

FRSecure White Paper

Characteristics of Effective Information Security Programs

Prepared By:
Evan Francen, CISSP CISM
Managing Partner
FRSecure LLC
evan@frsecure.com

Page 1

Table of Contents

Table of Contents	2
Introduction	3
Characteristic #1: Strattical	3
Strategic	3
Tactical	3
Characteristic #2: Holistic	3
Characteristic #3: Organized	4
Characteristic #4: Governed	5
Characteristic #5: Formal	5
Characteristic #6: Alive	6
About FRSecure	6

Characteristics of Effective Information Security Programs

Introduction

FRSecure has assessed the effectiveness of information security programs for over a dozen companies thus far in 2009. We have assessed the effectiveness of programs in companies as small as 20 employees and as large as 45,000 employees. We have worked with companies ranging from air couriers to banks to software developers. Through our engagements and past experiences, we have noticed some things that are characteristic of well-run and effective information security programs. Before we begin, let's define the term *effective information security program*.

An effective information security program is a program that understands and documents the risks to an organization's information resources and manages those risks according to that which has been deemed acceptable to the business.

The information that you find in this white paper is largely based upon firsthand experience gained from working with many of our client companies. We do not disclose our client names as a matter of policy.

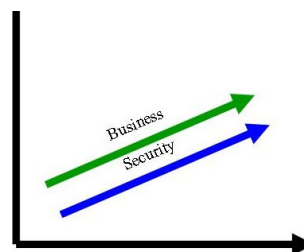
This white paper is written to communicate our observations of effective information security programs and is not intended to be a step-by-step guide.

Characteristic #1: Strattical

What is "strattical"? OK, it's a made-up word, but it does have real meaning. Effective information security programs are comprised of both **strategic** and **tactical** initiatives, carried out simultaneously.

Strategic

In order for information security to be effective, it must be aligned with the objectives of the business and must never be at odds with the business. Information security personnel must take the time to discover and understand business strategy before implementing information security strategy. Rome wasn't built in a day and neither will your information security program. Determine and document your one, three and five year plans for your information security program.



Tactical

There are numerous tactical, day-to-day functions in an effective information security program. These functions can include log review, incident response, intrusion detection tuning, firewall administration, patching, etc. The tactical functions in an effective information security program allow information security professionals to attend to current information security needs while fulfilling the strategic direction of the program as a whole.

Characteristic #2: Holistic

Have you ever heard the phrase, "you are only as strong as your weakest link"? When it comes to information security, you are only as secure as your highest risk. Risk is essentially the likelihood of an event paired with the impact of that event. Risks appear throughout the business, not just in IT. Information security is not an IT issue, it is a business issue. The ineffectiveness of a physical security control can be just as devastating as a poor technical (or IT control). The challenge here is that often times Information Security reports up through IT channels.

Characteristics of Effective Information Security Programs

An effective information security program takes all of the risks to information resources into account; administrative, physical and technical. The impact of a break-in to a corporate office should be addressed in as much importance as a remote compromise of your ecommerce site.

When information security is treated as an IT issue, there is often:

- **A lack of visibility** - Information security personnel must understand how the business uses information in order to understand the risks to the confidentiality, integrity, and availability of information in its various forms; written, printed, spoken, electronic, etc. A well-run IT department will often align technology with the business, but necessarily information security. Effective information security programs seek guidance and understanding from the various business units within an organization; often through the establishment of an information security steering committee.
- **A lack of applied specialized skill and/or training** - Information security personnel have acquired specialized skills that are not found in an IT skill set. Some examples of skills not typically found in an IT skill set include; policy development, physical security, human resources security, risk assessment, and compliance. You can expect an IT administrator to be very effective in the administration of servers, users and the like, but we probably should not expect this same administrator to be effective in aligning information security strategy or defining risk.
- **A conflict of interest** - Information technology uses technology to enable and improve business efficiency. Information security is often not viewed as a business enabler (even though it can be) and is often not given proper priority or budget.
- **Significant physical and administrative risk** - We know that information security consists of administrative, physical, and technical controls. IT controls are most often technical controls. Administrative and physical controls are critical to the success of an information security program as well.

One of the many reasons we like to use and reference the ISO 27002 (17999:2005) is because it is a comprehensive and holistic standard. ISO 27002 accounts for risks and controls in the following areas of information security:

- Security Policy Management
- Corporate Security Management
- Organizational Asset Management
- Human Resources Security Management
- Physical and Environmental Security Management
- Communications and Operations Management
- Information Access Control Management
- Information Systems Security Management
- Information Security Incident Management
- Business Continuity Management
- Compliance Management

An effective information security program must be holistic to be effective. A failure to be holistic leads to many missed risks and a false sense of security.

Characteristic #3: Organized

One thing you can do to improve employee, contractor and temporary worker compliance with your information security program is to make it easier for them to navigate through all the components that make up your program. One of the best ways to organize your information security program is by providing continuity.

Characteristics of Effective Information Security Programs

- Continuity between policies – Policies should use the same graphics, fonts, and structure. It should be clear that your policy is your policy at first glance. Policies should reference other policies through the use of an “umbrella” policy such as “Corporate Information Security Policy.”
- Continuity between policies and supporting documentation – Use guidelines, standards and procedures to elaborate on policy with more direction. Policies should reference supporting guidelines, standards and procedures and vice versa.

Understand that less than 10% of employees, contractors, and temporary workers will ever read your information security policies. In a practical sense, policies are best used as reference and as such organization is critical. A more organized and accessible information security program is more successful in achieving compliance. Publish your information security program documentation for easy reference, preferably in an electronic format such as an intranet site.

Characteristic #4: Governed

You can write as many policies and procedures as you want, but they are hardly worth the paper they are written on without action.

Main Entry: **gov-ern**

Pronunciation: \ˈgə-vərn\

intransitive verb

1 : to prevail or have decisive influence : [control](#)

2 : to exercise authority

If a policy is law, then governance is the police and court. We have seen more than our share of companies write policy to satisfy regulatory and/or customer requirements, but fail miserably in area of enforcement. Enforcement requires constant monitoring, assessment, and follow-through. Use policies as they are meant to be used; as rules that must be followed at all times.

Characteristic #5: Formal

If your information security program or any portion thereof is not documented, it doesn't exist. Documentation provides concrete guidance and proof of your actions. Ask yourself a few questions, or come up with your own.

- Do you intend to work for your company forever? If not, then how do you expect anyone who fills your position to be able to manage what you have worked so hard to implement?
- Are you ever audited, or will you ever be audited by regulators or customers? If so, how do you plan to convince them that you do what you claim to do?
- Are you 100% positive that your company will never experience a breach of security that could lead to legal proceedings (prosecution or litigation)? If not, then how do you expect to demonstrate that you did everything you could to prevent the breach and/or practiced due care?

Many of us information security folks came up through the years as IT professionals. Everyone knows that IT professionals (for the most part) detest documenting what we do. Trust me; your documentation will save you and your company someday. On the flip side; your lack of documentation could lead to some seriously bad consequences for your career and the future of your company.

Characteristics of Effective Information Security Programs

Characteristic #6: Alive

It's alive! No really, it is. Information security is not a one-time and your done deal. It is a lifecycle of continuous development, monitoring, auditing/testing, management and improvement. Businesses change; people change; technologies change; threats change; everything changes. Your information security program must change too.

**About FRSecure**

FRSecure LLC is a full-service information security consulting company dedicated to information security education, awareness, application, and improvement. FRSecure works with businesses of all sizes, in all industries; enabling clients to achieve optimal results per every information security dollar spent. All of our clients are in business to make money, so we design secure solutions that drive business, protect sensitive information assets, and improve the bottom line.

Regulatory and industry compliance is built into our solutions. Our experience has shown that good information security equals compliance, not the other way around.

To read more about FRSecure, visit us online at <http://www.frsecure.com>.