



[www.computer.org/itpro](http://www.computer.org/itpro)

# CIO Corner

*Tom Costello*

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

IEEE  computer society

© 2011 IEEE. Reprinted with permission from IT Professional. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

For more information, please see [www.ieee.org/web/publications/rights/index.html](http://www.ieee.org/web/publications/rights/index.html).



*What should you do to protect your company's information? And what must you do to follow the law?*

**Francis X. Taney Jr. and Thomas Costello**

# Securing the Whole Enterprise: Business and Legal Issues

Information security has become a hot-button issue for businesses of all sizes. And while these businesses tend to give the topic a lot of lip service, a look in the newspapers will show that even substantial enterprises aren't immune to security breaches. Achieving good information security isn't easy. And all too often, enterprises lack a clear understanding of what to do if they do discover a flaw or breach in their information security.

The consequences of failing to address information security are frequently disruptive and can even be catastrophic. Imagine, for example, that a contractor, employee, or visitor installs and uses unlicensed software on one of your desktops. Or imagine an employee spots someone viewing an improper photo and reports it to a supervisor. For either case, do you know what you are required to do? Does the supervisor know her legal obligation? What about the human resources person who gets brought in? What about the IT network administrator who starts checking out the machine or logs? Do you have to call the police? What should you prepare before they arrive? Does your enterprise have a strategy for dealing with the possibility of the police coming into your data center,

strapping yellow tape around the rack, and ripping out one of your servers?

If you think these are extreme or unlikely examples, consider the case of Ernie Ball, the world's lead-

ing maker of premium guitar strings. In 2000, the Business Software Alliance (BSA), having received reports of unlicensed Microsoft software running in Ball's environment, raided the company's corporate headquarters with armed marshals and shut down the facility. Ball eventually settled, paying \$65,000 in damages and another \$35,000 in legal fees, but not before making the nightly news. And the company ended up in one of the BSA's regional advertising campaigns encouraging compliance with software licensing laws (see Matt Berger, "Guitar Maker Plays a Linux Tune," <http://infoworld.com/articles/hn/xml/02/11/27/021127hnerniball.html?s=IDGNS>; and David Becker, "Rockin On Without Microsoft," [http://news.com.com/2008-1082\\_3-5065859.html?tag=lh](http://news.com.com/2008-1082_3-5065859.html?tag=lh)). This is but one example of what can befall an enterprise that fails to address information security issues. But simply making sure that all your software is licensed is just one aspect of a very complicated task. To conquer the problem, businesses must first understand it. Let's first take a look at some factors contributing to the difficulty of maintaining information security in an enterprise. Then we'll offer an approach to addressing the problem.

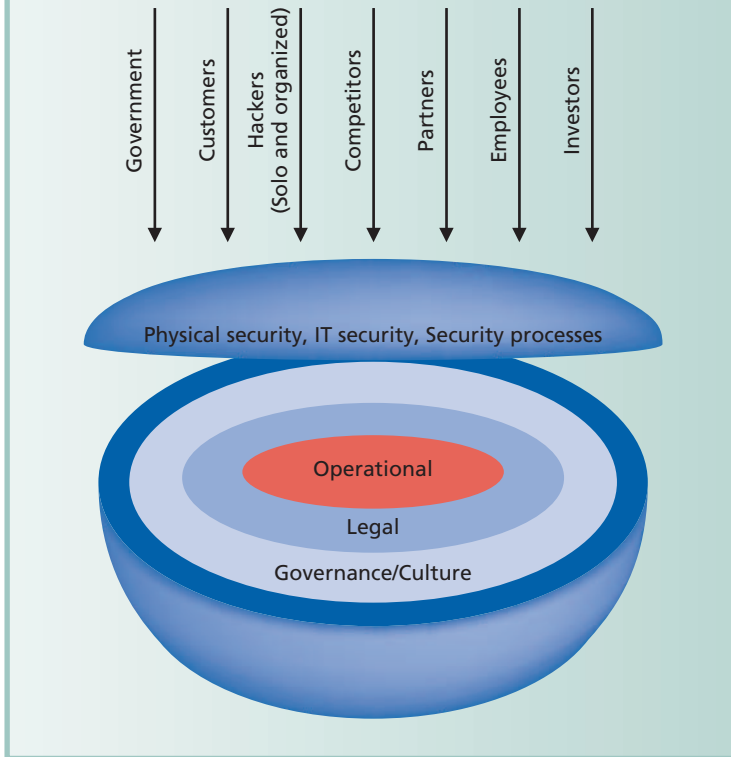
## THE PROBLEM

As Figure 1 illustrates, to secure the whole enterprise, you must balance and address the competing needs and pressures created by the legal, operational, technical, cultural, and behavioral forces acting on your enterprise.

### Inside

#### Know the Laws

**Figure 1. Securing the whole enterprise means balancing a host of competing influences.**



## So Much to Protect

With increasing frequency in our postindustrial economy, an enterprise's value resides in its information. This information might consist of financial and tax records, customer or client data, and vendor or business partner data, not to mention trade secrets and proprietary business information. Enterprises must ensure that this information remains intact, authentic, uncorrupted, and inaccessible to those who have no right to it. In addition, to ensure the information's availability, authenticity, integrity, and confidentiality, enterprises must also protect the information systems and the components that house the information. Thus, securing information usually means securing the whole enterprise.

## So Much to Protect Against

The range of threats to information security is wide and continually expanding. Threats can emanate from internal or external sources, from human and natural factors, from intentional or inadvertent conduct, and from inbound or outbound communications. Threats to the enterprise could be as sinister as corporate espionage by competitors; or they might be as mundane as employees utilizing corporate assets, inappropriately or illegally, for personal reasons. Of

course, threats vary widely in terms of the level of technology involved.

Enterprises also vary in the level of sophistication they bring to protecting themselves against these threats. Many currently address at least some of these threats through an array of hardware and software, such as secure hardware and intrusion detection software. Many enterprises use software applications that provide various levels of password protection for users, as well as application security to protect the data used by the application. Almost all enterprises protect the environment by checking inbound e-mail for viruses, and some endeavor to ensure user device compliance with the most current threat files. More sophisticated organizations incorporate tools that monitor and control activity on user devices and scan for applications that could expose the enterprise.

Unfortunately, enterprises often resort to "cherry-picking" in the way they structure their security approaches—that is, solutions target only the most obvious, well-documented threats. Enormous gaps might exist for items that are as obvious as air—all around us but not visible. For example, few organizations have any method for tracking, capturing, or restricting instant messaging. Fewer still scan for the presence of steganography applications, which allow users to embed material into something as simple as a graphic file. As long as the sender and receiver

use the same steganography application and encryption key, they can hide sensitive electronic information and ship it through corporate e-mail completely unnoticed.

Many enterprises have also failed to plan for and protect against "social engineering." The Great Wall of China, a famed example of a highly ambitious protection program, suffered three socially engineered breaches in the first full year following its completion: intruders talked or bribed their way through the gates. While our physical borders' security might have improved in the two millennia since the Wall was built, other aspects of our modern world are even more prone to social engineering. E-communication makes it easy to counterfeit valid roles. Intruders can easily gather incredible amounts of information and then phone or e-mail their way into the average enterprise.

## Shifting and Unclear Legal Obligations

Who or what defines "compliance" for your enterprise? Your level of internal control over the definition depends on your industry. Assuming you're a US-based, publicly traded organization strictly focused on US delivery, you might face a great many regulatory requirements. Sarbanes-Oxley is one of the most well-known; many other state and federal laws might apply to your enterprise. (The

“Know the Laws” sidebar lists Web sites that enumerate some of these.) Your particular industry might also have various self-imposed guidelines or standards of care that affect your security needs.

US information security law may currently be in flux, but it is also steadily growing more teeth, developing a standard of care. The Federal Trade Commission (FTC) and other enforcement agencies recognize that perfect information security does not exist; typically, these agencies haven’t required enterprises to adopt security measures that put them at a disadvantage vis-à-vis competitors. However, in enforcement actions and civil proceedings—or when something goes wrong—an enforcement agency, court, or jury might not be so generous in determining whether your enterprise acted diligently to prevent the problem. The FTC in particular has demonstrated a willingness to impose sanctions on companies whose security measures did not meet current standards, even in the absence of a security breach.

Of course, your enterprise might not be US based. Many of today’s smaller enterprises are visible to the global economy strictly through their Web presence, and many transact business internationally more substantially. These enterprises are potentially subject to an array of foreign regulations imposed by individual governments and regional entities such as the European Union. In some circumstances, evolving foreign requirements conflict with US law. If your organization offshores its IT services or IT security, you have additional legal and logistical risks and problems to manage.

### Financial and Operational Constraints

No enterprise is free from financial constraints. In considering how much to spend on information security, an enterprise’s leadership must balance the cost against the problem’s perceived impact. There is little financial margin for error.

Unfortunately, many enterprises addressing information security issues focus intensely on getting the right gadgets, but then neglect to invest in the necessary education, consulting, and support to properly install, configure, and update these devices. A large one-shot expenditure, however, isn’t a viable solution to the information security problem, especially in light of the limited financial resources

## Know the Laws

### Selected Information Security Laws

- **Fair Credit Reporting Act and Fair and Accurate Credit Transactions (FACT) Act**, <http://www.ftc.gov/os/statutes/fcrajump.htm>
- **Health Insurance Portability and Accountability Act (HIPAA)**, <http://www.hhs.gov/ocr/hipaa>
- **Sarbanes-Oxley Act**, <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>

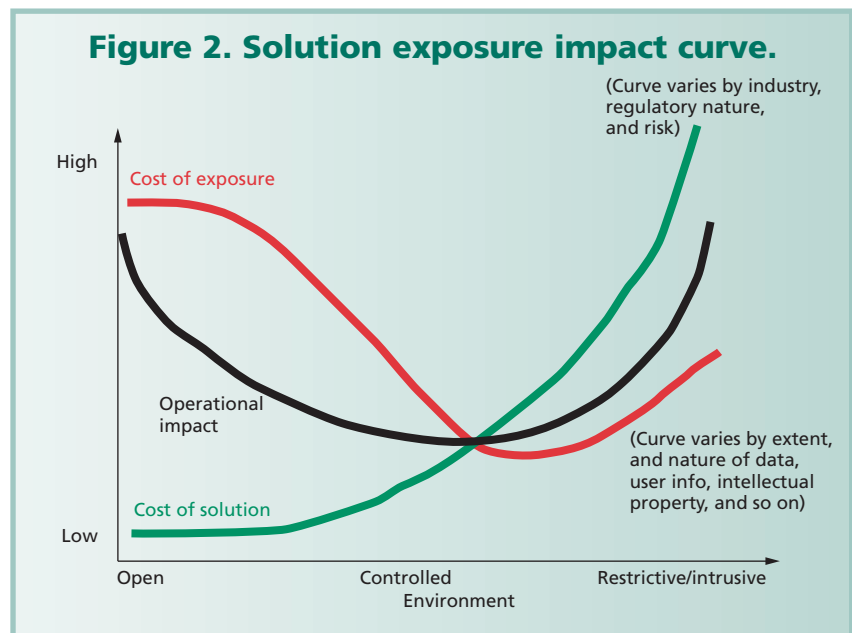
### Sites Listing and Explaining Regulations

- **The Center for Regulatory Effectiveness**, <http://www.thecre.com/fedlaw/legal8.htm>
- **CSO Online**, <http://www.csoonline.com/research/compliance>

typically available. Indeed, this approach can often create significant “security seams” within an enterprise because it lacks coordination and overview, and the upgrades and solutions will very quickly lag behind the problem.

In addition, an enterprise’s operational and information security needs might conflict. Executives must balance a wide array of parameters when constructing or authorizing an enterprise security model: privacy versus risk and surety; access versus security; security versus operational capability; and ultimately, cost versus risk (both exposure and liability). The solution exposure impact curve in Figure 2 depicts these various forces.

**Figure 2. Solution exposure impact curve.**



Ultimately, though, it isn't practical to keep the sea from the shore. By this, we mean that the hypothetically perfect set of security measures—that keeps everything out (or in)—would disrupt business. Happily, you'll find that “perfectly good” costs a lot less than “perfect.”

### Limited Support and Attention from Decision Makers

Depending on your enterprise's structure and financial resources, and on the cost of implementing appropriate security measures, buy-in from senior management might not be enough to make it happen; board or investor approval might be necessary. But few board members want to hear the details of how you configured your routers; even fewer want to hear about it during the board meeting. Further, the risk profile your investors and board want to create might not jibe with their attitude toward spending. Senior management keeps what it considers the appropriate projects portfolio based on available budget; security might not be even near the top of that list.

### Change

Security would be a difficult enough problem if your enterprise and its surrounding environment were static. Both are subject to change, however, and the rate of change appears to be accelerating. Changes in operational and security software, hardware, and access methods often create security holes and gaps. Even upgrades, improvements, and business-centered changes can expose unforeseen weaknesses in a previously stable environment. Attempts

to fix or secure a new tool or application without regard to the broader security context might result in unexpected problems.

### Complacency

Even the most conscientious, skilled, and talented security team is susceptible to “smelling its own exhaust.” Complacency, or an ingrown, unchanging perspective on security threats and solutions

can prohibit or delay an enterprise's ability to deal with real threats.

**Even the most conscientious, skilled, and talented security team is susceptible to “smelling its own exhaust.”**

Join the IEEE Computer Society  
online at



[www.computer.org/join/](http://www.computer.org/join/)

Complete the online application and get

- immediate online access to **Computer**
- a free e-mail alias — **you@computer.org**
- free access to 100 online books on technology topics
- free access to more than 100 distance learning course titles
- access to the IEEE Computer Society Digital Library for only \$118

Read about all the benefits of joining the Society at

[www.computer.org/join/benefits.htm](http://www.computer.org/join/benefits.htm)

## THE SOLUTION

It's difficult to see an effective information security plan emerging from the swirl of these competing forces. To achieve this, start with creating an enterprise-wide understanding of what's at stake and then follow a straightforward plan.

### Step 1: Determine Your Enterprise's Current Position

The developing legal standard for *information security* requires enterprises to perform an initial risk assessment of their current information security situation. The goals of the assessment are to

1. identify the material internal and external security risks, and the potential damage from those risks, in light of the sensitivity of the information the enterprise needs to protect;
2. match the current security measures with those risks; and
3. assess the sufficiency of the current security for addressing those risks, in light of the nature and scope of the enterprise's operations and the sensitivity of the information.

The initial risk assessment should address all relevant areas of operation, encompass both information and systems, and be conducted by personnel with requisite expertise and credentials.

Aside from being the legal standard, this risk assessment makes good business sense. Because information security problems can significantly affect an enterprise, senior management should have access to a sophisticated analysis of the enterprise's security program. This access should be informed by an appropriately broad array of informational and educational resources, including best practices within and outside an enterprise's industry sector.

Senior management must also understand the costs, benefits, and risks involved with the enterprise's current security measures, as well as with failing to devote appropriate resources to implementing appropriate security measures.

### Step 2: Determine Where Your Enterprise Should Be

Although an enterprise can quickly reduce exposure to some risks through relatively small expenditures, at some point a substantial investment might be required. As Figure 2 shows, the optimal balance point of risk, security, and cost depends on the nature of the enterprise's business, regulatory requirements, and other factors. Few enterprises will find an actual triple break-even point (where the three curves intersect); instead, most will find a triangular safe area between the curves. A good risk assessment can give senior management the information to reach the safe area, or even the optimal point.

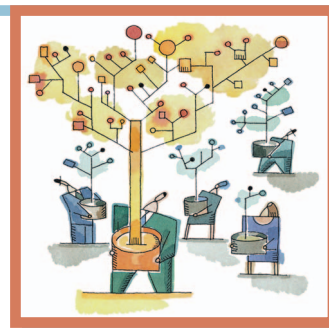
After performing the risk assessment, an enterprise

should create a comprehensive information security program. The program must be enterprise-wide; it must be in writing; and it must include the appropriate measures to address the risks apparent from the initial assessment. Along with technical measures, such as intrusion detection software, the plan must include administrative (procedural) and physical security measures.

Employee education and training, to prevent socially engineered attacks, are particularly important administrative security measures to include. The program should also require an enterprise to exercise due diligence in evaluating third-party vendors or consultants hired to provide security-related products or services, and it should further require that your enterprise obtain these third parties' agreement to follow appropriate information security procedures and measures in performing their services.

Your enterprise should appoint a person with the appropriate credentials and experience to administer the program. The FTC recently expressed approval of three particular credentials: Certified Information System Security Professional, Certified Information Systems Administrator, and the Global Information Assurance Certification. This is not, however, an exhaustive list of appropriate credentials.

As with the assessment, the legally required features of your plan dovetail with operational efficiency. While you can't assume that senior management will understand the



# JOIN A THINK TANK

**L**ooking for a community targeted to your area of expertise? IEEE Computer Society Technical Committees explore a variety of computing niches and provide forums for dialogue among peers. These groups influence our standards development and offer leading conferences in their fields.

Join a community that targets your discipline.

In our Technical Committees, you're in good company.

[www.computer.org/TCsignup/](http://www.computer.org/TCsignup/)

nuances and details of each component of a solid security regime, they must understand whether and how your plan addresses the breadth of potential breaches and threats.

### Step 3: Test and Monitor Your Enterprise's Progress

To be both operationally effective and legally compliant, your information security program should include measures for periodically testing and continually monitoring its effectiveness. Your enterprise should also document the occurrence and results of the testing and monitoring. This documentation serves a dual purpose: it lets your enterprise demonstrate that it acted responsibly in the event of a legal dispute or enforcement action; it also gives senior management valuable information about the effectiveness of the information security program.

In addition, your program should establish independent, third-party periodic performance audits of all people involved, including vendors and consultants. This will help prevent complacency or a narrow perspective from impairing the program's effectiveness.

### Step 4: See Step 1

Finally, an enterprise's information security program should require periodic reevaluation and adjustment in light of changes in relevant circumstances. Not only will reevaluation be an inevitability from a legal compliance standpoint, it will also help your enterprise avoid developing security openings that widen and escalate as employee turnover, time, and circumstances progress.

Enterprises are constantly challenged with new threats, while the array of tools, techniques, and requirements continue to rise to meet and defeat these invasions. It is easy for organizations to become myopic or complacent with their security approaches as they fund and implement security initiatives. Properly identifying your current capability and current threats and then creating a path of continuous improvement across the whole enterprise will yield the best results. Information security is not a milestone that an enterprise achieves once and for all; it is a state, subject to change, and maintaining it requires continuous vigilance and effort. ■

*Francis X. Taney Jr. is a shareholder of Buchanan Ingersoll PC where, as head of the IT Litigation Practice Group, he specializes in commercial litigation—including IT, anti-trust, IP, and construction litigation—as well as IT-related transactions. Contact him at [taneyfx@bipc.com](mailto:taneyfx@bipc.com).*

*Thomas Costello is the CEO of UpStreme, Inc., which specializes in addressing complex business and technology integration issues, including open source, enterprise information architectures, mergers and acquisitions, and advisory and interim CXO services. Contact him at [tcostello@upstreme.com](mailto:tcostello@upstreme.com).*

*For further information on this or any other computing topic, visit our Digital Library at <http://www.computer.org>*

## Evaluating the Performance of Software Engineering Professionals

By Lawrence Peters  
Software Consultants Int.

Surprisingly, the most common means of reviewing software engineering professionals actually have the effect of demotivating them and reducing their performance level. This ReadyNote advocates an alternative method for evaluating personnel based on the Balanced Scorecard. \$19  
[www.computer.org/ReadyNotes](http://www.computer.org/ReadyNotes)



# IEEE ReadyNotes



IEEE  
computer  
society  
60<sup>TH</sup> anniversary