



# IT Security Operational Maturity:

## Why You Need More Than Personal Heroism and Silver Bullets

By Ed Bassett, Vice President, Global Security Practice, CIBER, Inc.

### Abstract:

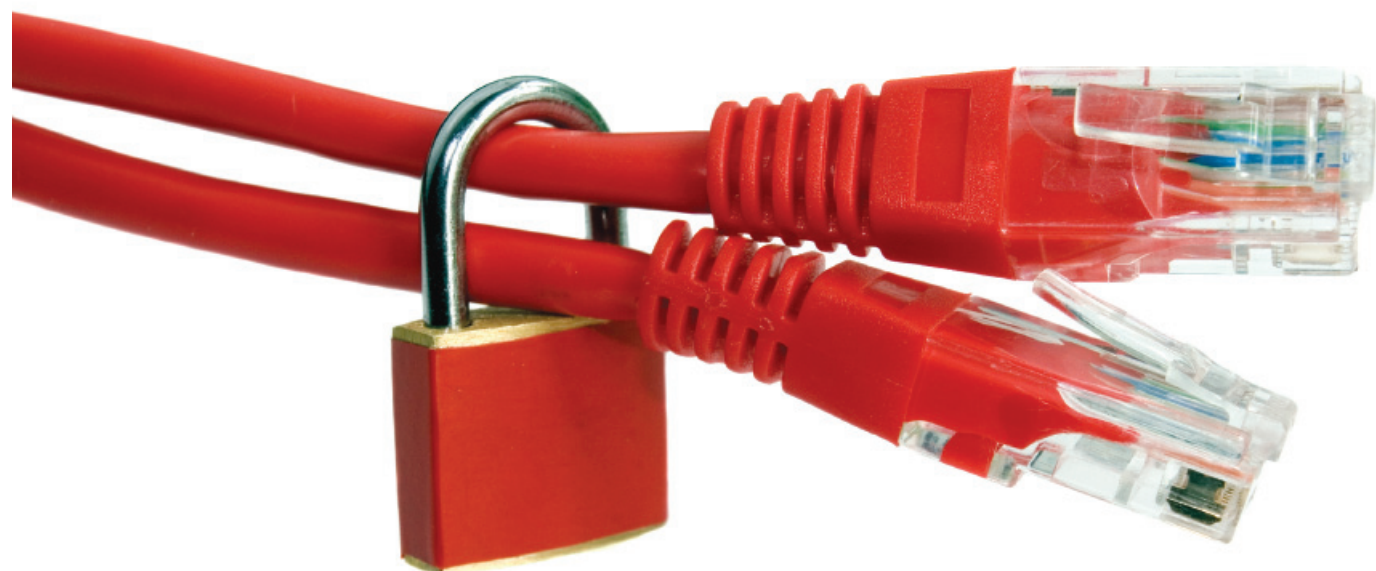
A leading analyst firm predicts that organizations' information technology (IT) security budgets will experience downward pressure in the next three to five years, from the 6% - 8% of overall IT budget that most organizations spend today to 3% - 5% of overall IT budget. Given that security incidents are on the rise and those with sinister motives continue to develop better methods for wreaking havoc, this may seem counterintuitive.

The reality is that most of you will be challenged to provide better protection against increasingly sophisticated threats—with a reduced security budget. Meeting this challenge will require new techniques that are more operationally mature.

This white paper illustrates the many business drivers shaping IT security, emerging risks, and the need to transform your security program into one that's operationally mature. After reading this white paper, you'll understand how to direct investments in your organization's IT security program to achieve security results that are consistent, reliable, effective, affordable, and auditable.

# New Business Drivers Are Changing the Direction of IT Security

Several business drivers are changing the IT security landscape. Until fairly recently only financial institutions, the military, and a few other organizations were even attempting to build comprehensive, mature security programs. Today this is no longer the case. Virtually every industry has been driven to take a more structured approach to security. There has been a dramatic fall-



off in the number of organizations that can afford to remain in what Gartner industry analysts call the “blissful ignorance” state. Today, any organization with sensitive data as part of their business model must be aware of security risks, and must manage them as an integral part of their business. Following are six business drivers that are changing the direction of IT security.

Database Breach Laws

Identity Theft Risk

Regulatory Compliance

Insurance Requirements

Heightened Consumer Expectations

Contractual Requirements



## #1: Database Breach Laws

Most states have enacted database breach laws that mandate disclosure of security incidents when personally identifiable information has been compromised. The intent of these laws is to alert consumers of a breach so they can take steps to protect their credit records and identities. Until these laws came to pass, it was fairly standard practice to keep such breaches quiet to avoid the attendant negative publicity. These laws do not require companies to provide better protection of consumer data. But the laws do motivate organizations to avoid breaches because the now-required disclosure of a breach can lead to a significant consumer backlash. In the most dramatic cases, large numbers of customers have fled to competitor companies because they no longer trust a business that has disclosed a major breach.

## #2: Identity Theft Risk

The risk of identity theft is no longer greatest from targeted attacks on individuals. Instead, large scale criminal operations have discovered that identity theft can be quite lucrative, providing a “raw material” that drives criminal operations and offers a safer alternative to drug trafficking. The security attackers that feed these criminal enterprises have found efficient, automated methods to probe vast numbers of IT systems for weaknesses.

The threat profile has moved from “amateur nuisance” to “well-equipped professional,” and any unprotected system is a potential target, regardless of industry, geography, or size.

## #3: Regulatory Compliance

Government regulations that mandate information security have been enacted in several industries, including healthcare, utilities, banking/finance, and government. Beyond industry-specific regulations, the database breach laws mentioned earlier, the Sarbanes-Oxley Act, and the Payment Card Industry Data Security Standard (PCI DSS) are also having an effect on a very large number of companies.

These regulations and industry standards create a specific mandate for certain security practices that companies must follow. Lack of compliance may lead to financial penalties and loss of business.

## #4: Insurance Requirements

More than a decade ago, Esther Dyson, a world-renowned commentator on digital technology, predicted that insurance requirements would be a significant factor in driving security decisions.

Just as your property insurance company will not insure you until you take steps to prevent and mitigate the risk of fire (e.g., installation of sprinkler systems, alarms, fire drills, etc.), insurance companies are starting to require that organizations demonstrate preventive IT security measures before insurance will be provided. This trend is expected to continue and become a mainstream insurance requirement in the next few years.

### #5: Heightened Consumer Expectations

Consumers are now highly aware of privacy and database breach laws, and are critical of companies that do not protect customers' data. At the extreme, consumers will "vote with their wallet" and move to competing companies if they believe a firm will not vigorously protect their sensitive information. This consumer pressure is difficult to quantify, but enough anecdotal evidence exists to demonstrate that this can be a deciding factor in corporate decisions about security protections.

### #6: Contractual Requirements

In the business-to-business arena, many large businesses are becoming more sophisticated about security and are requiring their vendors to demonstrate their security and pass audits to prove the effectiveness of their security controls. This increased oversight and more specific requirements are causing many companies—especially small- and medium-sized companies—to greatly increase their level of security.

---

**“Neither the firewall nor the subsequent new technologies have ultimately and finally solved the security problem.”**

---

# Evolving Risks— A Firewall Is Not Enough

The six business drivers described on the preceding pages are wielding more influence every day in determining the future strategy and operational maturity of organizations' IT security programs. In addition to this pressure, new emerging risks are also influencing the direction of IT security.

### Firewalls and Other Technologies

Technological solutions—such as firewalls—that address a significant class of threats have been heralded as nearly “silver bullet” solutions. For example, looking at the introduction of the commercial firewall, this then-new technology promised one low-cost device to protect scores of interior servers from the wild untamed Internet. At that time, the alternative approach was to harden each server individually—a costly and error-prone task at best.

The “fathers” of the firewall, Bill Cheswick and Steve Bellovin, at a large NSA-sponsored conference, expressed amazement at the standing-room-only crowd that gathered to hear their speech describing the firewall concept. Cheswick and Bellovin stated that, in a few years, everyone would have a firewall and the room would be empty. The expectation of many, given the threat at the time, was that the firewall would solve the problem of Internet attacks.

This cycle has been repeated over and over with each new security product touted as the perfect solution to whatever new attack has rendered previous solutions inadequate. The fact is that the rooms of people at the security conferences are still full because neither the firewall nor the subsequent new “silver bullet” technologies have ultimately and finally solved the security problem.

## Security Changes As Our Use of IT Changes

Why? Because new IT capabilities bring new security risks. With the introduction of Web 2.0 technologies, for example, we are seeing more direct access to back-end systems by remote users over the Internet. If this were just about transactions coming across the Internet, we could solve these challenges with firewalls and VPN appliances. But there is more to this story.

These new applications require access through the firewall—so we must open up a path for the transaction. The applications are making their own security decisions about who can access what information. This has resulted in development of new application-oriented attacks. In fact, a leading analyst firm states that 75% of hacks occur at the application level. So, if a firewall is your only method of protection, then you have to choose between blocking Web 2.0 access for your customers (and lose this channel for doing business with your customers), or risk a security breach at the application level.

### Discriminating Security

This means that security controls must be upgraded from first generation “blocking” controls to second generation “inspection” controls that can effectively discriminate between good and bad transactions. This includes security controls that must be **designed into** applications, as well as intrusion prevention and monitoring systems that are capable of handling application-level events.

# The Need for Operational Maturity

Within the realm of IT security, there are numerous security sub-categories, or topics, that must be addressed to effectively protect a system. In the earliest days of security, these included perhaps seven or eight categories, such as check fraud, wiretapping, piracy, and “backdoor” access to networks and applications.

However, since 2000, there has been a 300% expansion in the number of security topics that every meaningful security program must be prepared to address. Of the 312 unique security topics we have identified, many are complex enough to be worthy of their own dedicated staff, such as HIPAA Compliance, Forensic Analysis, or Academic “e-Cheating.”

Looking out on the security horizon, our analysis shows that by 2020, the number of unique security topics that a security program will need to address will likely expand to more than 1,500.

Clearly, IT security has become significantly more complex, and the previous security method of applying new security measures to each emerging threat is no longer cost-effective. The emergence of new security risks happens too fast, and the stakes of a breach are too high.

In addition, most security programs today have grown up in a piecemeal fashion and lack the programmatic structure needed to achieve operational maturity. For instance, many companies have an adequate assortment of security technology and in-house expertise, but often these technology purchases were made in response to an urgent security risk, the aftermath of a security incident, or as a result of an audit finding. These are valid reasons to deploy new security technology, but a series of such decisions does not generally result in an optimal security program. The typical result is a haphazard program that has gaps in some areas, redundant protections in other areas, and numerous operational inefficiencies.

The time has come for operationally mature security solutions that address multiple security risks with systemic fixes that permanently reduce risk.

### What is Operational Maturity?

Operational maturity, in the IT security context, refers to security programs that have some, or all, of the following characteristics:

1. The security program is **strategically planned and executed** to create consistent, effective, affordable, and auditable security across an organization.
2. The security program **uses modern analytical and modeling techniques** to evaluate security risks and implement the appropriate security controls.
3. The security program **anticipates and plans for the effective management of undesirable events**, such as a security attack or breach. Security failures **will** occur. Just as a mature storage solution gracefully handles the failure of a component hard drive, a mature security solution must gracefully handle security failures.
4. The security program **includes strategic use of IT to control risks**, and is integrated with other IT

systems to address large ranges of security risks (rather than one specific threat).

- The security program is **transparent** so auditors, customers, and organizational leaders can see and evaluate the program’s effectiveness and can ultimately perceive that the security protection is working as intended.

An operationally mature program takes a **long-term strategic approach** to security, providing all of the necessary tools and processes—both technical and non-technical—to ensure that your security system is robust, consistent, efficient, and effective.

# Achieving Operational Maturity

## Strategic Steps

There are three crucial steps to initiate strategic transformation of your security program.

- Formulate and announce top-level security objectives.** Senior management commitment is the foundation of a robust security program. Senior management must establish security as a key corporate objective for all lines of business, not just the IT security department. Specific corporate objectives must be established, and objectives and

accountability for each business manager must also be identified.

- Establish a strategic security plan.** Next, create a strategic plan that includes critical business assets and the necessary level of protection for each. Conduct a risk/benefit assessment to focus programmatic and protection measures. Be sure to include a mapping of tactical initiatives back to the plan, as well as a clear tie to the management objectives laid out in step #1.
- Establish security funding.** Finally, review the strategic plan to determine funding. Funding needs must be driven by the strategic plan, and specifically by the risk/benefit assessment. Create links between security and the largest business and IT initiatives, as these can be vehicles to more easily achieve and track progress toward corporate security goals. Structure security as a program, not as individual tactical initiatives being evaluated on a case-by-case basis.

Typically, organizations spend 6% - 8% of their IT budgets on security. If security will also include disaster recovery activities, then plan on 12% - 14%.

## Transformation Activities

CIBER uses a seven-layer “building block” model to illustrate the elements of a successful, mature security program. This model is useful for evaluating the relative maturity of an existing program, and can serve as the central planning tool for security program transformation projects (shown in Figure 1).

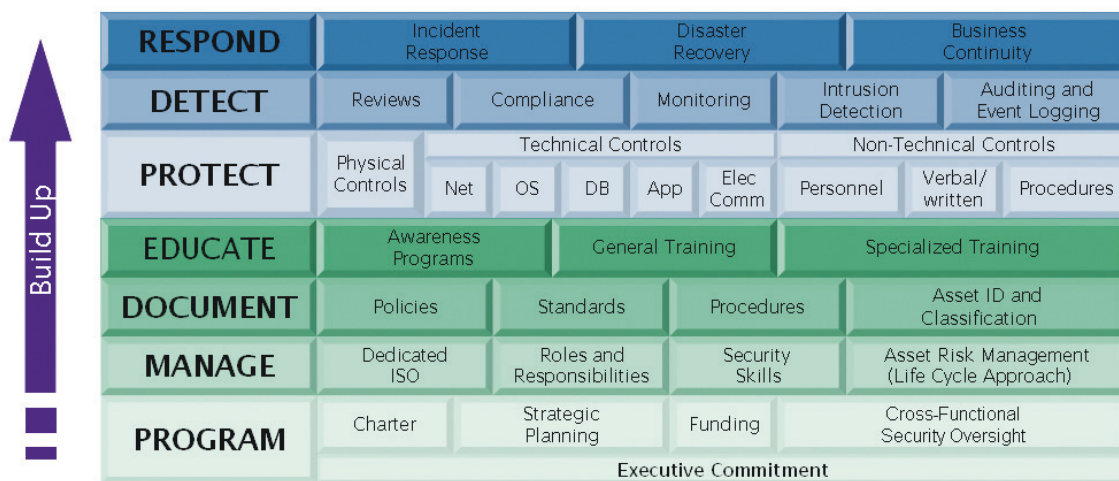


Figure 1: Security Building Blocks



As a security program is built or transformed, there are important activities in each of these layers, which are described in the following paragraphs.

### *Program*

The foundation of a mature security program, the Program Layer involves building a sense of communal responsibility to achieve security objectives, and incorporating group and individual accountability for the progress of the security program. It involves these transformational activities:

1. **Formulate and announce top-level security objectives.** Present a clear, consistent message to ensure that the vision for improving security is widely understood across the enterprise.
2. **Establish a strategic security plan.** Link security activities to management objectives through a roadmap or master plan.
3. **Establish a security budget.** Establish security funding as a programmatic initiative, as opposed to evaluating expenses for individual security projects on a case-by-case basis. It is often useful to establish, or at least evaluate, security spending as a percentage of overall IT spending. According to several studies across various industries, 6-8% of IT spending is a reasonable average to use as a benchmark, although during a period of build-up or transformation, spending may need to be higher.

If the steps here are not addressed adequately, all other steps will be less effective—this layer is truly the foundation on which a successful security program is built.

### *Manage*

The Manage Layer is where you establish the means to effectively manage security across an enterprise. It involves these transformational activities:

1. **Create a dedicated security officer position.** Assign a person to manage and govern security—generally someone without day-to-day security operational duties. The establishment of a position with a strategic focus is absolutely vital to moving up the maturity scale.
2. **Define the assets to be protected, and the protection requirements for each class of assets.** Focus security resources on specific business information and on processes that need protection. Ideally, security protections should

be tied to specific business goals, such as client expectations, contract requirements, or regulatory requirements.

3. **Spread accountability across the organization.** Nurture a sense of responsibility for security decisions and progress that extends beyond the dedicated security staff members, to staff outside the IT organization who can add a business balance to the security program.

### *Document*

The Document Layer is where you develop supporting documents that codify and institutionalize the security program. These activities are critical to gaining consistency and predictability. While it is not necessary to standardize every security function, it is important to have consistent security decision-making processes across the enterprise. This layer's transformational activities include the following:

1. **Develop a security policy framework.** Use an “umbrella” approach or framework to develop a security program that demonstrates traceability to your organization's collection of security regulations and external requirements. This proves more effective than creating a security program or activity for each regulation.
2. **Identify critical assets.** Conduct an inventory of organizational information assets and categorize them based on the asset classes defined in the Manage Layer. For most organizations, finding and classifying assets is a major step toward focused, rather than blanket, security protections. Focused protection is a cornerstone of a mature security program.

### *Educate*

During World War II, the U.S. military had a slogan that “loose lips sink ships,” meaning that you should not discuss military plans and operations because you never know who may be listening. In the military, the culture of secrecy is well-established and many security measures rely on correct behavior of the participants in an operation. In industry, the sanctity of the information is not as obvious, yet many corporate security programs still rely on correct behavior of users and system administrators.

The Educate Layer is the “loose lips sink ships” area for a strong security program. The transformational activities in this critical phase are to initiate security awareness among all employees, and provide training on proper security

procedures to those who have specific security-related job functions. Be sure to include concepts as simple as “Never give out your password. We will never send an email requesting your password, so if you receive one, notify the Security Officer immediately, as the email is probably an attempt to gain access to our systems.”

Clearly this is a non-technical measure, but it is one of many that—if not addressed—can quickly unravel all of the security precautions you've taken so far. During a program transformation, it is important to realize that specialized training on security job functions cannot be effective until the lower foundational layers have been addressed.

### *Protect*

The Protect Layer is where you deploy tactical measures to meet your long-term strategic goals. Most organizations already have many technologies in place here, and in most cases these should be retained and leveraged as much as possible. The goal is to approach the technologies as a collection of solutions to the overall security challenge rather than as individual patches that each address one area of risk.

The Protect Layer involves these transformational activities:

1. **Create a “roadmap”** to link existing technologies and upcoming technology investments to your strategic security plan and objectives.
2. **Identify where you have gaps and overlaps.**
3. **Evaluate the risk/reward of various protection options,** ensuring that protection mechanisms are focused on the critical assets identified in the Document Layer. Technology investments should target high-value assets and should tie in to the overall security priorities.

### *Detect*

The Detect Layer is where you continuously monitor the effectiveness of the security protections provided by the Protect Layer. This includes real-time or near-real-time event monitoring and periodic audits of your program to identify vulnerabilities, failures, and gaps. This is an important step, as many regulations require evidence of the effectiveness of your security program. Your ability to objectively assess your security status is vital to the overall success of your program.



There is generally limited activity in this layer in the early stages. Effectiveness reviews are not meaningful until new security processes are well established. However, as the program matures, the ability to detect and correct weaknesses in security controls will become more important since the ability to self-optimize defines the upper levels of most maturity models.

### *Respond*

The Respond Layer is where you create and test an incident response plan. This is the plan you will follow to respond to security incidents and report breaches as required by many government regulations. Disaster recovery efforts are also included in the incident response plan. Your overall objective is to ensure that everyone knows what to do to avoid chaos in case of a bad event.

In the initial stages of a security program transformation, it is usually sufficient to commit a basic plan to paper. As the maturity of your security program advances, this layer will be the focus of much activity as you use response mechanisms to limit the damage caused by a security failure in the lower layers. In fact, “perfect” protection is beyond the reach of most budgets. Therefore, mature security programs leverage the ability to quickly detect and respond to security failures as a way to further reduce risk below that which can be achieved by pure protection mechanisms alone.

---

*“Mature security programs leverage the ability to quickly detect and respond to security failures as a way to reduce risk below that which can be achieved by pure protection mechanisms alone.”*

---

# Building Your Business Case

Since few of us are lucky enough to be able to build our security programs from scratch, we must look for ways to transform existing security programs into something closer to a fully optimized security program. While “optimal” can be beyond the reach of most budgets, significant improvement is definitely achievable with modest investment. And those looking for a return on investment will find many benefits from a more mature security program:

- **More efficient management:** By strategically applying the right protections to the right assets, the operational costs of security can be driven downward.
- **Fewer unplanned costs and emergency incidents:** The cost of a planned, coordinated response is lower than the cost of a chaotic “all hands on deck” response. And, by anticipating security risks, the number of incidents requiring an emergency response should be significantly reduced.
- **Earlier correction of security problems:** Finding and fixing security problems earlier in the life-cycle gives you more options and lower costs. Studies of software bugs, for example, show that it is dramatically less expensive—up to an order of magnitude less—to fix bugs found during design or development as opposed to post-production.
- **Reduced labor costs:** By leveraging strategic technologies, such as enterprise security management tools, you can reduce labor costs to manage and monitor security tools. For example, log review by manual methods is very expensive and error-prone compared to the results that can be achieved with an enterprise-wide security information management (SIM) solution.

IT security has changed significantly in the last few years. It now encompasses much more than just firewalls. In order to address all of the categories that fall under the IT security umbrella—such as regulatory compliance, application security, network security, disaster recovery, and even voicemail security—executive management

must endorse and evangelize the importance of security initiatives across the enterprise, not just in the IT department.

By following the guidelines outlined in this paper, you can strategically transform your security program into one that is robust, efficient, cost-effective, and that permanently reduces risk.

## About the Author



**Ed Bassett**  
Vice President  
Global Security Practice

As Vice President of CIBER's Global Security Practice, Ed Bassett is responsible for helping CIBER's clients secure their critical information assets, whether it's for e-commerce transactions, sensitive customer records, or classified military communication.

Mr. Bassett's expertise is in state-of-the-art techniques for Internet and e-commerce security and systems design, such as application security, access control, authentication, encryption, network security, Public Key Infrastructure and security management practices.

He possesses more than 20 years of experience as an information systems security architect, and has been the principal advisor to Fortune 500 and government clients on information systems security. He was the lead security architect for several large-scale, high-value e-commerce and e-government systems, aerospace systems, defense systems, and IT infrastructure projects. He has managed comprehensive security programs involving all security disciplines. He designed security for the IRS's Electronic Federal Tax Payment System, the first IRS payment system approved for connection to the Internet, and which processes nearly \$2 trillion worth of transactions each year.

Mr. Bassett earned his Bachelor of Science degree in Computer Science from Clarkson University, in Potsdam, NY. He has published several articles on security topics and is a frequent speaker on effective security techniques at security symposiums, conferences, and CIO forums.

He can be reached at [ebassett@ciber.com](mailto:ebassett@ciber.com)



CIBER, Inc. (NYSE: CBR) is a pure-play international system integration consultancy with superior value-priced services and reliable delivery for both private and government sector clients. CIBER's services are offered globally on a project- or strategic-staffing basis, in both custom and enterprise resource planning (ERP) package environments, and across all technology platforms, operating systems and infrastructures.

Founded in 1974 and headquartered in Greenwood Village, Colo., CIBER now serves client businesses from over 60 U.S. offices, 25 European offices and seven offices in Asia/Pacific. Operating in 18 countries, with more than 8,000 employees annual revenue over \$1 billion, CIBER and its IT specialists continuously build and upgrade clients' systems to "competitive advantage status." CIBER is included in the Russell 2000 Index and the S&P Small Cap 600 Index.

[www.ciber.com](http://www.ciber.com)

**CIBER, Inc. • 5251 DTC Parkway • Suite 1400 • Greenwood Village, CO 80111 • 800.242.3799**

© 2008 CIBER, Inc. All rights reserved. CIBER and the CIBER logo are registered trademarks of CIBER, Inc.

CIBER stock is publicly traded under the symbol "CBR" on the NYSE.