

Every company needs to have a security program

No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a security program by information security professionals. Whether yours is five or 200 pages long, the process of creating a security program will make you think holistically about your organization's security. A security program provides the framework for keeping your company at a desired security level by assessing the risks you face, deciding how you will mitigate them, and planning for how you keep the program and your security practices up to date.

Your company's value is its data

Think you don't have anything of value to protect? Think again. The key asset that a security program helps to protect is your data — and the value of your business is in its data. You already know this if your company is one of many whose data management is dictated by governmental and other regulations — for example, how you manage customer credit card data. If your data management practices are not already covered by regulations, consider the value of the following:

- Product information, including designs, plans, patent applications, source code, and drawings
- Financial information, including market assessments and your company's own financial records
- Customer information, including confidential information you hold on behalf of customers or clients

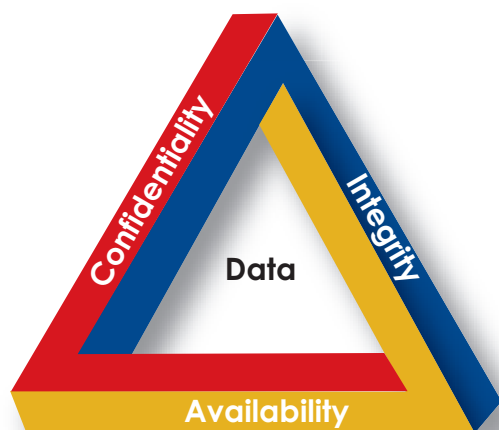


Figure 1: Securing your data means maintaining its confidentiality, integrity, and availability.

Protecting your data means protecting its confidentiality, integrity, and availability as illustrated by the C-I-A triangle (Figure 1). The consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company

goodwill. Consider the following examples:

- Failure to protect your data's confidentiality might result in customer credit card numbers being stolen, with legal consequences and a loss of goodwill. Lose your clients' confidential information and you may have fewer of them in the future.
- A data integrity failure might result in a Trojan horse being planted in your software, allowing an intruder to pass your corporate secrets on to your competitors. If an integrity failure affects your accounting records, you may no longer really know your company's true financial status.
- If your data becomes unavailable, you may be unable to serve your customers and/or process transactions, and possibly lose revenue.

Having a security program means that you've taken steps to mitigate the risk of losing data in any one of a variety of ways, and have defined a life cycle for managing the security of information and technology within your organization.

Hopefully the program is complete enough, and your implementation of the program is faithful enough, that you don't have to experience a business loss resulting from a security incident. If you have a security program and you do experience a loss that has legal consequences, your written program can be used as evidence that you were diligent in protecting your data and following industry best practices.

Elements of a good security program

A good security program provides the big picture for how you will keep your company's data secure. It takes a holistic approach that describes how every part of your company is involved in the program. A security program is not an incident-handling guide that details what happens if a security breach is detected (see *The Barking Seal* Issue Q1 2006). It's also not a guide to doing periodic assessments, though it probably does dictate when to do a security assessment (see *The Barking Seal* Issue Q2 2008).

Your security program defines what data is covered and what is not. It assesses the risks your company faces, and how you plan to mitigate them. It indicates how often the program will be re-evaluated and updated, and when you will assess compliance with the program. The key components of a good security program are outlined in the following sections.

1. Designated security officer

For most security regulations and standards, having a Designated Security Officer (DSO) is not optional — it's a requirement.

Your security officer is the one responsible for coordinating and executing your security program. The officer is your internal check and balance. This person or role should report to someone outside of the IT organization to maintain independence.

2. Risk assessment

This component identifies and assesses the risks that your security program intends to manage. This is perhaps the most important section because it makes you think about the risks your organization faces so that you can then decide on appropriate, cost-effective ways to manage them. Remember that we can only minimize, not eliminate, risk, so this assessment helps us to prioritize them and choose cost-effective countermeasures. The risks that are covered in your assessment might include one or more of the following:

PHYSICAL LOSS OF DATA. You may lose immediate access to your data for reasons ranging from floods to loss of electric power. You may also lose access to your data for more subtle reasons: the second disk failure, for example, while your RAID array recovers from the first.

UNAUTHORIZED ACCESS TO YOUR OWN DATA AND CLIENT OR CUSTOMER DATA. Remember, if you have confidential information from clients or customers, you're often contractually obliged to protect that data as if it were your own.

UNAUTHORIZED DATA REQUESTS. These might take the form of the phone call to talk to "the person in charge of the copier," or it may be the phishing email that victimizes one of your employees (and your data)

INTERCEPTION OF DATA IN TRANSIT. Risks include data transmitted between company sites, or between the company and employees, partners, and contractors at home or other locations.

YOUR DATA IN SOMEONE ELSE'S HANDS. Do you share your data with third parties, including contractors, partners, or your sales channel? What protects your data while it is in their hands?

DATA CORRUPTION. Intentional corruption might modify data so that it favors an external party: think Trojan horses or keystroke loggers on PCs. Unintentional corruption might be due to a software error that overwrites valid data.

3. Policies and procedures

Preparing your risk assessment hopefully gave you lots to worry about. The policies and procedures component is the place where you get to decide what to do about them. Areas that your program should cover include the following:

PHYSICAL SECURITY documents how you will protect all three C-I-A aspects of your data from unauthorized physical access.

AUTHENTICATION, AUTHORIZATION, AND ACCOUNTABILITY establishes procedures for issuing and revoking accounts. It specifies how users authenticate, password creation and aging requirements, and audit trail maintenance.

SECURITY AWARENESS makes sure that all users have a copy of your acceptable use policy and know their responsibilities; it also makes sure that your IT employees are engaged in implementing your IT-specific policies.

RISK ASSESSMENT states how often you will re-assess the potential threats to your IT security and update your security program.

INCIDENT RESPONSE defines how you will respond to security threats, including potential (such as unauthorized port scanning) and actual incidents (where security has been compromised). We discussed the importance of having an incident-handling guide in the Q1 2006 issue of *The Barking Seal*.

VIRUS PROTECTION outlines how you protect against viruses. This might include maintaining workstation-based products and scanning email, Web content, and file transfers for malicious content.

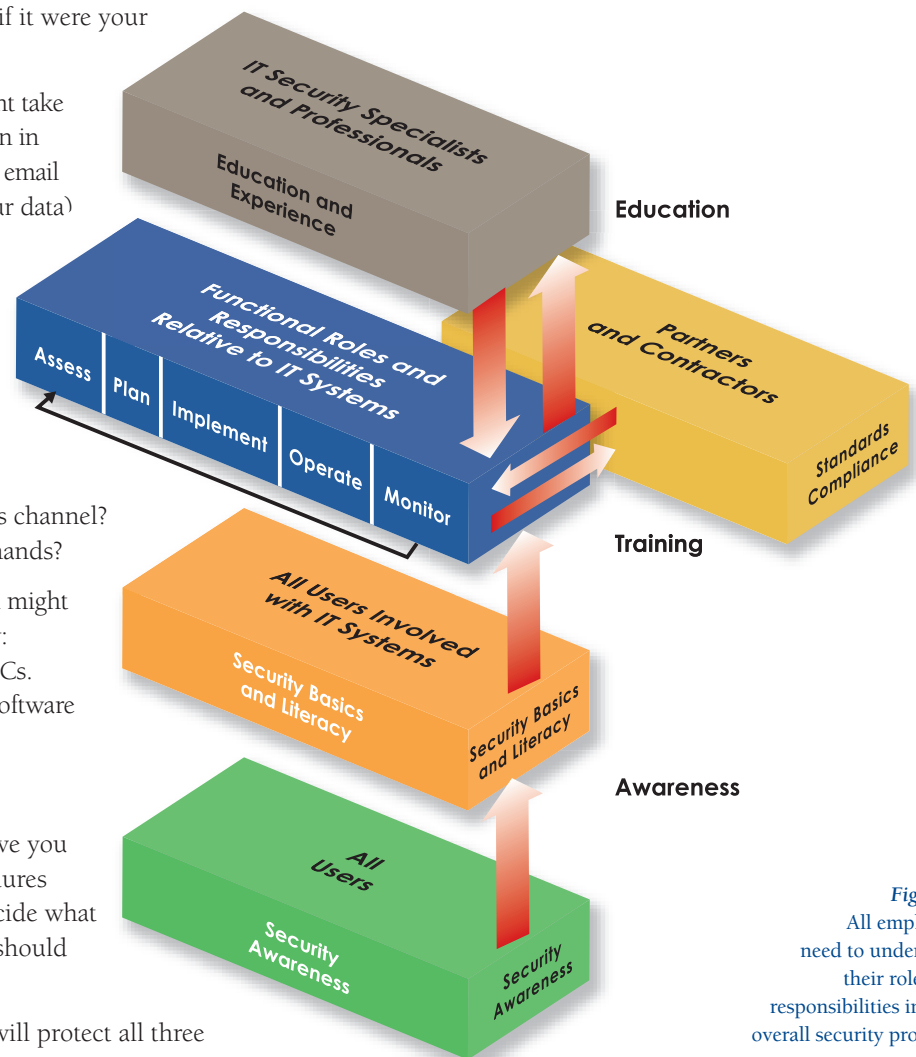


Figure 2: All employees need to understand their roles and responsibilities in your overall security program.

BUSINESS CONTINUITY PLANNING includes how you will respond to various man-made and natural disaster scenarios. This includes setting up appropriate backup sites, systems, and data, as well as keeping them up-to-date and ready to take over within the recovery time you have defined.

RELATIONSHIPS WITH VENDORS AND PARTNERS defines who these organizations are, what kind of data you might exchange with them, and what provisions must be in your contracts to protect your data. This is an often-overlooked aspect of data security because your IT organization probably has not had a lot of interaction with your legal organization over vendor contracts. You may need to take measures such as evaluating your partners' ability to safeguard your data and insisting on having reasonable security practices in place.

4. Organizational security awareness

The security community generally agrees that the weakest link in most organizations' security is the human factor, not technology. And even though it is the weakest link, it is often overlooked in security programs. Don't overlook it in yours.

Every employee needs to be aware of his or her roles and responsibilities when it comes to security. Even those who don't even touch a computer in their daily work need to be involved because they could still be targeted by social-engineering attacks designed to compromise your physical security. In its Information Security Handbook, publication 80-100, the National Institute of Standards and Technology (NIST) describes the importance of making all levels of your organization aware and educated on their roles and responsibilities when it comes to security (Figure 2). All users need to have security awareness training, while those involved with IT systems need to have more role-specific training. Your IT organization, which implements a continuous cycle of assessing, acquiring, and operating security-related hardware and software, needs even a higher level of involvement, taking direction from your own security specialists and those you hire as consultants.

5. Regulatory standards compliance

In addition to complying with your own security program, your company may also need to comply with one or more standards defined by external parties. This component of your security plan defines what those standards are and how you will comply. Regulatory standards that might affect you include HIPAA (for patient information), PCI (for credit card processing), FISMA (for governmental agencies and contractors, see *The Barking Seal* Q4 2006), Sarbanes-Oxley, and Gramm-Leach-Bliley (for corporate financial management).

6. Audit compliance plan

This component of your security program dictates how often you will audit your IT security and assess its compliance with your security program. As we discussed in the Q2 2008 issue of *The Barking Seal*, there are aspects of your security that you will want to audit on a frequency ranging from daily to annually. Periodic security assessments are important for finding out whether your security has already been breached. They help you to stay on top of new security threats with the right technology and staff training. And they help you make smart investments by helping you to prioritize and focus on the high-impact items on your list.

A security program is never "done." As Figure 2 illustrates, your IT organization is always in the process of iterating through the program's life cycle for all areas that it defines. You assess risks, make plans for mitigating them, implement solutions, monitor to be sure they are working as expected, and use that information as feedback for your next assessment phase. Likewise, your security program document has this life cycle built into it, as it specifies how often you will re-assess the risks you face and update the program accordingly.

Getting on the right footing

It doesn't matter whether your security program is five pages (as are some we've produced for clients) or 200 pages long (such as the NIST document cited above). The important thing is that you have a security program and that you use it to address your company's security in an organized, comprehensive, and holistic way. You can adapt the above elements to create a security program for your organization, or, if you need help, give us a call at 303.245.4545.

Everyone needs to have a security program because it helps you maintain your focus on IT security. It helps you identify and stay in compliance with the regulations that affect how you manage your data. It keeps you on the right footing with your clients and your customers so that you meet both your legal and contractual obligations. Its life cycle process ensures that security is continuously adapting to your organization and the ever-changing IT environment we live in. And, of course, it's the right thing to do because protecting your data's security is the same as protecting your most important asset. ■

This article was reprinted from the Q3 2008 issue of *The Barking Seal*, a publication of Applied Trust. You can subscribe to *The Barking Seal* online at <http://www.appliedtrust.com/barkingseal>. "Applied Trust" and the "Seal on a Rock" Applied Trust Engineering logo are registered service marks of Applied Trust. All other trademarks are registered to their respective owners.