

A Manual for Success: The Security Policy

By Mark E. Egan
Partner StrataFusion Group

Behind every effective Information Security Program are solid policies, standards, and procedures. By now, you should have a good handle on what information assets require protection, roles and responsibilities within your organization, current user privileges – as well as vulnerabilities that may result from these current practices. Next, you need to take stock of your current policies, and determine specific areas of your current policy that need to be updated, as well as unregulated areas that need to be covered by policy.

The Foundations of Policy

Information security policies, standards and procedures are different documents that all work together to support an information security program. Take a look at the following illustration:



Each enterprise has unique considerations that need to be taken into account when developing their own standards and procedures. In this article, we will focus on the high-level policies that are recommended for enterprises.

Things to consider

Creating an effective security policy is a balancing act – employees must have access to the information assets they need to do their jobs and stay productive, while at the same time, the integrity and confidentiality of the company's data must be maintained. In addition, each policy must be sensitive to varying global cultures and regulations, but at the same time, be consistent across all offices.

Once you have determined the scope and goals of your policy effort, here are some things that you should always keep in mind when developing a policy:

- **Policy format** - The format of your policy will be determined by the needs of your enterprise. Many enterprises have 20 or more policies in place at one time. One example of a policy would avow that your enterprise would comply with all government and industry regulations 30 days in advance of the deadline. In this case, you would set standards and procedures for how you would go about meeting the terms of each government and industry regulation (such as HIPAA, GBLA) that your enterprise is subject to.
- **Consistency** – When creating any policy, make sure it is consistent on a global basis. For instance, some data protection laws in Europe are more stringent than those in the United States. This requires that you create a policy that complies with European rules, but is implemented across all of your offices worldwide, so that it is the same everywhere. If your business is connected to the Internet, other companies from all over the World have access to your business. In order to do business on a global basis, you need to be aware of, and comply with international regulations.
- **Dynamic nature** -You may have a policy in place, but when is the last time you have updated it? Policies should never be viewed as static. As operating environments, business plans, regulations and the economics of your enterprise change, so your policy should be updated to reflect these changes. If you set up your program with a general policy for each area, supported by more specific standards and procedures, changes to policy will be easier, because you only need to change the individual standards or procedures– not the overall policies for the program.
- **Avoid long technical documents** - Policies are needed to protect information and people in the organization. Security policies should be concise, and written in a way that can be understood by all employees, even those that are not very knowledgeable about information technology.
- **Provide details regarding monitoring and enforcement** - Be clear regarding how policy compliance will be monitored, and the penalties for employees who fail to follow the terms of the policy.

Key policies

These days, it is not uncommon for enterprises to have many information security policies in place at one time. Here are some examples of important areas that should be covered with a policy:

- **Account Administration** – It is very important to have tight controls in place governing who has access to your systems. Access to the company's systems is like a key to your house, and you wouldn't give just anyone a key, would you?

These controls must include everyone that desires access to the systems (from full time to temporary employees), and then give access rights based on job function. It is also important to ensure that employees and contractors who leave the company have their access removed quickly, as you don't want to leave yourselves exposed in the event of a disgruntled employee. Passwords should follow industry best practices for length, use of special characters and be updated on a regular cycle, such as every 90 days.

- **Emergency Response** – If you are hit by a virus and are knocked offline for 24 hours or more, what would you do? Produce a predefined checklist of procedures that must be carried out in case of a security emergency. Among other things, the checklist should provide clear guidelines for communication – who needs to know what, and how they can be reached at all times. It is a good idea to engage your legal, public relations and human resources departments into this preparation. Chances are that something will happen, and you will be glad that you have prepared for it.
- **Remote access policy** – Today's enterprise networks are spread geographically and accessed remotely on such a regular basis that having a strong remote access policy in place is essential. First of all, it should be determined who is allowed remote access, and then how they connect to the company network. Security measures that remote users must take, including antivirus and firewall protection, should be clearly defined, as should the data that remote users should be able to access on the network.
- **Vulnerability Management** – Develop a regular schedule for running network scans, and designate members of the staff that will be responsible for running these scans. This way you can stay on top of things like applying patches, and ensuring that defaults are set properly, and known vulnerabilities are addressed.
- **Acceptable use** – An acceptable use policy covers Internet, email, and laptop computer use by employees in the policy. You need to make it clear that it is the employee's responsibility to protect the information stored on their accounts.

So there is no misunderstanding, the policy should spell out specific user guidelines. Here are some things you might include in an acceptable use policy:

- Define limits of non-business use of email and Internet at work.
- Specify what activity will be considered offensive, and in violation of the policy, such as: inappropriate emails, visits to adult Web sites, distribution of confidential information internally or externally via the company network, etc.
- The user's responsibility for safeguarding their workstations – password protection, locking computers when not in use, etc.
- Outline the rules for accessing file-sharing sites, downloading unauthorized software, etc.

Communicating the policy

Enterprise-wide compliance is necessary in order for a policy to be effective. It is your responsibility to make everyone understand the importance of security initiatives. Here are some things you can do to increase employee compliance:

- **Educate employees** – Inform your employees about various security issues, from information misuse, to proper use of email, to physical security. This will help your employees better understand the security policy and their important role in the overall security of the enterprise.
- **Make it accessible** – All employees need to know about the security policies, and where to find them. Make the policy easily accessible, whether via email, an employee handbook, or intranet, so employees can access it at a moment's notice. Whenever updates are made to the policy, employees should be given an update and an explanation of the changes.
- **Get signatures**– If possible, have your employees sign and date the policy, with their signature being a testament to their understanding and willingness to cooperate with the policy. Most people want to understand things before they sign them, so chances are, your employees will take time to read through the policy more carefully. When requesting their signatures, let your employees know that this is not to be taken as an indication of lack of trust, rather, a desire on your part that they fully understand the importance of the program.
- **Incident response procedures** - Employees should know to whom they should report, and what actions they should take if they are confronted by security breaches. Don't make employees jump through too many hoops in order to make a report, or they might not bother the next time around.

Measuring compliance

An internal or external audit team can be set up to measure policy compliance. If it is an internal team, make sure they are not the same team in charge of defining and enforcing policy. There are also tools that will automatically monitor and manage the discovery of policy compliance, or deviations and vulnerabilities on the enterprise network.

Set an example

Involve your human resources and legal departments when setting policies – this will help them understand and promote the policies on your behalf. Getting buy-in from other departments and other executives is key – this will increase company-wide support and awareness for your security initiatives.

As the executive in charge of security, ultimately your employees will look to you for a positive example. Change attitudes and bring more attention to security by making it a major enterprise concern. Provide security education for your employees to help them become more security-aware. Through education, you can reiterate the importance of every single person's contribution in making the security practice a success. Make security an everyday theme, and a part of the daily routine at your enterprise. To encourage everyone's participation, acknowledge or reward exemplary policy-compliant behavior, such as prompt reporting of an incident. A security-conscious enterprise is likely to have less weak links within it.

About the author

Mark Egan is a partner of the StrataFusion Group, Inc. and has over 25 years of experience in information technology. Prior to joining StrataFusion, Mark was a CIO at Symantec Corporation for 6 years during the company's rapid growth from a consumer software publisher with \$600 million revenue to the market leader of security with \$5 billion revenue. During his tenure with Symantec, he led the information technology integration through 28 acquisitions, including a \$13 billion acquisition of Veritas Software that helped Symantec become the world's 4th largest software company.

Mark's expertise includes information technology strategy & planning, information security, and mergers & acquisitions. He is the author of *Executive Guide to Information Security: Threats, Challenges, and Solutions* and was a contributing author of *CIO Wisdom* and *CIO Perspectives*. Mark is also a frequent speaker on best practices for information technology and security. He currently teaches a graduate class, "Building Business Value through IT Innovation", at the Haas School of Business at UC Berkeley.

Next Article in Series: The next stop on the Information Security Roadmap is Technology.

Related links:

- Read the first article in Mark Egan's perspective series, "Look Before You Leap Into a Security Program"
- Read the second article in Egan's perspective series, "Starting From the Ground Up: Constructing a Security Team"