

# Conducting an Information Security Gap Analysis

by Rochelle Shaw

Copyright 2012, Faulkner Information Services. All Rights Reserved.

Docid: 00018422

Publication Date: 1207

Report Type: IMPLEMENTATION

## Preview

An information security gap analysis is a critical step in the Business Continuity Planning process and is a form of risk assessment. A gap analysis is designed to determine the differences between the present state of information security within an enterprise and its ideal, or optimum, state. Existing standards, including those developed by the International Organization for Standardization (ISO), the Information Systems Audit and Control Association (ISACA), and the National Institute of Standards and Technology (NIST), represent guidelines for the process of gap analysis, but should be used as a part of comprehensive business security plan. This report defines an Information Security Gap Analysis, looks at possible pitfalls, and provides a step-by-step implementation plan.

Report Contents:

- [Executive Summary](#)
- [Description](#)
- [Possible Pitfalls](#)
- [Step-by-Step Implementation](#)
- [Web Links](#)

## Executive Summary

[return to [top](#) of this report]

An information security gap analysis is a necessary part of a business' risk management and business continuity programs.

One of the preferred methods of performing this security gap analysis is to ask a series of probing questions, in the manner of a security audit. For example, if one of the objectives of the Enterprise Information Security Plan is to limit access to central servers and other IT infrastructure components, critical queries may include:

- Are all enterprise servers housed in a restricted area, such as a computer room?

- Is access to the server room limited to essential personnel?
  - Are biometric access controls employed to govern entry?
  - Is the server room monitored by video surveillance cameras?
- 
- How many attempts at unauthorized access are routinely recorded, and how are these incidents investigated?

The purpose of the survey is not punishment but rather to determine the actual level of existing security, what gaps exist between the security plan and the actual level of security, what security measures must be taken to narrow or eliminate the gaps, and what costs are involved. While a survey of this nature may be seen as adversarial by those providing the answer, care must be taken to ensure that the process is not used as a means to punish survey respondents or to gain some kind of political advantage. If responders see the survey being used as a punitive measure, fewer employees will respond to the survey, making it likely that the results will be compromised.

While the survey is one part of the gap analysis only, just as gap analysis is one part of a Business Continuity Plan (BCP); however, it can be the step in the process that makes or breaks the analysis. Much of the remaining steps are objective measurements that are necessary but give little insight into the mindset of a particular organization regarding security.

## Description

[return to [top](#) of this report]

An information security-related gap analysis identifies information security gaps that may exist within an organization by examining the current information security stance to industry best practices or standards and regulations. However, gap analysis is not a standalone process. It is a step, albeit a strategic one, in the development of a BCP.

## Business Continuity Plans

A Business Continuity Plan (BCP) is an over-arching program for organizational security that includes:

- A Business Impact Analysis - Used to identify the critical functions of a business.
- Risk Assessment and Analysis - Determines what the potential risks are, how each will affect business, and how to deal with them. This includes an information security gap analysis.
- Disaster Recovery Processes - Includes recovery processes for each critical business function.
- Development of the BCP.
- Testing and Re-Testing of the BCP - Includes conducting regular security gap analyses as part of an ongoing risk assessment process.

## The Gap Analyst

While it may seem counterintuitive, the individual conducting an information security gap analysis does not have to be a security "expert." Experts tend to focus narrowly on one aspect of security such as network security while ignoring other aspects such as laptop security. Also, experts are inclined to concentrate on technical details, rather than seeking to implement the overall BCP.

## Finding the Gaps

While there is a natural tendency to focus on network security, ensuring proper protection from viruses, worms, and other forms of malware that propagate over the Internet, an information security gap analysis is not complete without considering other common, but often overlooked, exposures, such as laptop security, physical security, and personnel security.

**Laptop Security.** A source of security failure since the invention of the devices and their adoption inside businesses, laptops continue to be the source of major leaks of information used by malicious individuals to steal personal identities, make use of proprietary information, or discover passwords to the internal business network. In almost all cases, an information security gap analysis could have been used to reveal:

- The failure to password-protect files.
- The failure to encrypt sensitive data.
- The failure to store laptops in a secure location.
- Unauthorized use of laptops that contain business critical data on non-secure networks and in non-secure locations such as restaurants or donut shops.

**Physical Security.** Although physical security and information security are considered separate disciplines, they actually overlap to some degree. In particular, when performing an information security gap analysis, an examiner should determine:

- Who has physical access to IT infrastructure components, such as servers and routers?
- What environmental safeguards exist, such as temperature and humidity controls?
- What provisions have been made to protect equipment against fire and water damage?

**Personnel Security.** Most experts agree that the majority of security incidents, either inadvertent or intentional, are committed (or enabled) by employees (or other insiders). An information security gap analysis must explore:

- How are security personnel vetted?
- Are there security awareness programs that discourage insider attacks?
- What actions are taken to protect systems from employees that are laid off or fired during their exit and after departure?
- What action (or actions) are taken against individuals who deliberately and maliciously violate information security?

## Benefits of Conducting a Gap Analysis

Quite possibly the most important benefit of conducting a gap analysis is that it identifies a beginning point from which an organization can measure its improvement over time. Additionally, a gap analysis can identify what the organization already does well, thus saving time and money by not fixing something that, as the saying goes, "ain't broke." Gap analysis can frequently identify capabilities that already exist within an organization, offering the ability to promote these capabilities rather than adopt new ones.

Gap analysis can diagnose problems and provide recommendations on how to solve these problems. Since it enables long-term planning by setting goals and outlining changes and practices, the ultimate goal of a gap analysis is to gain a list of prioritized activities that an organization can complete to move itself closer to its vision.

# Possible Pitfalls

[return to [top](#) of this report]

## Not Establishing Gap Analysis as A Regular, Ongoing Task

Unless a company regularly performs a gap analysis, it may be overwhelmed by the number of gaps it finds when it eventually conducts one. Prioritize the gaps, patch the ones that present the greatest threat, and perform other analyses to determine the next round of fixes. Even if an analysis shows no gaps, an unlikely occurrence, an annual gap analysis makes sure that policies continue to be followed.

## Lack of Objectivity

It is difficult for internal systems administrators to objectively analyze a company's security controls. While it may be prudent to engage outside experts, a company's or agency's IT department should be involved in all phases of a gap analysis, including the preparation, the conduct, and, most important, the development of plans designed to eliminate any security exposures. The reason is twofold. First, the IT staff is a valuable source of operational information; and second, the IT staff will almost certainly be involved in implementing and maintaining any security fixes. In short, the IT staff definitely needs to be onboard with any proposed changes.

## Using Consultants without Industry Knowledge

Whether intentional or not, consultants may feel pressure to overstate elements that they can fix and understate other elements. Boilerplate analyses and remedies are also hazards. Choose a consultant that knows the applicable industry and has a business orientation that is consistent with that of the company.

Check a consultant's references. The consultant should have a background of working with the applicable industry but also of working with organizations of equal size - a multi-national corporation should look for a consultant that has worked with multi-nationals before. Smaller businesses should seek consultants with commensurate experience.

## IT Staff Turnover

High turnover in the IT field has laid the groundwork for an increased threat of security breaches. Attacks by disgruntled ex-employees and disgruntled current employees represent a high percentage of database and network attacks.

## Security as a Low Priority

Large companies are so focused on rolling out new infrastructure and products that they frequently lose sight of security. In addition, companies find it easier to cut back on security programs when times get lean since security can rarely be shown to produce revenue.

## Fear of Bad News

Many firms are reluctant to conduct a gap analysis for fear of what it might reveal. The good news is that a gap analysis highlights both weaknesses and strengths. This dual perspective can help empower an organization by

acknowledging what it does right while at the same time encouraging that organization to change what it does wrong.

## Step-by-Step Implementation

[return to [top](#) of this report]

Experts suggest a methodical approach to gap analysis, stressing pre-analysis preparation.

1. Adopt an information security standard (if one is not already being used). The ISO 18028-5:2006 standard deals with information security and includes gap analysis. The ISO-17799:2005 was withdrawn in June 2010 and replaced by ISO 27002:2005, which presents guidelines and best practices for organizations to use when conducting risk assessments. ISO 27000 is a family of information security management standards that includes all phases of a BCP. NIST SP 800-65 also represents a guideline for security management, including security gap analysis. The NIST SP 800 family of publications deal with different aspects of information security, including the latest publications involving cloud computing. ISACA's COBIT 4.1 is an IT governance model that includes gap analysis. COBIT 5.0, which is in draft format, will supersede COBIT 4.1.
2. Define the scope of the analysis. In a large enterprise, it may be necessary to conduct multiple analyses, evaluating, for example, one location at a time, or assessing network security apart from mobile and wireless security.
3. Assemble all relevant documents. These include all information security standards, policies, plans, protocols, procedures, and guidelines.
4. Gain senior management approval. If necessary, the chief security officer (CSO) should provide the visible support for the analyst, persuading business and technical managers to cooperate in identifying and filling security gaps.
5. Create a comprehensive information security questionnaire. Use the questionnaire to elicit information about current information security practices, and expand the questionnaire as avenues of inquiry appear. Suppose, for example, a preliminary question reveals the use of two different types of physical access controls. A follow-up question might reveal how each type is used, setting the stage for a new enterprise standard. In addition to improving efficiency, the use of a standardized questionnaire permits a year-over-year comparison of gap analysis results, revealing how security performance varies over time.
6. Look for gaps from a total systems management perspective. Information security exists within multiple systems management disciplines, including incident and problem management, change and release management, configuration management, service level management, and IT service continuity management. Ensure that information security is consistent across the full range of these functional areas.
7. Publish a preliminary Information Security Gap Analysis report. Before documenting any deficiencies for senior management, offer security personnel an opportunity to review and challenge any findings. Where gaps are discovered, offer these same personnel the opportunity to close or reduce the gaps before a final report is issued. In this way, analysts can earn the trust and confidence necessary to perform an in-depth analysis.
8. Develop a remediation plan. Working in concert with the CSO, develop a plan to reduce or eliminate any information security gaps.<sup>1</sup>

The following are steps in a standard gap analysis.

### Step 1: Stage a Systems Break-In

Engage a security consulting company to conduct a systems break-in. Ask the company to operate in the manner

of a hacker or cyber-terrorist and penetrate enterprise defenses. If they are successful (and, unfortunately, they probably will be), their simulated attack will offer two major benefits:

- For anyone who still needs to be convinced that security is a major issue, it will elevate the level of concern beyond the realm of perceived risk to one of real risk.
- The attack will probably target the same vulnerabilities that real-world cyber-criminals would exploit, allowing the most serious exposures to be identified and eliminated.

### Step 2: Secure Senior Management Approval

Much like business continuity planning, conducting a gap analysis requires cross-organizational cooperation. In many enterprises, achieving such cooperation is only possible through the eager endorsement of senior executives. The time to gain organizational cooperation is at the outset as it is important to get everyone on board early.

### Step 3: Establish the Scope of the Analysis

Establish the extent of the gap analysis as well as its general objectives. This can be accomplished by asking the following key questions:

- Will the analysis include physical as well as electronic security?
- Will the investigation focus on the headquarters location, or will it also encompass branch office and remote sites?
- Will the analysis concentrate only on "customer-facing" applications, or will it include all IT systems?
- What budgetary, personnel, and physical resources will be available to conduct the analysis?
- What is the timetable? When will management expect to see concrete results?
- What regulatory mandates must be adhered to? Are there any mandated procedures that must be used to meet them?
- Have all of the project parameters been established? In particular, have all of the issues been identified? If there are outstanding issues, when will they be resolved?

### Step 4: Determine Whether to Outsource or Conduct the Analysis In-house

After receiving permission to conduct a gap analysis, the big question is whether or not to outsource. Table 1 summarizes some of the advantages and disadvantages of outsourced analysis.

**Table 1. Outsourced Gap Analysis**

| Advantages   | Disadvantages   |
|--|---|
| In general, greater and more current security expertise. | Unfamiliarity with specific enterprise systems and operations.                                |
| More experience in gap analysis.                         | Ironically, the potential for exposure of critical or sensitive information to third parties. |

|  |   |
|--|---|
| Greater objectivity relative to enterprise security practices. | In general, higher costs.   |
| Less reluctance to criticize enterprise security practices.    | Resentment from in-house security personnel, who may feel threatened. |

Both outsourcing and in-sourcing are viable options. If outsourcing is selected, the process must be closely supervised by management to ensure the cooperation of all personnel. In addition, in-house security staffers can learn a great deal from their outsourcer colleagues. If in-house development is selected, proceed with Step 5.

### Step 5: Assemble a Gap Analysis Team

Coordinate all activities related to the gap analysis, including planning, implementation, analysis, reporting, and assembling a gap analysis team. This multi-disciplinary team should include:

- In-house security experts.
- Members of the IT department.
- Customers, both internal and external.
- Trusted business partner personnel, particularly any analysts who are wrestling with the same or similar security problems within their own enterprises.

### Step 6: Resolve Any Jurisdictional Issues

Closely related to the previous item, determine which enterprise organizations might claim jurisdiction or authority over all or part of the analysis process. Consult with groups such as:

- Finance.
- Corporate Auditing.
- Business Continuity.
- The Project Management Office (PMO).
- The Risk Management Office.

Ask these organizations to appoint individuals to participate as members of the gap analysis team to contribute their own expertise and experience and function as liaisons to their respective groups.

### Step 7: Identify Current Security Standards

Determine all relevant security standards and protocols. This includes the enterprise security policy, any statement of enterprise security standards, and, depending on the affected industry, any relevant governmental regulations, such as HIPAA, Sarbanes-Oxley, and the Gramm Leach Bliley Act (GLBA).

### Step 8: Collect All Relevant Security Documents

In concert with the previous item, collect all pertinent documentation relating to security standards such as policies, protocols, plans, and procedures, plus any pre-existing analyses of the organization's security infrastructure. It is also important to gather all documentation relating to the deployment and use of enterprise hardware and software.

## Step 9: Create a Gap Analysis Checklist

As with any project, a gap analysis should proceed according to a specific plan or checklist. The checklist will:

- Ensure the analysis is complete and comprehensive by allowing others to review it prior to implementation.
- Provide a structure for recording (and later reporting) the results of the analysis.
- Provide a baseline for future gap analyses.

## Step 10: Conduct a Hardware and Software Inventory

Conducting a hardware and software inventory is vital. The inventory not only allows the enterprise to confirm its hardware and software assets, making sure that nothing is missing but can help determine whether or not the enterprise's systems are configured according to asset management plans.

## Step 11: Review All Information Security Classifications

Because all information assets are not critical, it is important to ensure that security efforts are commensurate with the value of the information being protected. In some cases, organizations categorize their information assets according to relative asset value and sensitivity, by applying such terms as:

- Unclassified.
- Classified.
- Confidential.
- Restricted Use.
- Limited Availability.
- Secret.
- Top Secret.

For businesses that use such categorization schemes, answer the following questions:

- Is the classification scheme employed on an enterprise-wide basis? If not, why?
- Is critical information properly classified? Check some common information types, such as financial data, personnel records, customer information, and research and development data.
- Are critical information assets marked as critical? In other words, are terms such as classified or confidential attached to each critical asset?
- Are secured information assets consistent with their classifications?
- Are the graduated security controls adequate to protect the most sensitive assets?

## Step 12: Review All Information Access Controls

By one estimate, over 80 percent of all security breaches are initiated by individuals inside the organization, or by persons who have left the organization under unhappy circumstances. Some employees have grievances, even if they have not left the company, and many also have access to critical systems. When the two converge, the effects can be deadly.

The best way to mitigate the risk is to ensure that employee access to critical or sensitive information is strictly controlled. To help evaluate such safeguards, determine the following:

- Are access privileges granted on a need to know basis? If not, how are they allocated?
- Are employees required to sign non-disclosure agreements?
- Are passwords and other logical access controls routinely changed, especially after employees leave?
- Are the user accounts of terminated employees suspended?
- Are inactive or dormant accounts suspended?

### Step 13: Examine the System Maintenance Logs

Determine if vendor security patches are being applied in a timely fashion. Patches for the client devices as well as the server must be installed to fully protect the network. Most office infections come as a result of not applying patches in time to stop attacks and viruses.

### Step 14: Examine the System Software Settings

Determine if any unnecessary options are enabled. Consider, for example, that four days after Microsoft's Windows XP shipped, a California firm, eEye Digital Security, discovered a gaping hole in the operating system's Universal Plug and Play service; a hole that would allow a hacker to literally take control of another person's PC. Enabled by default in Windows XP, Universal Plug and Play, or UPnP, is designed primarily to help consumers link their PCs with other home appliances. While Microsoft produced a patch to remedy the problem, corporate IT departments were overwhelmed by the number of security patches Microsoft issues each month. In most months, Microsoft releases multiple bulletins to repair multiple vulnerabilities. In a number of instances, Microsoft has had to issue patches for the patches, or to re-release a patch, which caused problems in the enterprise environment.

Despite the work involved and the threat of installing flawed fixes, it is not an option for an enterprise not to install the patches as they become available. Microsoft is not the only software and system vendor experiencing these problems as almost all major software programs experience similar situations, and, the more popular the program, the more attention it draws from hackers.

One way for organizations to determine if there are problems with the various patches (i.e., the patch will not install, the patch is infected, flaws exist in the patch) is to install the patches in a test environment on individual systems before installing them on the actual corporate network. This process, alone, could save an enterprise an enormous amount of time, resources, and money.

Check all clients on a regular basis to determine if rogue software has been installed. Many computer systems and networks are compromised when unapproved software is installed by users. This rogue software is often full of bugs, can be used by hackers to install backdoors to systems, and can be programmed to act as bots in a hacker's botnet.

### Step 15: Verify the System Backup Procedures

While normally discussed within the context of business continuity, there is no process more fundamental to the interests of information security than backup and recovery. If information is lost or destroyed as the result of a security breach, all or part of that information can be restored from off-site media. As a function of the gap analysis, organizations should determine the following:

- Is electronic data being backed up on a regular basis?
- Is the backup data being stored in a secure offsite location?
- Considering that offsite data can deteriorate over time, what controls are in place to ensure its continued viability?

## Step 16: Interview Employees, Customers, and Selected Partners

Despite a business' best laid plans, there is often a wide gap between a system's intended use and its actual use. To measure the level of compliance with access and other security controls, interview the users on a confidential basis to ensure cooperation and candor and then try to determine the following:

- Has the importance and need for security been explained to employees?
- Are employees aware of the latest security policies, practices, protocols, and procedures?
- Do employees feel these procedures interfere with their work?
- Do employees attempt to circumvent any of these inconvenient procedures? Are they successful in doing so?
- Which procedures, if any, would employees retain, and which procedures, if any, would they eliminate?
- What would employees do if they had the responsibility for administering security?
- Are customers confident with organizational security when dealing with the company via Web, email, or other means?
- Have customers had problems with security?
- Do partners understand the security procedures when dealing with the organization?
- Are any policies not being followed by the organization in dealing with partners?
- Are any policies in need of update or alteration?

## Step 17: Evaluate Current Security Practices

Determine the efficacy of current security practices by comparing the conduct of those practices against established enterprise norms and generally accepted security principles. For example, most enterprises require that corporate PCs be equipped with anti-virus software. To assess compliance with this practice, ask the following:

- Do all PCs have anti-virus protection?
- Are these anti-virus packages updated as soon as vendor maintenance patches are released?

## Step 18: Document All Findings and Recommendations

At the conclusion of the gap analysis, it is vital to document (in detail) all findings and recommendations.

## Step 19: Develop a Remediation Plan

While not technically a part of the gap analysis, it is a good practice to develop a plan to plug the holes the gap analysis discovered. In developing a plan, schedule activities according to the severity of the exposures, with high-risk items earning first attention.

## Step 20: Schedule the Next Gap Analysis

Security planning is not a one-time-only event. Because the enterprise environment is subject to constant change, and new security threats arise on a daily basis, the shelf life of a security gap analysis is relatively short. A new gap analysis should be conducted every three to six months or more frequently if enterprise resources can support it.<sup>1</sup>

## References

[return to [top](#) of this report]

<sup>1</sup> "Conducting an Information Security Gap Analysis." YouSigma.com. 2008.

## Web Links

[return to [top](#) of this report]

International Organization for Standardization: <http://www.iso.org/>

ISO 17999 Gap Analysis: <http://documents.iss.net/literature/PS/ISOGapAnalysisDataSheet.pdf>

ISO 27001 Online: <http://www.iso27001security.com/>

ISACA: <http://www.isaca.org/>

ISACA COBIT: <http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx>

National Institute of Standards and Technology: <http://csrc.nist.gov/publications/PubsSPs.html>

## About the Author

[return to [top](#) of this report]

Rochelle Shaw is a Web designer and freelance author who has been tracking high technology for nearly 30 years as a writer, editor, and industry analyst. She is a frequent contributor to Faulkner Information Services.

[return to [top](#) of this report]