

## FRSecure White Paper

# The Five W's of Information Security

Prepared By:  
Evan Francen, CISSP CISM  
Managing Partner  
FRSecure LLC  
[evan@frsecure.com](mailto:evan@frsecure.com)

Page 1

## Table of Contents

Table of Contents	2
Introduction – The Five W's of Information Security	3
What is Information Security?	3
Why do you need Information Security?	4
Who is responsible for Information Security?	6
When is the right time to address Information Security?	7
Where does Information Security Apply?	9
About FRSecure	10

## The Five W's of Information Security

## Introduction – The Five W's of Information Security

Thank you for your interest in this FRSecure white paper! This white paper is written to provide you, the reader with a basic understanding of information security concepts. The concepts presented here are based on a combination of industry best practices and the experience we have gained while helping dozens of companies secure their sensitive information. We use plain English wherever possible.

The Five W's of Information Security are:

- **What** is Information Security?
- **Why** do you need Information Security?
- **Who** is responsible for Information Security?
- **When** is the right time to address Information Security?
- **Where** does Information Security apply?

The target audience for this white paper is business leaders, employees, and the public. Use this white paper as a general reference and guide, not as a comprehensive information security manual.

## What is Information Security?

*Fundamentally, information security is the application of **Administrative, Physical, and Technical** controls in an effort to protect the **Confidentiality, Integrity, and/or Availability** of information.*

In order for us to understand this statement, we have to gain an understanding of some well established information security concepts; Administrative Control, Physical Control, Technical Control, Confidentiality, Integrity, and Availability. We'll start with the controls

**Administrative Control** - Address the human factors of information security. Typically administrative controls come in the form of management directives, policies, guidelines, standards, and/or procedures. Good examples of administrative controls are:

- Information security policies
- Training and awareness programs
- Business continuity and/or disaster recovery plans
- Hiring and termination procedures

**Physical Control** - Address the physical factors of information security. Physical controls are typically the easiest type of control for people to relate to. Physical controls can usually be touched and/or seen. They control physical access to information. Good examples of physical controls are:

- Locks
- Fences
- Building alarm systems
- Construction materials

**Technical Control** - Address the technical factors of information security. Technical controls use technology to control access. Much of the information we use everyday cannot be touched, and often times the control cannot be either. Good examples of technical controls are:

- Firewalls

### The Five W's of Information Security

- Access control lists
- File permissions
- Anti-virus software

Easy enough, right? Some controls are meant to prevent an event from occurring; some are meant to detect when an event has occurred; and some are meant to help restore (or correct) things to normal after an event has already occurred. Thus, we have *Preventive*, *Detective*, and *Corrective* controls. These controls are somewhat self-explanatory. Let's pair these controls with the three mentioned earlier.

- Preventive/Administrative - ex. Background checks, training, policy, etc.
- Detective/Administrative - ex. Performance reviews, drug screening, etc.
- Corrective/Administrative - ex. Disciplinary procedures, incident response procedures, training, etc.
- Preventive/Physical - ex. Locks, building layout and construction, fences, etc.
- Detective/Physical - ex. CCTV surveillance, alarm systems, etc.
- Corrective/Physical - ex. Guards, fire suppression, etc.
- Preventive/Technical - ex. Access control lists, authentication, firewalls, etc.
- Detective/Technical - ex. Intrusion detection systems (IDS), anti-virus software, logs, etc.
- Corrective/Technical - ex. Backups, standard builds, snapshots, etc.

A single control can serve more than one need and fit more than one type. These are the basic types of controls used to protect the Confidentiality, Integrity, and/or Availability of information, which is the second part of our definition

*Fundamentally, information security is the application of **Administrative, Physical, and Technical** controls in an effort to protect the **Confidentiality, Integrity, and/or Availability** of information.*

**Confidentiality** - In essence, keeping information secret and only allowing disclosure to authorized entities. The classic military "need-to-know" principle applies pretty well. Think of the information that could cause harm to you or your company if it were given into the wrong hands.

**Integrity** - Ensuring that information is accurate. If a company's inventory systems report 50 units are available, there should be 50 units physically available. This is a very simple example of external integrity.

**Availability** - Ensuring that information is available when it is needed (by an authorized entity). When feasible, information needs to be available following a disaster or incident. Business continuity plans, disaster recovery plans, and incident response plans are all tied to availability.

Information security people like to use acronyms as much as anyone else, so we use **C.I.A.** to refer to Confidentiality, Integrity, and Availability. The opposite is **D.A.D.**, Disclosure, Alteration, and Destruction.

## Why do you need Information Security?

This is sometimes tough to answer because the answer seems obvious. No? Read on.

As we know from the previous section, information security is all about protecting the confidentiality, integrity and availability of information. Answer these questions:

- Do you have information that needs to be kept confidential (secret)?

### The Five W's of Information Security

- Do you have information that needs to be accurate?
- Do you have information that must be available when you need it?

If you answered yes to any of these questions, then you have a need for information security. Maybe you're expecting more. Let's go back to our three questions above.

Do you have information that needs to be kept confidential? Or accurate? Or available? You likely answered yes if your company has any or all of the following:

- Intellectual property
- Financial data
- Personally identifiable information (Social Security Numbers and the like)
- Personal Health Information
- Business Intelligence
- Future planning information

You can add to the list as you see fit. We would be hard pressed to find a company that doesn't have information that needs to be protected. The lack of control (security) often has an impact on the bottom line (your profits), which leads us to consequences.

The consequences of poor information security can include:

- Civil penalties - individual, class-action, and/or regulatory
- Lost opportunity - intellectual property loss, marketing plan loss, competitive advantage, missed deadlines and service level agreements (SLAs)
- Damaged corporate image - embarrassing media coverage, lost consumer confidence, and identity theft, and;
- Criminal penalties (it's only a matter of time)

We usually use consequences as a last resort to justify the existence of information security.

Reality is what it is, but can information security actually provide value to a business beyond protection? Absolutely! An effective information security program translates into formalized processes and improvement, which leads to efficiencies, which leads to greater profits for your company. Effective information security programs reduce risk and improve efficiency. Let's take one real-life example...

A client needed to send large files containing sensitive information to a vendor of theirs on a regular basis. The personnel sending the large files knew that it would be infeasible (and potentially risky) to send them through email, so they decided to burn the files to DVD and ship the DVDs to the vendor. Nobody knew this was happening except for the business unit personnel responsible for getting the files to the vendor.

The company hired FRSecure to conduct an information security (sometimes called risk) assessment. During the assessment this practice was identified and reported as a significant risk. The risk was reported as "High" due to the fact that the files contained sensitive intellectual property and clinical trial data. *On a side note, you do conduct regular independent information security assessments at your company, right?* Needless to say, the risk was unacceptable to management.

If a risk is unacceptable as is, then we need to mitigate (or transfer) the risk. The risk mitigation strategy in this instance was to devise a "secure" method of transferring the files to the vendor online. The company purchased and installed an SFTP/HTTPS server that allowed files to be transferred online securely (i.e. encrypted, authenticated, etc.). The added benefit was the fact

### The Five W's of Information Security

that the process could now be automated which significantly improved efficiency. The company saved up to 30 FTE hours per week because there was no longer the need to copy files, burn DVDs, and mail DVDs to vendors. The SFTP/HTTPS solution paid for itself within 10 weeks! The improved efficiency translated to less expense, which translated into increased profit.

Let's sum this up. Why do we need information security?

We need information security to reduce the risk of unauthorized information disclosure, modification, and destruction. We need information security to reduce risk to a level that is acceptable to the business (management). We need information security to improve the way we do business.

## Who is responsible for Information Security?

This is an easy one. Everyone is responsible for information security! A better question might be "Who is responsible for what?"

We'll tackle this from two perspectives. The first is a top-down approach, and the second is a role-based, data-centric approach. Both approaches should be used simultaneously, not one in lieu of the other.

### Top-down Approach

#### Senior Management

First off, information security must start at the top. The "top" is senior management and the "start" is commitment. Senior management must make a commitment to information security in order for information security to be effective. This can't be stressed enough. Senior management's commitment to information security needs to be communicated and understood by all company personnel and third-party partners.

The communicated commitment often comes in the form of policy. Senior management demonstrates the commitment by being actively involved in the information security strategy, risk acceptance, and budget approval among other things.

Without senior management commitment, information security is a wasted effort.

#### Business Unit Leaders

Keep in mind that a business is in business to make money. Making money is the primary objective, and protecting the information that drives the business is a secondary (and supporting) objective. Information security personnel need to understand how the business uses information. Failure to do so can lead to ineffective controls and process obstruction.

Arguably, nobody knows how information is used to fulfill business objectives more than employees. While it's not practical to incorporate every employee's opinion into an information security program, it is practical to seek the opinions of the people who represent every employee. Establish an information security steering committee comprised of business unit leaders. Business unit leaders must see to it that information security permeates through their respective organizations within the company.

#### Employees

All employees are responsible for understanding and complying with all information security policies and supporting documentation (guidelines, standards, and procedures). Employees are responsible for seeking guidance when the security implications of their actions (or planned actions) are not well understood. Information security personnel need employees to participate, observe and report.

## The Five W's of Information Security

### Third Parties

Third parties such as contractors and vendors must protect your business information at least as well as you do yourself. Information security requirements should be included in contractual agreements. Your right to audit the third-party's information security controls should also be included in contracts, whenever possible. The responsibility of the third-party is to comply with the language contained in contracts.

### Role-Based Approach

A good and creative information security professional can apply the top-down approach mentioned above with our other approach; the role-based approach. The role-based approach is more data-centric and is comprised of three roles. The three roles are Data Owner, Data Custodian, and Data User.

#### Data Owner

The Data Owner is normally the person responsible for, or dependent upon the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

- The Data Owner determines the appropriate value and classification of information generated by the owner or department;
- The Data Owner must communicate the information classification when the information is released outside of the department and/or company;
- The Data Owner controls access to his/her information and must be consulted when access is extended or modified; and
- The Data Owner must communicate the information classification to the Data Custodian so that the Data Custodian may provide the appropriate levels of protection.

#### Data Custodian

- The Data Custodian maintains the protection of data according to the information classification associated to it by the Data Owner.
- The Data Custodian role is delegated by the Data Owner and is usually Information Technology personnel.

#### Data User

The Data User is a person, organization or entity that interacts with data for the purpose of performing an authorized task. A Data User is responsible for using data in a manner that is consistent with the purpose intended and in compliance with policy.

No matter how you assign information security roles and responsibilities, just make sure that you DO assign roles and responsibilities! Define specific information security roles and responsibilities and be sure to do so formally. Add information security responsibilities in policy, job descriptions, and wherever else you see fit. Responsibility leads to accountability and accountability leads to enforceability.

## When is the right time to address Information Security?

On the surface, the answer is simple. The right time to address information security is now, always, and all of the time.

There are a couple of characteristics to good, effective information security that apply here.

### The Five W's of Information Security

**Information security must be holistic.** Information security is not an IT issue any more or less than it is an accounting or HR issue. Information security is a business issue. A disgruntled employee is just as dangerous as a hacker from Eastern Europe. A printed account statement thrown in the garbage can cause as much damage as a lost backup tape. You get the picture. Information security needs to be integrated into the business and should be considered in most (if not all) business decisions. This point stresses the importance of addressing information security all of the time.

**Information security is a lifecycle discipline.** In order to be effective, your information security program must be ever changing, constantly evolving and continuously improving. Businesses and the environments they operate in are constantly changing. A business that does not adapt is dead. An information security program that does not adapt is also dead. This is just another point to stress the importance of addressing information security all of the time.

Perhaps your company hasn't designed and/or implemented an information security program yet, or maybe your company has written a few policies and that was that. When is the right time to implement an information security program? When is the right time to update your existing program?

You have the option of being proactive or reactive.

Proactive information security is always less expensive. Less expensive is important if your company is into making money as most are. Don't take my word for it, let's use an example. Arguably the most common source of breaches is a lost or stolen laptop computer. 21% of all breaches reported in the Open Security Foundation's [DataLossDB](#) come as a result of a lost or stolen laptop, compared with 16% from hacking (or cracking).

**Situation:** A laptop is stolen from an outside salesperson's car. Stored on the laptop's hard drive is an Excel spreadsheet containing approximately 15,000 customer records. It is not known if the spreadsheet contains Social Security Numbers, but it is known that the database from which the data comes from does. It is feasible (and probable) that the spreadsheet does contain Social Security Numbers. The laptop computer was not encrypted.

The average cost of a breach like this, according to the Ponemon Institute, is \$202 per lost record. Do the math and it appears as though this breach could end up costing the company over \$3,000,000! The costs include consulting fees, attorney fees, customer notification, call center support, media management, credit monitoring, regulatory fees, and state/federal fines or fees.

Had the company taken a proactive approach to information security it would have likely identified the actions that led to this breach to be an unacceptable risk. Furthermore, a proactive company would have likely mitigated this risk. The costs of proactive security and implementation of mitigating controls would have been considerably less than \$3,000,000! A preventative control such as full-disk encryption would cost less than \$150 per laptop.

The example outlined above is hypothetical; hypothetical but based in reality and backed-up by some statistical data. The fact of the matter is that breaches happen and information is lost every day. Companies that make the investment of time and money into information security based upon the risks come out ahead in the long term.

In conclusion, the right time to address information security is now. Companies have learned time and time again that;

1. Proactive information security is less expensive than reactive information security; and,
2. Information security takes a long-term, continuous commitment.

## The Five W's of Information Security

Don't wait for something bad to happen.

### Where does Information Security Apply?

You may recall from our definition in “*What is Information Security?*”, that fundamentally information security is:

*the application of Administrative, Physical, and Technical controls in an effort to protect the Confidentiality, Integrity, and Availability of information.*

We could have made the definition more accurate by adding the word “**holistic**” before the word application.

(adj) **holistic** (emphasizing the organic or functional relation between parts and the whole);  
Source: Princeton WordNet

In order to gain the most benefit from information security it must be applied to the business as a whole. A weakness in one part of the information security program affects the entire program. Now we are starting to understand where information security applies in your organization. It applies throughout the enterprise.

#### Information Security is NOT and IT Issue

It IS a business issue. The thought that information security is an IT issue is a common misconception that has prevailed for years. Evidence of this can be found in where many companies align information security. Information security often reports up through the IT organization to the Chief Information Officer (CIO). Smaller companies often rely on their information technology consultants for information security guidance. So, what's the problem?

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, and electronic. A well-run IT department will often align technology with the business, but not necessarily information security.
- **A lack of 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.
- **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.

Some examples of unaccounted for risks in IT-centric information security programs\*:

- **Information security training and awareness** - The most effective way to get your organization's information is to ask you (or an employee) for it. Employees need to be made aware of information security and integrate it into their daily work. Social

### The Five W's of Information Security

- engineering, employee mistakes, and risky behaviors introduce serious risks to employees and the organization they work for.
- **Human resources security** - Hiring and termination practices, the on boarding process, personal information handling, and disciplinary actions should all be assessed for risk, but are often missed.
  - **Physical controls** - Tailgating, alarm systems, environmental controls, and external security.

\*a very small representation of risks. An FRSecure [information security assessment](#) may evaluate 1000 or more risks, depending on the organization being assessed.

Where does information security apply? It applies throughout your organization.

An [information security assessment](#) will help you determine where information security is sufficient and where it may be lacking in your organization.

## 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>.