

# Computer Security - It's Not Just About the "Bad Guys"

By Susan Farago and Ben Briggs, Tivoli Software-IBM Software Group

---

## I. Overview

It goes without saying that security has become a more prominent concern among businesses in recent times, yet many companies continue to view security as a passive "insurance policy"—and even a hindrance—in the deployment of e-business initiatives, rather than as a business-enabling asset. This perception has deep roots in the underlying belief that the primary role of security is to protect against technology threats, rather than to serve as a stimulus for greater cost efficiencies and new revenue streams that boost company growth.

Simply put, many companies focus on keeping the bad guys out rather than finding ways of letting the good guys—their most profitable customers—in to where they can more efficiently and effectively do business with the company.

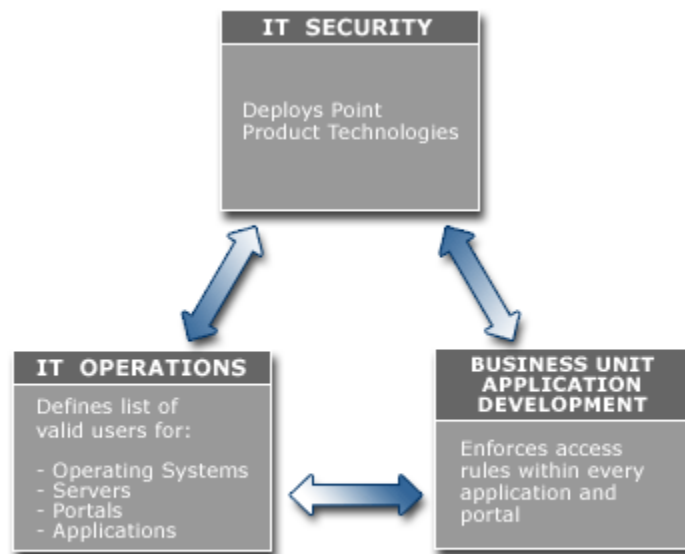
Additionally, who is managing the implementation and administration of these companies' security infrastructures and policies? Companies can no longer throw caution to the wind and have so called security "gurus" learn on critical business systems. As security practices are becoming more institutionalized, the demand for proven skills is increasing.

This article provides an overview of the key security issues and concerns in the marketplace today, outlines the need for experienced computer security experts in the four key areas for security management, and illustrates how companies such as IBM are using technical certifications to ensure the right skills meet companies' needs for secure business environments.

## II. The Security Opportunity versus the Security Liability

Historically, the security spotlight has been focused on keeping out intruders, hackers, and others without proper authorization through the use of sophisticated point products: firewalls, intrusion detection software, content filters—to protect corporate e-business infrastructures. But the real security opportunity lies in the more efficient development of advanced e-business initiatives and applications for new customer acquisition and corporate expansion. In short, security must come to be perceived as an asset, rather than as simply an insurance policy.

The challenge of creating an IT security infrastructure that acts as a business enabler—in addition to effectively keeping the bad guys out—can be seen by examining how information security policies are generally enforced today. The following diagram illustrates these challenges.



**FIGURE 1: The Current Organizational Challenge for Security**

- **IT security** - Focuses on securing the network infrastructure using a variety of point product technologies for protecting against a wide range of threats.
- **IT operations** - Works with the business units to define the list of valid users (customers, partners, and employees) of its IT resources (operating systems, servers, portals, applications, etc.)
- **Business unit application deployment** - Enforces the appropriate level of access for each user within each application and portal.

Most point network products do not support these critical tasks, so both IT operations and business unit application developers are left to manually implement security policies. Although this approach has been a widespread practice for some time, it causes three fundamental business problems for IT operations, as seen in Figure 2.



**FIGURE 2 The High Cost of the Current Organizational Paradigm**

- **Long cycle times for getting users online and productive.** As administrators are forced to manually obtain approvals, provision resources, and create multiple accounts for each user, it can take a long time to get a new user online.
- **High costs for administering users.** Having multiple accounts for each user can lead to a high number of help desk inquiries for forgotten passwords and other common administrative tasks.
- **High total cost of ownership for user management.** Security policies don't typically change substantially over time, but users' relationships to the policy often do. For example, the relationship with a partner might change based on a new partnership agreement, or a new entry-level customer might evolve into a high-margin customer over time. These changes must be reflected across a firm's e-business infrastructure, but because each application, portal, and server is typically populated with their own set of user definitions and security access rules, each relationship change must be encoded manually within each customized security model. This generates a higher than necessary management cost that can grow proportionally with the number of deployed resources.

### III. Four Key Areas for Security Management

Computer security is no longer a single component within a business environment managed by ad-hoc processes. It has become a multi-faceted arena that encompasses four key areas for computer security: access management, identity management, threat management, and privacy management.

Many software companies offering security solutions have developed applications specific to each of these key areas. For example, IBM offers a complete security solution that is comprised of these critical security areas that includes: IBM Tivoli Access Manager, IBM Tivoli Identity Manager, IBM Tivoli Risk and Intrusion Manager, and IBM Tivoli Privacy Manager.



**FIGURE 4: Lowering the Costs of Managing a Secure e-Business**

#### IV. Need for Experienced Security Experts

Given the high costs of the current organizational paradigm, and the specific areas that encompass computer security, there is a rising demand for experienced security experts. These experts understand these complexities and can help companies realize the significant benefits that advanced security solutions can bring to a company implementing an e-business strategy.

Companies cannot afford “trial and error” security implementations by people who have minimal computer security experience. This need is putting pressure on technical professionals to prove their level of expertise by maintaining portfolios that detail their experience, education, and certifications.

#### V. Need for Objective Validation of Skills

Highly-specialized professions, such as computer security, require an individual to have knowledge and skills that cannot be verified by the possession of a college degree alone. Keeping a resume or bio-data current is essential for any consultant but recording the months of time spent at a given client’s site working with a laundry list of products is not enough. This is why vendor product certifications are important. These certifications are objective measures of the ability to perform a specific job using a specific product. *When combined with experience and education*, certifications form an excellent indicator of real ability.

Most companies in the IT industry offer role-based product certifications. These certifications do not simply test knowledge of a product’s features and functions but are designed specifically to test the ability to perform a specific job with that product.

Common job roles include:

- User – use the product to do what the product was designed to do
- Administrator – keep the system running, fix problems and perform customizations so others can use it effectively
- Deployment or Engineer – (this category is broad) plan, design, install, configure, troubleshoot and integrate with existing systems
- Architect – perform high-level design and integration

- Trainer – teach another person how to perform one of the above roles

Vendor product certifications may show an employer or prospective client that a consultant has expertise with a specific group of products but these certifications do not demonstrate the fundamental domain knowledge of the computer security profession. The new vendor-neutral CompTIA Security+ certification fills this need by validating fundamental security skills and knowledge.

CompTIA partnered with many leading computer security consultants and vendors such as: IBM Tivoli Software, Verisign, Microsoft, and Sun Microsystems to define baseline skills required in the computer security industry. Gaining this certification attests to basic understanding of computer security fundamentals.

Many of the best security software vendors already have their own certifications and are incorporating the CompTIA Security+ certification into their programs. This certification will identify individuals who are well-rounded and can provide services to their employers and customers that go beyond the ability to deploy the vendor's products alone.

## **VI. IBM Tivoli's Approach to Security Certification**

IBM Tivoli Software offers a variety of deployment-based product certifications across the four main pillars of their business, including Security. In order to offer a higher level IBM Tivoli Security certification, candidates will be required to pass multiple IBM Tivoli specific exams in addition to the CompTIA Security+ exam.

When it is announced later this year (i.e. some details may change), this certification will require candidates to earn the following:

- **CompTIA Security+** – fundamental knowledge, skill and vocabulary of the computer security industry (required)
- **Access Management** – authorization solutions for the enterprise – (one certification from this category is required)
- **Identity Management** – policy based user and identity management (one certification from this category is required)
- **Threat Management** – centrally manage attacks, threats and exposures (one elective certification is required and may be selected from this category)
- **Privacy Management** – dynamically define, enforce and manage enterprise privacy policies (one elective certification is required and may be selected from this category)

We believe that a candidate, whether an IBM employee, IBM business partner or independent consultant who demonstrates the skills contained in these certifications will have an excellent understanding of the computer security profession and will provide their employers and clients with significant benefits.

## **VII. So What Does this Mean to You?**

If you are a technical computer security expert, it should be apparent that computer security is a large and diverse field that is rapidly evolving. The transition from infancy to adolescence is accompanied by an effort within the industry to define a "fundamental" core of knowledge and adopt a common language. With all the press computer security has received in the past year, many people will be eager to jump in and start handing out business cards declaring that they

are security gurus. The best way to differentiate yourself from this crowd will be to carefully combine education, experience and certification by respected organizations.

If you are manager of IT resources or a CIO in need of computer security advice, look for documented skills in the people you hire. Look for people who have solid backgrounds in computer security with significant and varied engagement experience. It is equally important to look for people who have the specific education, hands-on experience and certifications working with the products you own or plan to deploy. Certification programs spend a significant amount of time and effort developing certifications that effectively differentiate between those who have the skills to work effectively with their product from those who do not. Take advantage of this and, where appropriate, request certified individuals when hiring or contracting security experts.

Susan Farago and Ben Briggs manage the Tivoli Professional Certification Program for Tivoli Software, IBM Software Group. They can be reached at [tivcert@us.ibm.com](mailto:tivcert@us.ibm.com).

For more details around Tivoli Professional Certification, visit <http://www.tivoli.com/services/certification>

For more information, or to read the full IBM Security Products article (excerpts above), visit <http://www.tivoli.com/news/features/security/>

For more information about the CompTIA Security+ certification, visit <http://www.comptia.org/certification/securityplus/index.htm>