

# Is Your Business at Risk?

*10 Things Every CFO Should Know About IT Security*

WHITE PAPER



centerbeam®

## 10 CATEGORIES OF RISK MANAGEMENT

# Table of Contents

**IT Security** ..... 1  
*Can You Afford Not to Ask the Right Questions?*

**Business Runs on Technology** ..... 1  
*The Same Tools That Streamline Business Also Increase Opportunities for Breach*

**Obstacles to Security** ..... 2  
*Why is it so Difficult to Implement Proper Protection?*

**Sources of Security Breaches** ..... 3  
*The Mundane, The Malicious, and Acts of God*

**Ten Categories of Risk Management** ..... 3  
*A CFO's Guide to Asking IT Staff the Right Questions*

**CenterBeam Understands IT Security** ..... 6  
*Expert Resources for Executive Peace of Mind.*

**Get a State-of-Your-Infrastructure Report** ..... 6  
*Find Out How Your IT Operations Compare to Best Practices*

## IT Security: Can you afford not to ask the right questions?

The irony in today's business world is that the same technology that has advanced communication, productivity, and efficiency has also made companies vulnerable to a host of threats that can cripple day-to-day operations. For this reason, executives need a basic understanding of IT security so they can assess their vulnerabilities and the impact they may have on business operations.

For businesses of all sizes, the threats are real—from major breaches that result in substantial losses to smaller incidents that create problems for you and your customers. Statistics from a University of Texas study showed that half of all companies go out of business within two years after a major data loss, and DTI/Price Waterhouse Coopers found that a full 70 percent of small firms go under within a year. Even if you manage to stay in business after such an event, technology glitches can compromise your credibility with your customers and partners.

### **Few executives are experts in technology or security, so they must rely on their IT professionals to cover the risks and protect their businesses.**

That's a lot to ask since only a small percentage of IT staff, themselves, have the extensive training to be considered true security experts. And most executives don't know the right questions to ask to ensure their businesses are adequately safeguarded.

In mid-size companies, IT professionals are under pressure to handle a growing number of responsibilities, including "help desk," hardware and software provisioning, networking, application management, training and more. Security, which touches every aspect of your business, is just one more item on the list. In addition to juggling multiple responsibilities, IT is often understaffed and overwhelmed with putting out the fire of the day. Due to this workload and shifting priorities, the proactive planning and daily attention that security requires is often neglected.

Companies recognize security is a specialty, and in the information security sector, the widely recognized International Information Systems Security Certification Consortium addresses ten domains, or key focus areas, for a professional to become a Certified Information Systems Security Professional (CISSP). These ten domains offer a benchmark for knowledge and expertise in security.

### **A basic understanding of IT security and vulnerabilities is vital to your company's growth and survival.**

Although it may seem like a daunting task, there are steps that can be taken to increase your understanding and protect your business. In this paper, we offer a high level security overview, as well as provide a question guide to help you engage your IT staff in a productive discussion about your IT environment. This will allow you to compare your situation to current best practices and assess the implications for your business.

## Business Runs On Technology

*"Every enterprise, large or small, is exposed to risk in proportion to their reliance on information technology for their processes and business continuity."*

Richard Stienon

Chief Marketing Officer, Fortinet

provider of Unified Threat Management (UTM) systems

Without IT business as we know it would come to a grinding halt. From simple databases and email to the most sophisticated on-demand applications, companies require high availability and security to maintain daily operations.

However, the same digital tools that have streamlined business operations have also increased the opportunities for calamity. Without proper security precautions, a single programming mistake, worm or lost laptop can grease the

skids for disaster. Chaos can come in the form of stolen customer records and public relations fiascos to natural disasters that corrupt data or make it inaccessible.

However, disasters do not always happen on such a grand scale. Businesses can lose customers because of inadvertently passing on a virus that shuts down client email or a worm that impairs day-to-day system operations.

According to the National Data Awareness Project and International Data Corp., billions of dollars are lost annually in the U.S. due to security breaches. To avoid becoming part of this statistic, businesses must implement a comprehensive, dedicated and fully supported approach to IT security.

While even the largest corporations struggle to accomplish this, at least they have the staff and in-house expertise to continually test and develop their strategy. Unfortunately, mid-sized organizations lack the internal resources to adequately address security, and they are often resigned to taking a “best effort” over “best practice” approach.

## Obstacles to Security: Why is it so difficult to implement proper protection?

Technology is a core part of today’s business environment and it continues to evolve at a breakneck pace. That means that IT professionals’ time and attention is stretched thin trying to stay up to date with the latest advances while simultaneously providing expertise to nearly every facet of an organization’s operations.

Brian Karney, Chief Operating Officer of AccessData Corporation, says most mid-size companies also believe they have fewer security risks than larger, higher visibility organizations. In reality they have to deal with the same threats, but with access to significantly fewer resources and less expertise. This scenario can lead to overconfidence that actually increases midsize business’s risk. In addition to this danger, he points out that turf issues and worries about job security may make IT professionals in these companies more sensitive to internal politics than to recognizing and addressing threats to data security and operations.

“Admitting a computer incident has occurred is like admitting you can’t handle your job. No one is willing to admit to being hacked unless it’s huge and becomes publicized. But it’s not about the big event that makes you run for the exits and hit the red button. It’s about connecting with people on the fire fight level—and paying attention to the ‘ordinary’ stuff that goes on everyday,” he says.

The challenges to implementing adequate IT security can be grouped into several basic categories:

- Limited IT resources
- Limited executive knowledge of IT security
- Inadequate time devoted to security planning and contingencies
- Protective technology lagging behind that of attackers
- Lack of a disaster response plan
- Broadband and wireless connections increasing vulnerability

*“The new risks are much harder to defend; they take a level of commitment to continuous monitoring and uncompromising adherence to policy with real penalties that, so far, only the largest banks and most sensitive military organizations have been willing to implement.”*

Alan Paller

Director of Research at SANS  
(SysAdmin, Audit, Network, Security)  
Institute

*If organizations of this size and stature have fallen victim to such malicious activity, what chance do smaller organizations have?*

IT’s focus is stretched thin keeping pace with evolving technology and juggling the demands of day-to-day operations. Security often takes a backseat.

*“It’s not about the big event that makes you run for the exits and hit the red button. It’s about connecting with people on the fire fight level—and paying attention to the ‘ordinary’ stuff that goes on everyday.”*

Brian Karney

COO, AccessData Corporation

## Sources of Security Breaches: The Mundane, The Malicious, and Acts of God

There are many different sources of risk. Here we list some of the most common.

### Data Exposure

The more portable company information is, the easier it can be lost or stolen. According to the Ponemon Institute's 2007 Annual Study (*U.S. Cost of a Data Breach: Understanding Financial Impact, Customer Turnover and Preventative Solutions*), lost or stolen laptops and other portable devices accounted for 49 percent of data breaches in its sample.

### Employee Error

Even with the best of intentions and adherence to recommended security practices, employees can easily pass on malicious viruses or worms embedded in email attachments or other downloaded documents. This can set off a chain of events that affects overall company operations as well as those of its clients. Without multiple layers of regularly updated filters, viruses and worms are extremely difficult to detect and guard against.

### Disgruntled Employees

Whether looking to "get even" or spend company time and resources for personal use, employees can easily introduce extraneous artifacts that corrupt data, reveal proprietary information or otherwise degrade or compromise system performance.

### Competitor Espionage

While this type of data compromise may be less malicious than run-of-the-mill hackers (who do damage for damage's sake), the importance of protecting proprietary and customer data remains crucial.

### Hacking

According to Symantec's *Internet Security Threat Report* for the first half of 2007, malicious attacks have become more professional, quickly adapting to companies' latest security strategies. The reports says, "Today's attackers are increasingly sophisticated and organized, and have begun to adopt methods that are similar to traditional software development and business practices." Reliable, robust attack kits and phishing toolkits can be found for sale online. Trojans can even establish positions within a company's system that leave backdoor entries even if they are successfully removed.

### Fire, Flood and Natural Disaster

No matter where your business is located, environmental factors pose risks. Proper planning (including adequate hardware backup) is essential in order to retrieve affected data and return to normal operations quickly.

No company or product is immune.

Qualsys found an increase of 300% in vulnerabilities in Microsoft® Office products from 2006 to 2007.

This demonstrates the importance of staying up to date on critical security patches.

## 10 Categories of Risk Management

Within IT circles, the International Information Systems Security Certification Consortium is known as an authority when it comes to addressing IT security issues. The consortium has developed ten domains, or key focus areas, as benchmarks of both security best practices and the required knowledge and expertise for a professional to become a Certified Information Systems Security Professional (CISSP).

These same guidelines can be used to assess the security of any business. However, most CFOs and COOs don't know the right questions to ask to attain relevant reports from their IT staff. For that reason, we provide the following explanations of the ten domains, along with questions to help you become more familiar with your IT infrastructure and identify risk.

### 1. Access Control Systems

These elements identify and manage who has "right of entry" to different categories and levels of security. The most efficient method is single-sign-on, which utilizes one "event" to grant admittance, track activity, issue or revoke authentication/credentials, etc. This function can cross-reference physical location with authentication requests in order to detect unauthorized remote attempts at access when the "legitimate" individual is physically on the premises.

### 2. Telecommunications Security

This area focuses on the physical network's layout and hardware configuration. Because of the intermingling of data lines, voice communication and IT phone networks, they have become a part of the security protocol.

### 3. Disaster Recover Planning/Business Continuity Plan

*Contingency Planning and Management Magazine* has shown that 40 percent of businesses that were forced to close for three days failed within 36 months, so this category is highly important. According to Franklin Fletcher in his *Checklist for a Successful Disaster Recovery/Business Continuity Plan*, the key best practices include:

- *Management support* at senior levels
- *Staffing* with resources provided from broad-based departments (IT, as well as individual business units)
- *Risk assessment*, which should candidly review vulnerabilities (including geographic locations, hardware, software and network design)
- *Business Impact Analysis* to assess essential functions, staff, contractual obligations and how the most critical functions can be supported
- *Prevention* to review physical security, personnel procedures infrastructure (like generators, fire suppression, etc.) and backup and retention processes
- *Incident command structure*
- *Data backup and storage procedures* (along with processes for data and system restoration)
- *Identification of alternate locations* for systems and staff
- *Plan maintenance and distribution* to provide specifics on how the plan will be disseminated enterprise-wide

### 4. Security Management

This category examines how security priorities are integrated into ongoing administration and procedures. It also makes sure staff is aware of security policies and understands how they are implemented.

### 5. Law, Investigation and Ethics

Mechanisms need to be in place that can track security incidents and their sources. They should also be able to identify when a security event takes place and have forensic capabilities to provide details for law enforcement, regulatory compliance and respond appropriately and efficiently to legal actions.

## Questions to Ask Your IT Staff for Each Risk Category

(1) *What is our policy for granting systems access? (employees, contractors, suppliers, customers, auditors)*

(2) *What telecom diversity does our business require?*

*Do we audit our voice, web, email and IM traffic?*

*Who has access to our telecommunications system?*

(3) *Have we drafted a business continuity plan? When was it last reviewed?*

*What are our primary systems?*

*In terms of our backup and recovery environment, what are our recovery time objectives? (RTO<sup>1</sup>)?*

*How many hours' worth of data we can lose without compromising our business (RPO<sup>2</sup>)?*

*How do we evaluate and prioritize our information assets?*

(4) *Do we have real-time processes in place to alert us when something is going wrong?*

*How do we prioritize events when there is a problem?*

*Do our policies differentiate between threats to business operations and privacy violations?*

*Do we have guidelines for notifying management, the press, employees, partners, suppliers and investors in case of security incidents?*

(5) *Can we provide detail to authorities in the event of a hacking incident?*

*Who is designated to provide details to authorities?*

*Do we have guidelines on how to protect evidence? Who has the authority to conduct an investigation?*

*Do we have contact information for local law enforcement?*

1. RTO = Recovery Time Objectives

2. RPO = Recovery Point Objectives

## 6. Application Security and Systems Development Security

Even when a network is designed to be as secure as possible, modifications, additions and other alternations occur over time. New components (hardware and software) or even new business functions can adversely affect what was originally an iron-clad system. Careful, routine monitoring and testing will ensure reliability and security.

## 7. Cryptography/Encryption

This is a basic strategy for protecting data even if it is stolen or breached. Interestingly, the California Database Security Breach Notification Act, which requires organizations to provide notification of security breaches, exempts companies with encrypted data from having to notify customers of such events.

## 8. Computer Operation Security

This category focuses on protecting software from errors and infections. Multi-tier, multi-layer architecture of various software barriers are highly recommended so that if one application is less effective against a particular threat (e.g., newly launched virus), another is in place to provide added protection. In his white paper *Operation Security*, Allen Fernandes describes four different types of operations security controls:

1. *Preventative* for keeping out unintentional errors
2. *Detective* for recognizing errors after they occur
3. *Corrective* to implement backup data procedures
4. *Deterrent* to limit and prevent unauthorized access

## 9. Operational (Physical) Security

Although options may be limited by an organization's existing location, Franklin Fletcher, author of *Physical Security and Your Data Center*, recommends that locations housing servers, backup sites and other critical hardware should:

- Be housed in a single tenant facility outside of risk areas like flood zones, airport flight patterns, heavy traffic or near chemical plants
- Have access to multiple utility sources
- Limit the number of windows
- Avoid exterior identification, like company signs
- Have adequate fire detection and suppression
- Require several levels of authentication for physical entry

## 10. Security Architecture and Models

In addition to creating a culture of security in which security-minded behavior is the norm, an effectively designed system is at the core of data protection. In *Security Architecture*, Dan McGinn-Combs lists several threats that a system must address:

- *Covert channels*, which provide entryways that bypass the usual mandatory controls
- *Buffer overflow attacks*, which use programming flaws to gain entry
- *State attacks* that use "timing and transition from one state to another" to enter the system
- *Emanations*, electrical impulses that come from equipment inside the secure perimeter and may carry proprietary information to the outside
- *Maintenance hooks* used to provide software access during development, but inadvertently provide access in the production version

- (6) *When did we last take inventory of our applications? Are they the latest versions?*

*How often do we update for critical patches? Who decides what is considered critical?*

*Have we tested for application vulnerability?*

*Do we have the latest anti-virus software?*

- (7) *How are we handling sensitive data?*

- (8) *Do we have policies to limit physical and logical access to our IT systems, including data repositories?*

*Are logs and records kept of physical access to key IT infrastructure (video, syslog, paper logs)?*

*How are these logs archived, protected and accessed?*

*How are authorized devices identified and removed (servers, wireless access points, printers)?*

- (9) *Do our badges have the company name on them? (If so, one lost badge tells the finder where to go to gain access.)*

*Do we monitor badges and who enters the building after hours?*

*Do we provide access to critical areas only to those permitted?*

- (10) *When did we last examine our security model?*

*Have we reviewed the various components of our model to determine which organizations we regularly deal with?*

*Do those organizations expose us to potential threats?*

## CenterBeam Understands IT Security

For mid-size companies without in-house security experts or the budget to continually upgrade to the latest of security software revision, outsourcing IT responsibilities to a managed services company like CenterBeam can be a viable and cost effective solution.

With an architecture designed with multiple security layers throughout (including multi-tiered anti-virus protection), security is part of the fabric of CenterBeam's operating philosophy *and* operating system. This allows you to focus on your core business while also taking a proactive approach to security.

CenterBeam provides valuable expertise from CISSP professionals whose sole focus is to provide state-of-the-art IT management and the most current security practices to protect your infrastructure against evolving threats. CenterBeam's services, processes and policies are SAS 70 Type II certified. The company is inspected annually to ensure the highest levels of security, stability and reliability for its clients.

CenterBeam develops customized solutions based on in-depth analyses of your IT environment. These solutions are implemented in partnership with your IT staff to be sure that they are seamlessly integrated into your company's operating systems and day-to-day activities. The result is expert protection against outside threats, assurance of operational integrity and an in-house IT staff that is free to devote time and expertise to the core functions critical to the success of your business.

To ask questions or schedule a meeting, call **1 (877) 710-8880** (US/Canada toll-free) or visit [www.centerbeam.com](http://www.centerbeam.com).



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