

STRATEGY & PLANNING

Info-Tech Advisor Premium - Strategize



About this research note:

Strategy & Planning notes define the critical decisions and actions surrounding successful adoption of a specific technology, tool, or process.

Top-Down Planning for Effective IT Security

Publish Date: March 12, 2008

Many enterprises complicate business-critical application security by failing to identify and apply suitable end-to-end security measures on a per application basis. IT executives should consider using a top-down approach to security based on information derived from corporate security policy, business application importance, and potential liability.

INFO~TECH
research group

Passionate About Research.

Driven By Results.

www.infotech.com

© 1998-2008 Info-Tech Research Group



Executive Summary

Numerous enterprises have a corporate security policy, but it is not always referenced when IT selects end-to-end business application security measures. The application's overall importance is often overlooked as the IT staff focus on more technical concerns. Enterprises should consider the following recommendations to ensure appropriate security measures are selected and implemented.

- » Ensure IT complies with corporate security policy direction.
- » Establish the application's security based on its corporate importance.
- » Review the impact of a security breach with executives and legal counsel.

Effective business application security complies with corporate security policy, takes into account the application's importance, and considers any potential liability resulting from a security breach.



Strategy Point

A bottom-up security approach that focuses on piecemeal, component security instead of application requirements, corporate security policy, and potential liability will likely fail to provide adequate protection. It can also result in a complex, expensive security infrastructure that is difficult to administer, manage, and scale.

Conversely, a top-down security approach addresses the complete end-to-end delivery path, including user environments and the transport network – plus it complies with corporate security policy.

Key Considerations

A bottom-up security strategy works well for many small enterprises. However, it is quite a different story for mid to large-sized companies with a wide variety of business applications and a diverse group of user environments. Ensuring appropriate security measures are utilized across the complete delivery path for all business-critical applications is not easy. However, the following top-down security recommendations can help most enterprises identify, classify, and protect their most important business applications.

IT Compliance with Corporate Security Policy Direction

Trying to implement application security without a well-crafted corporate security policy is injudicious. Although many IT organizations have their own standards for security, a corporate policy is still required to provide guidance in the areas of organizational roles, business application value, and overall security direction. The corporate policy must identify those applications considered as business-critical to enable IT to select and install suitable end-to-end security measures.

Some of the major items an enterprise corporate security policy should address are as follows:

- » **Information asset descriptions and estimated corporate value.** Identify and classify business application importance as low, medium, or high value. Do not make the classification process more difficult than it has to be. For example, most revenue-generating applications are placed in the high value category. These applications demand the highest possible levels of security across the entire delivery path. However, the security budget must be compatible with these needs.
- » **Minimum security requirements for local and remote users.** Identify the baseline requirements for local and remote access. For example, the policy may state that the baseline security for remote users is an eight digit alpha/numeric password that must be changed monthly. In other cases, a two-factor user authentication may be the minimum for remote access.



- » **Responsibilities for planning, testing, and implementing security.** The roles of any CSO, the IT organization, and any internal or external security audit groups must be clearly defined to minimize confusion and identify task ownership.
- » **Security breach policy including directives and actions.** Defines the actions that must be taken in the event of a breach. For example, if a high value application is breached, corporate policy may require the immediate notification of the executive team, law enforcement, and legal counsel. In addition, IT may be required to shut down the application until the breach is eliminated.
- » **Employee compliance, education, and training responsibilities.** Focus on specific employee responsibilities, and education/training requirements – especially for new employees and teleworkers. Identify the organization responsible for providing the training.
- » **A security code of ethics.** Describes what is expected of all executives, employees, and business partners, including penalties for non-compliance and/or criminal activity. Also, identifies the responsible party to contact in the event of any security issue or question.

Application Security based on Corporate Importance

Critical applications must be identified and secured first because they require the strongest layered security solutions possible. Enterprises utilize various layered solutions to provide end-to-end security for high-value applications including PKI, two-factor user authentication, data encryption, and various intrusion detection systems.

Typically, enterprises utilize several different criteria to determine a business application's category of importance.

- » **Revenue generation capability.** The highest revenue generating and/or the greatest liability applications must be identified and protected first. It is essential that the executive team and business executives identify these applications.
- » **Daily operational impact.** Applications such as order entry, e-mail, HR services, etc. must be reviewed to determine their enterprise importance. Based on their final classification, the appropriate security measures should be identified and applied.
- » **Business unit impact.** Although some of these applications may not be significant revenue generators, they may provide critical support services such as inventory management, CRM, order fulfillment, etc.



- » **Business partner impact.** Business applications that support third-party relationships must be reviewed from a financial and liability perspective. In addition, if there is an SLA, it must clearly define limits on the enterprise's risk exposure in the event of a breach.
- » **Potential liability.** Group business applications into a low, high, and medium risk category. Next, begin the liability analysis by addressing all concerns from the high risk application category. Low value applications should be addressed last.

Review Impact of a Security Breach with Executives and Legal Counsel

IT executives must take the lead because senior executives and legal counsel must first understand the purpose of the application and the user environment it supports – at least those applications of high value. Once understood, the potential revenue loss or liability aspects of a security breach can be discussed.

Loss of revenue. Loss estimates for a security disruption or breach vary from a few dollars per minute to thousands of dollars per minute, depending upon the application. Identifying exact dollar figures is not important, but identifying those applications that have major revenue impact on the corporation is essential. For example, a security breach to a Web-based order fulfillment application could generate, in just minutes, a major revenue loss in comparison to a longer duration disruption in a corporate e-mail system. When potential revenue loss or liability is high, the cost and complexity for the appropriate security solutions will increase substantially.

Liability costs. Liability must figure prominently in corporate security strategy because of its potentially crushing financial impact. Enterprises are forced to continue to comply with various, and in some cases, vague industry and government directives and regulations. Unfortunately, failure to comply with these murky directives and regulations could open the door to a corporate liability lawsuit and/or fine.

Furthermore, those enterprises that provide third-party IT services to other corporations and/or business partners must ensure they are fully protected if an unintended security breach occurs. Although there may be some degree of liability, legal counsel must ensure the impact is minimal and not enterprise crippling.

Business partners and third-party companies can also initiate a damaging liability lawsuit against a company that is contractually providing IT services if a security breach occurs. Some of these lawsuits, whether adjudicated or not, seek damages in the hundreds-of-thousands of dollars. Legal counsel should be consulted to ensure all service contracts for providing third-party IT services address the liability risk issue.



Recommendations

Top-down planning for business application security involves the executive team in crafting a corporate security policy that steers enterprise security direction. IT must then implement the end-to-end security solutions required. The following recommendations can help ensure the top-down planning process is successful.

1. **Review corporate security policy directives.** IT executives should spearhead this activity. The executive team and IT should review corporate security directives to verify if they are outdated, ambiguous, or require new additions. For more information on the implementation of an enterprise security policy, refer to the ITA Premium research note, "[Four Steps for Implementing a Security Policy](#)."
2. **Review business application importance categories.** Start the review by focusing on high-value applications and determine if anything has changed that requires a security reclassification. Do this on a semi-annual basis.
3. **Review/update employee education and compliance requirements.** A security-wise workforce makes things easier for IT and improves overall security. An employee security compliance policy must be updated and disseminated to the workforce as required. Consider placing employee security policies on the intranet.
4. **Identify and review application liability concerns.** This moving target requires constant vigilance – especially when providing IT services to outside companies. Pay special attention to any contractual requirements proposed by business partners or outside clients in this area.
5. **Compare top-down security requirements against any bottom-up initiatives.** Sometimes the technical team does not see the entire security picture unless they understand corporate security policy directives. IT executives must ensure the technical staff understands the total picture before implementing bottom-up solutions.

Bottom Line

Many enterprises complicate business-critical application security by failing to identify and apply suitable end-to-end security measures on a per application basis. IT executives should consider using a top-down approach to security based on information derived from corporate security policy, business application importance, and potential liability.



Info-Tech provides IT research and advice to more than 21,000 IT professionals worldwide. Our practical, actionable research is specifically designed to have a clear and direct impact on your organization.

Info-Tech's products and services help our clients work faster and more effectively. Our research improves the IT decision-making process, expedites critical IT projects, and helps our clients keep current – enabling them to achieve greater personal and corporate success.

[More About Info-Tech](#)

FREE IT Benchmarking!

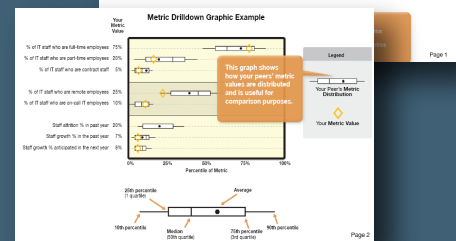
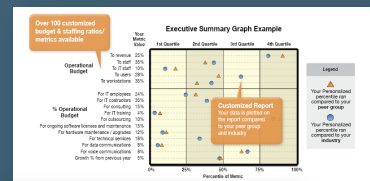
Under budget pressure? Need to justify every dollar you spend? Info-Tech's new program is designed to provide real world answers to your IT budget and staffing questions.

Start my custom survey

Begin your metrics program now with our survey and you'll receive:

- 8 Info-Tech Research reports on reducing your IT costs, rich with over **50 cost reduction strategies, 100 recommendations & 200 pieces of related research, tools & case studies**
- 2 detailed benchmark reports on budget and staffing, customized for your company
- Metrics compared to peer companies of similar size in your industry

There is no cost to participate, no sales person will call you and the survey takes only 15 minutes to complete.



Sample Benchmark Reports