should not be written in a way that implies they are merely suggestions.

Information Security Procedures

Information security procedures describe how to implement the policies. Procedures document the step-by-step detailed actions necessary to successfully complete a task that supports the policies. Procedures provide personnel with the information necessary to complete a task and provide assurance to management that the tasks are being completed in a consistent approved manner. Procedures improve efficiencies in employee workflow and assist in the prevention of misuse and fraud.

For example, a policy may require all information that leaves the organization to be encrypted. The corresponding procedure would define the tools and methods for encrypting the information, such as requiring the use of a virtual private network (VPN), along with details about each step to take to implement the software and hardware necessary to use the VPN in a way that is acceptable to the organization.

Information Security Standards

An information security standard is a detailed specification for hardware, software, and human actions to support the information security policies. Standards can detail the requirements for a wide range of issues, from the software to hardware that must be used to the remote access protocols that must be implemented to describing who is responsible for making information security approvals. Standards provide a documented way of ensuring that programs and systems will work together. By establishing standards, the enterprise limits the possibility of rogue applications systems, platforms, hardware, or software. There is less time spent in supporting non-standard activities or products. In short, standards define cost-savings processes that support the efficient running of the enterprise.

For example, a technical information security standard to support the policy requiring only corporate approved solutions be used to connect to the Internet might include a detailed description of how the transmission control protocol/internet protocol (TCP/IP) must be implemented, managed and used. A standard details the specific technical choices for implementing particular policies. For example, a policy may require strong identification and authentication be used when accessing information classified as confidential. The supporting standard might specify the specific brand and model of a microprocessor-equipped smart card to be used to enforce the access control restriction. Generally, those who are responsible for implementing policies use standards. Most standards do not need to be communicated to all personnel—only those responsible for the implementation of the policies. Standards also typically must be modified more regularly than policies in response to changing technologies and systems.

Regulatory Requirements for Information Security Documents

Many United States and international laws and regulations require organizations to document and implement policies, procedures, and standards. Additionally, business leaders must demonstrate that a standard of care exists within the enterprise. The implementation of these information security documents provides a demonstration of exercising due care.

Some of the laws and regulations that require organizations to document and implement information security policies, procedures, and/or standards include the following:


- The Gramm-Leach-Bliley Act (GLBA)
- The Health Insurance Portability and Accountability Act (HIPAA)
- Canadian Personal Information Protection and Electronic Data Act (PIPEDA)
- The European Union's Data Protection Directive



Additionally, the United States Federal Sentencing Guidelines for Organizations takes into consideration the policies implemented and clearly supported by executive management when they determine judgments for fines and penalties.


The Goal of an Information Security Policy

An information security policy documents executive management's direction on, and commitment to, information security. To be effective, you must communicate the security policy to everyone within your enterprise that handles your information or uses your systems.

 Executive management must communicate their direction on and commitment to information security within a high-level information security policy that applies to all parts of the enterprise.

An effective information security policy will

- Include a statement of direction from executive management supporting the goals and principles of information security.
- Communicate the business risks associated with information security incidents and accidents.
- Document information security, responsibilities, and the high-level principles personnel must observe.
- Specify key activities that must occur within the organization, such as carrying out security classifications and risk analyses, safeguarding important records, and reporting suspected security weaknesses.
- Require information to be protected in terms of its requirements for availability, integrity, and confidentiality.
- Emphasize the need for compliance with software licenses and other legal, regulatory, and contractual obligations.
- Prohibit unauthorized or personal use of the organization's information and systems and the use of obscene, racist, or otherwise offensive statements (for example, via email or over the Internet).
- Document that disciplinary action will be taken against individuals who violate policy requirements.

 An information security policy should be reviewed periodically and revised as necessary to reflect changes within the organization as well as technology changes.

Challenges of Policies, Procedures and Standards

The 2005 State of Information Security Study from CIO and CSO magazines includes results from interviewing 8100 IT security professionals from 62 countries. The survey results reveal that 8 percent of the companies have no documented security policy. The policy topics that occurred most frequently, as demonstrated by the accompanying percentages, within companies who had them included:

- User administration (69%)
- Appropriate use of email (56%)
- Systems administration (67%)
- Network security administration (55%)
- System security administration (52%)
- Appropriate use of the Internet (46%)
- Role-based access control (45%)


Twenty-four percent of companies had neither measured nor reviewed the effectiveness of their security policies and procedures.

These statistics reveal some of the challenges of creating and implementing policies, procedures, and standards:

- Organizations often do not base the policies upon existing leading practice frameworks and end up with a set of policies that have significant topics missing.
- Organizations often issue policies because they must, but then do not take any actions to verify the policies, procedures, and standards they have issued are effective or realistic in their environment.
- The majority of organizations are not addressing major security vulnerabilities, risks, and threats within their policies, such as mobile computing security and social engineering.

Policies Are Viewed as Business Inhibitors

In practice, information security seems to interfere with everyone's business. Network administrators work hard to make the networks as user-friendly and easy to use as possible, but then when security is applied—because of the mindset of the typical end-user—the security as implemented is very user-unfriendly and slows down users when they are trying to get their work done. Security policies challenge information and systems users to change the way they think about their responsibilities for protecting corporate information.

 When you attempt to implement security policies on an unwilling audience, you will be met with resistance not only because the security is viewed as making jobs harder and more tedious but also because the typical worker does not like to be told what to do...especially by an information security expert, who they do not see as having any authority over them or as having a place in their chain of command.

A big challenge worth tackling is to present information security to everyone within the organization in a way that enables them to recognize that they, personally and professionally, are responsible for information security. To be successful, information security officers must involve all personnel from throughout the enterprise in developing information security policies. Personnel must justifiably believe that they own their security procedures that support the policies. Personnel with real involvement in policy development will become partners to advance information security instead of being opponents of security.

Education

Supplying your personnel with the security information they need and ensuring they understand and follow the requirements is an important component to your organization's business success. If your personnel do not know or understand how to maintain confidentiality of your information or how to secure it appropriately, you risk not only having one of your most valuable business assets (information) mishandled, inappropriately used, or obtained by unauthorized persons but also being in noncompliance of a growing number of laws and regulations that require certain types of information security and privacy awareness and training activities. You also risk damaging another of your valuable assets—corporate reputation.

Regulatory Requirements Compliance

There are an increasing number of laws and regulations that require some form of training and awareness activities to occur within the organizations over which they have jurisdiction. Issues under the United States Federal Sentencing Guidelines that impact the severity of the judgments include consideration of the types of training and awareness organizations provide to their personnel. The following list is not exhaustive but provides some of the laws and regulations requiring training and awareness:

- HIPAA
- 21 CFR Part 11 (Electronic Records/Electronic Signatures)
- Bank Protection Act
- Computer Security Act
- Computer Fraud and Abuse Act (CFAA)
- Privacy Act
- Freedom of Information Act (FOIA)
- Federal Information Security Management Act (FISMA)
- 5 U.S.C. §930.301 (for United States federal offices)
- Appendix III to OMB Circular No. A-130
- Digital Millennium Copyright Act (DMCA)
- GLBA
- Department of Transportation DOT HM-232
- The Sarbanes-Oxley Act
- The Organization for Economic Cooperation and Development (OECD) Security and Privacy Principles
- The European Union Data Protection Directive
- Canada's PIPEDA


Customer Trust and Satisfaction

Respect for customer security and privacy is one of the most important issues facing your company today. To gain and keep customer trust, your company must exercise good judgment in the collection, use, and protection of personal information. Not only do you need to provide training and awareness about this requirement to your personnel, but you also need to communicate to your customers (with whom you have a business relationship) and consumers (with whom you would like to have a business relationship, and who may have provided some information to you) what you are doing to preserve their privacy and ensure the security of their information through various awareness messages.

All workers (employee and contract) or companies who directly handle or impact the handling of your company information should take your security training before handling your company information, with refresher training every year, or more often based upon your business and the potential impact to your business if information is not handled correctly. You should provide training and awareness to ensure all your company activities comply with the company privacy policy as well as laws and regulations.

Compliance with Published Policies

Organizations need to educate personnel about their information security roles and responsibilities—especially in support of published policies, standards, and procedures. Awareness and training should be constructed to support compliance with security and privacy policies. Executive management act as role models for personnel; their actions heavily influence the level of employee awareness and policy compliance. Senior management should clearly and noticeably support, encourage, and show commitment to information security and privacy training and awareness activities.

 Implement a procedure to obtain a signed information security awareness agreement at the times you deliver the training to document and demonstrate that training and awareness activities are occurring, that the personnel acknowledge and understand procedures, and that the education efforts are ongoing.

In addition, include evaluation of information security and privacy actions within the yearly job performance appraisal for all personnel.

Due Diligence

In general, due diligence means providing demonstrated assurance that management is exercising adequate protection of corporate assets, such as information and compliance with legal and contractual obligations. This requirement is a powerful motivator to implement a training and awareness program. Key provisions of the United States Federal Sentencing Guidelines and 2004 amendments include establishing an effective compliance program and exercising due diligence in the prevention and detection of criminal conduct. Any organization with some type of compliance requirements and/or plans (basically all public entities given the Sarbanes-Oxley Act of 2002) is directly impacted by the guidelines. One way such due diligence is demonstrated is through an effective, executive-supported information security education program.

It is no longer good enough simply to write and publish information security and privacy policies and procedures. Organizational leaders must now have a good understanding of the policies and the program, support the program, and provide oversight of the program as reasonable for the organization. This new requirement reflects a significant shift in the responsibilities of compliance and ethics programs from positions such as the compliance officer and/or committee to the highest levels of management. The guidelines require that executive leaders support and participate in implementing the program. To do so, an effective ongoing information privacy, security, and compliance education program must be in place.

Corporate Reputation

Reputation is another critical organizational business success asset. Without a good reputation, customers leave, sales drop, and revenue shrivels. Reputation must be managed well. A component of managing good reputation is ensuring personnel and business partners follow the right information security actions to lessen the risk of something bad happening to information; such incidents will likely lead to very unseemly news reports and media attention.

There are many issues that impact corporate reputation that can be addressed through effective ongoing information security training and awareness activities:


- Customer complaints
- Competitor messages and internal messages related to competitors
- Customer satisfaction levels with your organization's security and privacy practices
- Providing for customers with special needs and requests
- Number of legal noncompliance reports regarding security and privacy
- Perceived strength of posted security and privacy policies
- Marketing with what is considered as spam
- Number of staff grievances
- Upheld cases of corrupt or unprofessional behavior
- Number of reported security and privacy incidents
- Staff turnover related to training and communications
- Value of training and development provided to staff
- Perception measures of the company by its personnel
- Existence of confidential grievance procedures for workers
- Proportion of suppliers and partners screened for security and privacy compliance
- Proportion of suppliers and partners meeting expected standards on security and privacy
- Perception of the company's performance on security and privacy by consumers worldwide
- Proportion of company's managers meeting the company's standards on security and privacy within their area of operation
- Perception of the company's performance on security and privacy by its employees
- Perception of the company's performance on security and privacy by the local community
- Dealing with activist groups, especially militant groups, opposed to the organization

Accountability

Most personnel understand that if they are being measured for certain activities, they need to be accountable for those activities because those measures can impact their career with the company in some way. If an organization reports information security compliance and connects it with personnel performance, personnel understand more clearly their accountability and are even more likely to comply.


Accountability has more impact on a company, and corporate personnel, than ever before. There are a growing number of legal actions being filed by victims of inadequate information security and privacy practices against organizations that were not necessarily the perpetrators of an incident but whose systems and poor practices contributed to allowing the incident to occur. Such shifts in accountability start moving the enforcement of policy from management to individuals. Such shifts are also being supported by new regulations and government moves, such as requiring federal agencies to increase personnel accountability for breaches and requiring security to become standard in all network and computing products.

Implementing the use of signed information security awareness acknowledgements not only establishes personal accountability but also increases awareness and accountability for information security and privacy. Such signed acknowledgments document your organization's efforts and due care to ensure all personnel are given the information they need to perform their job responsibilities in a manner that protects information and network resources. Signed acknowledgments should be considered a facilitator for your awareness and training efforts. Signed acknowledgements could also provide valuable support for any sanctions you need to administer for policy noncompliance.

 Your organization should expect all employees, officers, contractors, and business partners to comply with privacy, security, and acceptable use policies and protect your organization's information and systems assets.

Audit and Validation

Security audits and compliance validation reviews provide an in-depth examination of an organization's security infrastructure, policies, people, and procedures. When performed effectively and successfully, they will identify areas of weakness within the infrastructure. The auditor or reviewer can then provide recommendations for appropriate actions to address the weaknesses and reduce the accompanying risks.

 Audits are important to ensure that corporate security policies are being followed and enforced. How can you ensure your access control policies are effective unless an audit is performed to review them?


Audits need to be performed to provide individuals who are responsible for particular IT environments, as well as executive management, with an independent assessment of the security condition of those environments and to validate that necessary controls are indeed in place and functioning as they should. The information security status of the enterprise environments should be subjected to thorough, independent, and regular security audits and control validation reviews.

Security audits and compliance validation reviews must include consideration of the business risks associated with the particular environment (the security clouds described earlier) under review and should be performed for critical business applications, information processing environments, communications networks, system development activities, and manual administrative and operational tasks.

Security audits and compliance validation reviews should be:

- Agreed upon and supported by the individual responsible for the environment under review
- Performed by qualified individuals who have sufficient technical skills and knowledge of information security
- Conducted frequently and thoroughly enough to provide assurance that security controls function as required
- Complemented by reviews conducted by independent third parties

Recommendations for improvement resulting from the audits should be discussed and agreed upon with the individuals responsible for the environment under review and should be implemented and reported to executive management.

 Information systems, processes, and practices security should be regularly reviewed. Perform the reviews against the appropriate security policies and the technical platforms and information systems for compliance with applicable security implementation standards, documented security controls, and regulatory and contractual compliance.

Audit requirements and activities involving checks on operational systems must be carefully planned and communicated to the audited area's management to minimize the risk of disruptions to business processes. You want information security to be viewed as a business enabler not as an obstacle to achieving business goals. To help enable the success of an audit, keep the following guidelines in mind:

- Obtain agreement with the audited area's management for the activities being performed
- Determine and document the scope of the activities
- Limit the audit checks to read-only access to software and data; if necessary for the audit, allow access other than read-only for isolated copies of system files
- Explicitly identify the resources that will be used to perform the checks
- Identify and agree upon with management the requirements for special or additional processing
- Monitor and log all access to produce a time-stamped reference trail for all critical data or systems
- Document all procedures, requirements, and responsibilities for the audit activities
- Ensure the person(s) carrying out the audit are independent of the activities audited


Planning

Senior management should establish a plan to perform regular and independent audits to evaluate the effectiveness, efficiency, and economy of security and control procedures in addition to management's ability to control information security function activities. Senior management should determine priorities with regard to obtaining independent audits within this plan. Auditors should plan the information security audit work to address the audit objectives and to comply with applicable professional auditing standards.

Challenges of Audit and Validation

Organizations must integrate their information security goals within business strategies to reach their overall enterprise objectives, get the most value out of their information, and capitalize on the technologies available to them. As computerized applications are penetrating nearly all business functions and processes, organizations are mixing hardware platforms from different vendors with a combination of commercially available software and in-house developed software. Issues such as IT governance, international information infrastructure, e-commerce, security, privacy, and control of public and enterprise information have driven the need for self-review and self-assurance. These issues combined make the audit and validation process much more challenging and complex than in the past when information processing was generally limited to a large mainframe computer.


As a result of this increasing complexity, business risk increases. Audits and reviews are needed to evaluate the adequacy of information security to address the adequacy of all the information security and controls used by all the people, places, and processing systems. Recent situations such as those at Enron, WorldCom, and others have clearly shown the need for audit and independence.

 The Sarbanes–Oxley Act of 2002 is one example of a regulation providing the needed support for organizations to address their organizational policies and controls and use the capabilities of their internal audit and information security teams.

Legal Implications


In the years preceding the Sarbanes-Oxley Act, limited liability partnerships formed following the result of a Big Five audit organization that was taken to court by a client. The client selected a support system based on the firm's recommendation. However, the support system failed to perform in the manner recommended and caused the company financial loss. The courts held the Big Five firm liable for failing to exercise "due professional care" in the conduct of their work performed. The Big Five company sought the protection of a limited liability partnership with its audited client.

With the fall of Arthur Andersen LLP during the Enron scandal, there is now a Big Four. Arthur Andersen LLP was the first major international accounting firm taken to court and successfully convicted for a lack of due professional care in the destruction of client documents and obstructing justice. After a month-and-a-half trial and 10 days of deliberations, jurors convicted Andersen for obstructing justice when it destroyed Enron Corp. documents while on notice of a federal investigation. Andersen and their lawyers had claimed that the documents were destroyed as part of its housekeeping duties and not as a ruse to keep Enron documents away from the regulators.

 The Sarbanes-Oxley Act regulation is not the only law that serves to compel organizations to perform regular information security audits and compliance reviews. A few of the others include HIPAA, GLBA, 21 CFR Part 11, the Bank Protection Act, the Computer Security Act, the Computer Fraud and Abuse Act (CFAA), the Privacy Act, FOIA, and the Federal Information Security Management Act (FISMA).

Simplifying Complexity

The beginning of this chapter discussed the many different components and multiple dimensions of addressing information security. Many organizations find themselves trying to fight fires and tackle all the related information security issues without first taking the time to create a thoughtful information security strategy. The strategy needs to simplify the complexity resulting from such highly diverse, dispersed, and dimensional environments.

 Organizations must simplify the complexity of information security management by taking the large number of technology, human, and compliance issues and making them understandable to the business. At the same time, organizations must implement solutions to integrate these issues throughout all business processes so that information security is built-in to all products and services from the beginning of a business idea right through until the resulting service or product is no longer offered.

These complexities can be simplified using a common framework of information security disciplines and by getting the support of the information security efforts by the leaders throughout the organization rather than focusing on each individual issue at a time. The first step in simplifying information security complexity is by appointing an enterprise-wide information security officer to oversee and coordinate information security activities and decisions for the entire enterprise. This oversight will not only be the first step in simplifying complexity but also lead to consistency in addressing information security issues throughout the enterprise.

Challenges in Simplifying Complexity

Information security practitioners have been struggling with how to simplify the complexity of information security management for years. To many of them, it seems as though for every step forward they take with progress, they take two steps back because of how swiftly technology changes, how swiftly new connections are made to their networks, and how swiftly more and more employees and business partners are mobilizing their business information processing. Most also focus on just one business unit issue at a time, resulting in the information security function hop scotching back and forth between different services and products, and not coordinating efforts or maximizing the benefits of rolling information security controls out to all enterprise areas at the same time. Information security leaders end up constantly fighting security fires as each business unit information security cloud lightning strikes.

Divide and Conquer

To be effective, information security leaders must implement an information security strategy to simplify their efforts. To do so, consider each of the components within the multi-dimensional information security issues, divide your security responsibilities throughout the organization, and use automation to simplify and conquer your information security activities and challenges.

Too many times information security practitioners try to take on all the information security tasks themselves. This undertaking is not only unfeasible in most situations but also does not foster the need for all personnel to take responsibility for information security. When everyone is part of the development of information security, as a whole, organizations can then identify tools to address those activities that can be automated. There will be many areas where you can automate some of your information security activities throughout the enterprise (for example, through the use of centralized intrusion detection systems, access logs, antivirus solutions, and so on).

Address Information Security Components Using an Enterprise-Wide Action Plan

Dividing and distributing the information security responsibilities throughout the entire enterprise can accomplish simplification of complexity. One way to do so is by implementing the following:

- Assign overall responsibility for enterprise information security oversight.
- Establish an information security oversight board consisting of management representatives from each business unit and corporate functional office.
- Assign responsibilities for each of the governance categories:
 - Education through training and awareness
 - Regulatory and legal requirements
 - Audit and validation
 - Policies procedures and standards

- Assign responsibilities to representatives from each corporate and business unit for each of the security dimensions:
 - Connection Points
 - Endpoints
 - Internet
 - Wireless
 - Dial-In
 - End users
 - Employees
 - Customers and consumers
 - Business partners
 - Contractors and consultants
 - Processing and storage
 - Mobile devices
 - Transmission channels
 - Mainframes
 - Applications
 - Servers
 - Backup media

Figure 3.5 provides an illustration of an example distribution of security responsibilities.

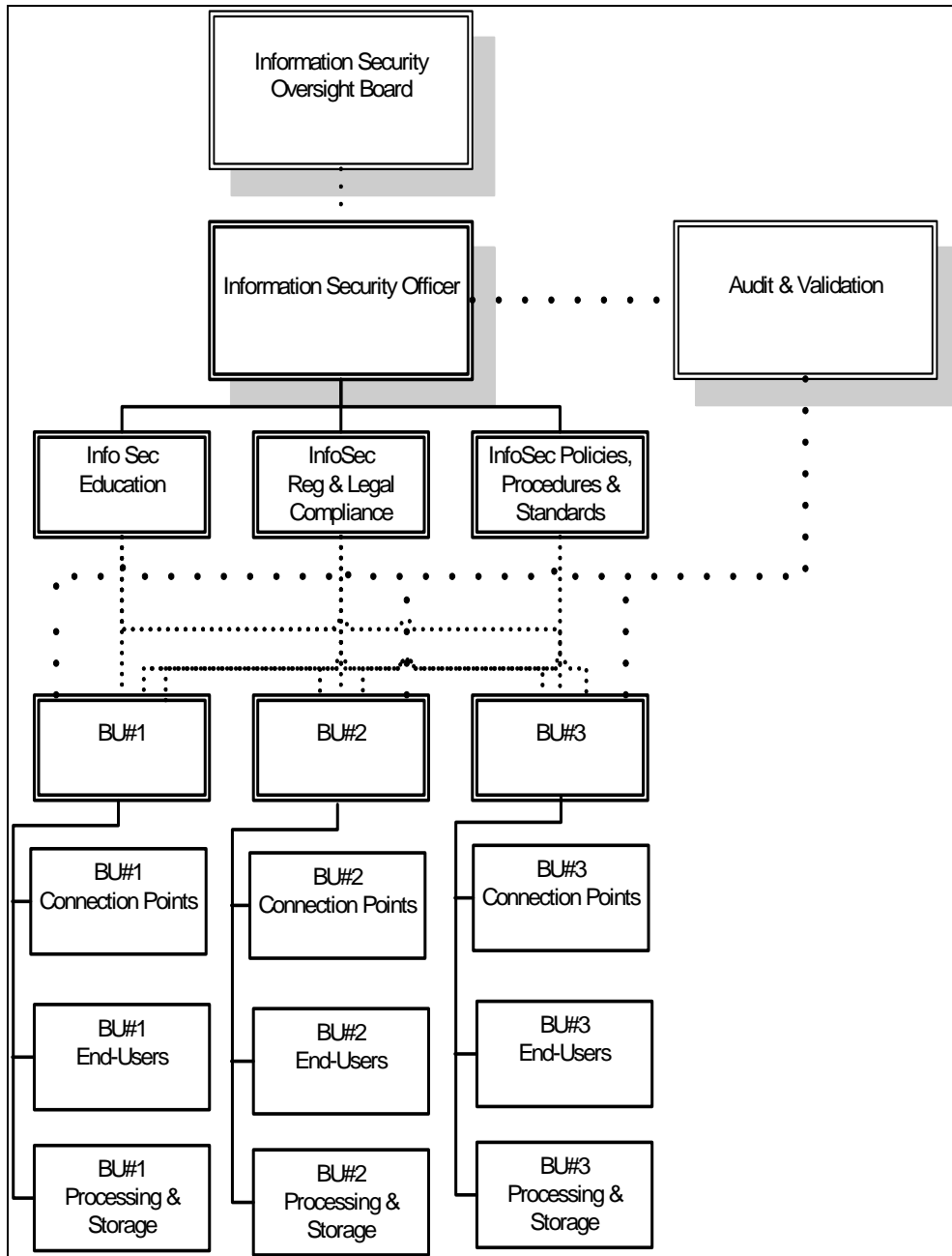


Figure 3.5: Example distribution of enterprise information security responsibilities.



Each role with information security responsibilities should use proven technology tools to automate as much as possible their responsibilities.

Challenges to Simplifying Complexity

Even when dividing and distributing information security responsibilities throughout the enterprise, information security leaders will still face challenges to simplifying the accompanying complexity of information security management. Some of these challenges include:

- Communicating the need for information security effectively so that it is not seen as just a technology issue.
- Making information security seamless to end users.
- Staying abreast of new regulatory and legal requirements for information security activities.
- Making sure business partners are adequately securing the information that you have entrusted to their care.
- Keeping up-to-date with new information security risks, threats, and vulnerabilities.

Summary

For an effective information security program, a business must implement a multi-dimensional security program that includes the use of:

- Protection strategies
- Risk analysis and assessment
- Security policies, procedures, and standards
- Education
- Audit and validation
- Simplification of complexity

Establishing a thoughtful information security strategy based upon identified risks and managed by one enterprise role with responsibilities distributed throughout the enterprise help to simplify the complexity of addressing security and help to ensure an effective information security program. The next chapter will discuss the value of zoning to address these complex multi-dimensional information security issues and challenges.

Content Central

[Content Central](#) is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, learning about new development tools for Windows and Linux, or deploying new enterprise software solutions, [Content Central](#) offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBooks!

If you found this eBook to be informative, then please visit Content Central and download other eBooks on this topic. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to other great IT eBooks and video guides. Please visit: <http://www.realtimepublishers.com/contentcentral/>.