Dopkins & Company, LLP

CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Information Systems Security:

The Missing Piece of the Puzzle

OVERVIEW

Think of your business as a jigsaw puzzle. There are many pieces that go into the puzzle, and each piece needs to be situated just right if you're to be successful. Undoubtedly, your business will have a piece that represents your customers, another for employees, and perhaps, one for a product line or service offering. Now, in addition to the three pieces just listed, there are countless other pieces that are almost always noted by individuals; however, there is one piece that is often omitted.

Think of this omitted piece as the center of the puzzle. It is one of the most difficult pieces to identify quickly, but without it, your puzzle will remain incomplete. As you may have already gathered, this piece that is often missing is that of information security. In this whitepaper, you will learn about information security and its components, including why many information security programs are unsuccessful. The paper concludes with a self-assessment that can be used to determine if your organization is currently at-risk for an information security incident.

Table of Contents

What is information security?

Information Systems Security: The Missing Piece of the Puzzle

Think of information security as an asset

Although it doesn't appear directly on a balance sheet, information is an asset that, like other business assets, is essential to an organization's success. As such, it is imperative that information is properly safeguarded from threats, both external and internal.

Information is unique in that it can exist everywhere

Unlike other assets, information is unique in that it can exist in many forms. Information can be handwritten, printed, stored electronically or on film, and it can even be spoken. Such a wide array of media lends itself to an environment exposed to a multitude of threats, including those that are intentional or unintentional, external or internal.

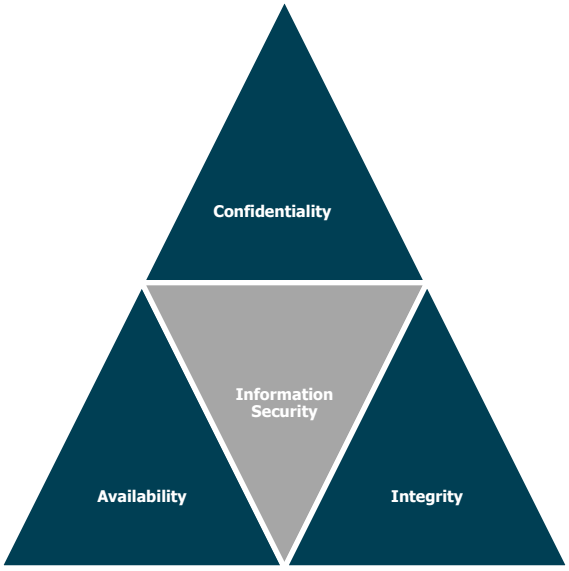
Information security is needed to protect information from threats

Due to the wide array of threat exposure concerning information, information security is needed to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Security is more than just protection from unauthorized access

When discussing information security, many are quick to assume that this simply means protecting information from unauthorized access, but information security is much more than that. In addition to protecting information from unauthorized access, information security is also needed to protect information from unauthorized:

- Disclosure
- Disruption
- Destruction
- Inspection
- Modification
- Perusal
- Recording
- Use



A key aspect of information security is to preserve the confidentiality, integrity and availability of an organization's information.

Where does IT security fit in?

Laptops, flash drives, smartphones and cloud-computing represent a few of the technological innovations that have increased the need for proper information security

Just because you can't see it, doesn't mean it can't hurt you

Whether we like it or not, information technology pervades every aspect of daily life in the 21st century. Collectively, we use technology to communicate and collaborate, manage operations and finances, to access and deliver information, and ultimately, to increase efficiency. Yet, despite the unquestionable importance of information technology, it continues to operate in the background of organizations. That is, it exists, we expect it to work with absolute logic and speed, and it is not until something goes wrong that we begin to take notice. Now, despite our wishes to the contrary, information technology is not infallible. Problems will occur, and ignorance is bliss, but at what cost to your organization.

The risks associated with technology are constantly evolving

Over the past 10 years, the pervasiveness of technology has exceeded most expectations. With laptops, tablets and now, smartphones, the field of information technology is constantly evolving, and businesses both large and small are beginning to take advantage of the benefits that can be derived from such technologies; however, the risk factors associated with these technologies are often not properly addressed.

What are the risks of not protecting your information?

Cyber risks are not only generated by outsiders

Breaches of privacy, heavy financial losses, and in extreme circumstances, even the downfall of corporations can be attributed to companies' inability to protect themselves from cyber-risks. Materializing both externally and internally, cyber-risks can be generated by a multitude of perpetrators. In the movies, the individual responsible for a data breach is often a highly trained evil-doer, who goes to great lengths to breach security; however, in the real world, most cyber-security breaches can be attributed disgruntled employees, or more commonly, just simple mistakes and a lack of awareness.

To better understand the nature behind a data breach, let us first consider what a data breach is. In the most basic sense, a data breach is any incident wherein confidential data may have been viewed, stolen or used by unauthorized individual. Notice, this definition is not concerned with how, who or to what degree, as this is inconsequential.

Many organizations are unaware if they are at risk

As you can see on the table to the right, it is interesting to note the percentage of attacks which were avoidable through simple controls, in addition to the manner that breaches were discovered. First, the ease in which attacks were conducted indicates that many companies do not have the proper preventative controls in place to avoid such an attack.

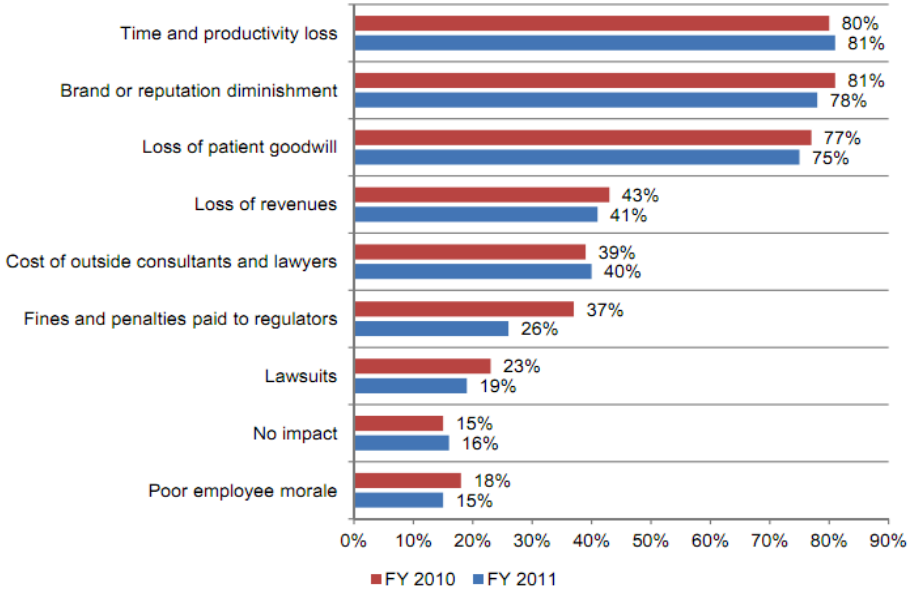
Then, in regard to breach discovery, the high prevalence of 3rd party discovery in the weeks following the breach demonstrates a lack of detective controls that are necessary to minimize the damage caused by the attack. Such an apparent lack of preventative and/or detective controls reiterates the notion that many organizations are not aware of their current IT security risk exposure. That is, your organization may be at risk and you do not even know it!

WHAT COMMONALITIES EXIST?	
79%	of victims were targets of opportunity
85%	of breaches took weeks or more to discover
92%	of breaches were discovered by a third party
97%	of breaches were avoidable through simple or intermediate controls

Source: Verizon 2012 Data Breach Investigations Report

Information Systems Security: The Missing Piece of the Puzzle

Bar Chart 9: What best describes the negative impact of data breach incidents experienced by your organization over the past two years?
More than one choice permitted



Notice, for organizations that have experienced a data breach, the top three negative impacts were unrelated to the direct costs of the breach.

Source: Ponemon Institute – "Second Annual Benchmark Study on Patient Privacy & Data Security"

HIPPA, HITECH & PCI Data Security Standards

In certain industries, a lack of awareness such as that previously discussed can lead to a violation of information security legislation and standards that have been passed. For example, those in the healthcare industry are required to comply with the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Health Insurance Portability and Accountability (HIPAA) Act, and in some instances, the Payment Card Industry (PCI) Data Security Standards. Failure to comply with any of the previously mentioned legislation and standards can result in significant fines being levied upon an organization.

Fines should be the least of your concerns

While the aforementioned standards and regulations do not apply to all companies, the need to mitigate such risks as a means to safeguard treasured assets and protect customer information applies to all businesses. As such, it can be said that proper information security is not only needed to comply with ever changing regulations, more so, information security is essential to avoid a loss of customers, capital and corporate value.

Why are many information security programs unsuccessful?

Increasing your awareness is the first priority

Despite not being aware of the information security risks facing their company, many organizations have started to increase security spending; however, increased spending does not necessarily equate to enhanced security – as many firms are now discovering. That is, when attempting to find the solution to a problem, it is logical that the identification of the problem is the first step of the process. For many, this first step represents a significant challenge for their organization. With limited knowledge surrounding information security, how can one begin to tell if their organization is adequately protected? Depending on your current standing, the answer may lie in utilizing the expertise of an outside firm, or possibly, a self-review process may be all that is required. Regardless of which solution is used, the ultimate goal is to increase awareness prior to implementing an abundance of controls.

It's possible to have too much of a good thing

For every conceivable threat to an organization, there is a multitude of safeguards that can counter that threat to some extent. Now, the solution isn't to enact every available countermeasure, as doing so would not prove to be cost effective. More so, an organization should take a risk-based approach to determining the security controls that will reduce the threat to an acceptable level. While taking a risk-based approach to determining controls is ideal, the scope of such a process can prove daunting. It is for this reason that before conducting a risk assessment, it is strongly suggested that companies first ensure that they are prescribing to "minimum" information security standards.

Aside from the obvious cost burden, implementing too many controls can slow down business processes and have a negative effect on your business.

Information Systems Security: The Missing Piece of the Puzzle

In essence, such a program is akin to locking the front door of your home, but leaving the windows wide open.

Focusing on just one piece of the puzzle often leads to failure

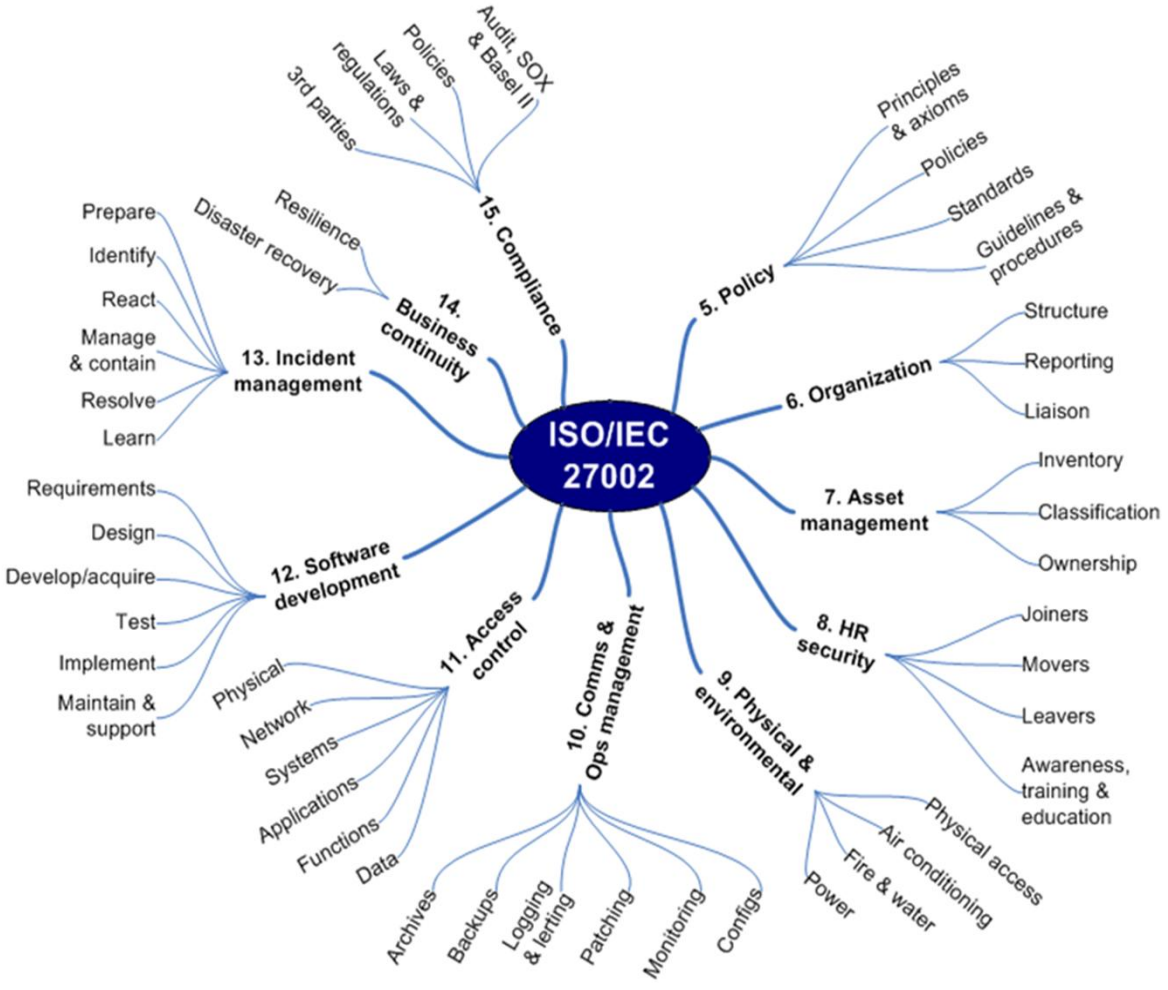
Despite the inherent ubiquity of information, some enterprises view information security in isolation, perceiving it to be someone's else responsibility. In general, organizations typically place this responsibility on the shoulders of their IT staff, as they believe information security is solely a technical discipline; however, this practice often leads to information security programs that do not align with enterprise goals and priorities.

As a result, such programs bring little value to the organization and are deemed unsuccessful. Why are these programs unsuccessful? It is because they need a larger framework to bring them in line with business objective .

For example, although a critical component of information security, information technology security is only one piece of the puzzle. Therefore, by just focusing on information technology, the processes and people unique to your organization are ignored.

Information Systems Security: The Missing Piece of the Puzzle

The ISO/IEC 27002 standard covers a wide array of topics, thereby ensuring that your company is covered from all angles.



Focusing on just one piece of the puzzle often leads to failure

While we have previously discussed such standards as those that apply to HIPAA and the Payment Card Industry, there exist more high-level standards which encompass a larger scope. An example of such a standard is that of ISO/IEC 27002, an internationally recognized standard for Information Security controls. With over 200 specific control issues, the ISO standard is an excellent resource for businesses concerned about information security.

The Dopkins nVISIOND process is a unique combination of your knowledge of your business, and our knowledge of information security controls and how they work together.

Think of a security review as an enterprise-wide project

Undergoing an ISO 27002 security review should not be viewed as an IT project; more so, it should be viewed as an enterprise-wide project, wherein relevant people from all business units should take part. Taking such a holistic approach can ensure that your organization is protected from the biggest risks, both IT and non-IT related.

How can you tell if you're at risk?

The following general questions have been provided to assist you in determining where your organization currently stands in regard to information security:

Does your organization have an Information Security Policy, which is approved by management, published and communicated as appropriate to all employees?

Are policies and procedures in place regarding the transfer, removal, disposal, and re-use of electronic media?

Are users required to utilize passwords that are at least 8 characters in length, which includes a combination of alphanumeric and special characters?

Does your organization have a current, up-to-date, and communicated disaster recovery and emergency mode operations plan and have they been tested recently?

Are employees trained and aware of the information security policies and procedures they are required to adhere to?

Did you know that by answering no to any one of these questions, your organization is considered to be at risk for a data breach?

Four key takeaways

Information Systems Security: The Missing Piece of the Puzzle

Action not reaction needed to avoid disaster

When concerned with information security, many organizations take the approach that in order for there to be an issue, there must first be an event. That is, if no information security issues has presented itself, then there must be nothing to worry about. The problem with this stance is that many information security incidents are not discovered until weeks or months after the incident's occurrence, and even then, the discovery is often made by a third party. To prevent such a disaster from occurring, it is imperative that organization's begin to take a proactive stance when evaluating and implementing an information security program.

Improving information security awareness should be your first priority

Now, before implementing a litany of control measures, it is important to first improve awareness at your organization. Primarily, focus should be placed on gaining an understanding of your business processes and the manner in which information travels across your organization. Gaining such knowledge is of critical importance when deciding what controls must be in place at your organization.

Defense in-depth is critical to a program's success

Due to budgetary and time restrictions, many organizations often choose to implement an abundance of reactive controls in place of proactive controls. Reactive controls, although necessary, must be complemented by proactive measures if an organization is to avoid a information security incident. Essentially, it is more beneficial to utilize a small amount of controls in a wide range of areas, as opposed to a large amount of controls in one specific area.

Ask for help

Understandably, the challenges associated with evaluating an information security program can prove to be daunting. On a micro-level, the verbiage used in certain standards can be challenging to comprehend due to their technical nature. Additionally, on a macro-level, when performing a self-review, it can be difficult to maintain objectivity throughout the process. If at any time you feel overwhelmed with the material or unsure where to begin, do not hesitate to call and ask for help before it is too late.

Contact:

William Prohn, CISSP

Managing Director

(716) 634-8800

wprohn@dopkins.com

www.dopkins.com