INFORMATION SECURITY FOR SMALL BUSINESSES

Part 1 *- Information Security Framework*

Strategies For Protecting Small Businesses From Today's Cybercrime Threats.

Cyrus J. Walker,
Managing Principal,
Data Defenders , LLC

January, 2015

TABLE OF CONTENTS

ABOUT THE AUTHOR

Cyrus J. Walker is Founder and Managing Principal at Data Defenders, LLC, a business-to-business professional services company providing information assurance, election system auditing, infrastructure management, and software development solutions to local, state, and federal agencies as well to the corporate sector.

Cyrus is an experienced Information Security industry executive with a diverse technology background. He has served, or is currently serving, in several executive-level capacities in the commercial and academic sector of the Information Security and Computer Forensics industry.

Cyrus pioneered the concept of Applied Computer Forensics and related forensic analysis models and processes that are now being used by Data Defenders to aid election jurisdictions in ensuring the operational integrity of the their electronic voting systems. Cyrus has been providing election system auditing solutions to the election jurisdiction marketplace since 2007 and has a diverse technical background including expertise in Data Communications, Information Security, and Computer Forensics.

In addition to his responsibilities at Data Defenders, Cyrus served as a subject matter expert on Computer Incident Response Management in the Cyber Defense Analysis Center at the University of Arkansas funded and directed by the U.S. Department of Homeland Security. He also served as chairman of the Computer Security and Computer Forensics department at the Wilbur Wright College, one of the City Colleges of Chicago.

Cyrus's theoretical work on the topic of Modeling, Analysis and Simulation of Computer and Telecommunications Systems has been published in the IEEE journal (1997). His work on Applied Computer Forensics for Election System Auditing was published in the EVOTE - 5th International Conference on Electronic Voting Conference Journal (Bregenz, Austria - 2012). .Additionally, in 1995 President Bill Clinton recognized him for his groundbreaking work and leadership in the telecommunications industry.

Cyrus holds a Computer Forensics Examiner certification from *the Information Assurance Certification Review Board* and possesses a unique technical background in network architecture and design, disaster recovery, information security, and computer forensics.

INTRODUCTION

The information age is now. Information detailing every aspect of our lives and businesses can be readily accessed from the palm of our hand in the form of smartphones, tablet computers, and wearable technologies. Businesses, large and small, are now able to connect with and conduct business with anyone anywhere in the world in a matter of seconds. Small businesses are now able to reach potential consumers and markets locally, nationally, and globally, more quickly and effectively than ever before. To reach these markets, small businesses have come to rely on and directly integrate technology into their business infrastructures to enable this capability but with this integration and reliance, comes an expanded risk to the business overall. It has allowed small businesses to perform and deliver services to regions throughout the world that previously required a local presence to do so. Businesses in retail, professional services, manufacturing, and healthcare, for example, can now effectively provide services to consumers in other regions and compete with larger businesses doing so. How can small businesses do this? Through technology!

With this increased connectivity comes a greater exposure to those with malicious intentions seeking financial gain through acquisition and misuse of this information. Information that was once kept in file cabinets under lock and key and only accessible on-site by a handful of people with the proper authorization and credentials, can now be accessed anywhere in the world by anyone with the means, the talent, and the expertise to covertly usurp countermeasures meant to keep data private and accessible only to those granted the authorization to do so.

Today's Cybercrime, which threatens the privacy of our information, has evolved from destructive objectives where the goal was to delete and destroy that information for ego-centric purposes to financial objectives today where the goal is now to earn money. Maliciously minded individuals have realized that cybercrime can be more lucrative by deploying malicious code that encrypts data, making that data inaccessible to its owner, then ransoming that data back to the victim for a "small" fee. Ransomware, as this scheme is known by, is malicious software used for encrypting data and is a new and growing trend primarily targeting small businesses. A recent small business data security study conducted by an international telecommunications provider concluded that "***65% of security all related attacks are directed at small businesses with less than 100 employees."***

Why? The primary reason is that small businesses generally lack the ability, resources, skills, and deployed countermeasures to properly protect their digital infrastructures from these kinds of attacks. Small businesses are basically sitting ducks. To deal with this expanded risk, small businesses must recognize information security now as a business imperative; as important as managing the business' finances.

To facilitate small business' expanded thinking and awareness around the importance of information security; Data Defenders developed this white paper series, ***Information Security for Small Businesses,*** with the goal of presenting key concepts in information security from the perspective of the small business. The goal of this series

is to dispel any false beliefs that information security risks don't exist at the small business level or that small businesses don't have the resources, knowledge, or capability to effectively protect themselves from threats to their digital infrastructure or business.

The ***Information Security for Small Businesses*** white paper series will focus on topics ranging from the information security framework to implementing technical countermeasures and provide simple ideas and strategies that can help the small business raise their security profile.

Part 1 of this series; ***Information Security Framework;*** introduces the building blocks that constitute a simple but strong information security architecture and program that can be used by the small business to strengthen its security profile. Each installment in this series will cover one component of the framework defined in this first installment and provide more in-depth insight into the component to arm the reader with the information necessary to mitigate the risks to its digital infrastructure.

Data Defenders strongly believes that if small businesses implemented simple, affordable strategies as outlined in this white paper, they can significantly increase their security profiles and drastically reduce the growing and alarming trends of malicious attacks against them.

STRATEGIES FOR INCREASING THE SMALL BUSINESS SECURITY PROFILE

Strategies for small businesses to protect themselves against cybercrime related activities don't differ that much from the strategies large businesses employ. The overall framework is the same and is integral to mitigating the risks and threats that both business classes deal with on a daily basis. The differences really manifest in the magnitude of the solutions between the small and large business levels which is determined by the size and complexity of the digital infrastructure under consideration. The framework of the strategy breaks down to the following:

- **Addressing, Defining, & Enforcing Behavior**
- **Creating & Expanding Awareness**
- **Assessing & Implementing Technology**

Some technical circles like to refer to this framework as people, process, and technology and while this is the more formal reference to the framework, the aforementioned reference is much easily understandable for small businesses because it defines the framework as actionable objectives.

Behavior & Awareness

Addressing, defining, & enforcing behavior and creating & expanding awareness we will consider as the first part of the framework. Both are closely related and while they each have different objectives, the behavior of the small business does have a major impact on its security awareness level. First, in order for a business to increase its security profile, it must change its behaviors related to technology and information usage. Most small businesses don't think they could ever be a target of malicious activities such as having a security breach from the internet. They have the mindset that they are a very little fish in a very large pond. "Who would ever find us and why would anyone waste their time breaking into our systems?" is a common line of thinking among small business owners. What they don't realize is that the technology does exist for their digital infrastructure to be easily detected and easily exploited if their digital infrastructure is not adequately protected. Behavior is the core reason that a company's security profile is weak and inadequate. Behaviors such as how people access, share, and use information, how they assess technologies to be incorporated into their digital infrastructure, and who they allow access to, their digital infrastructure and information will, to a large degree, determine their overall security profile. Generally, in most businesses, there is no specific behavior defined but a behavior does exist and it typically is not aligned with the expectations of the business. Most behaviors that exist related to technology and information usage were created based on need which did not consider the idea of security at all. These behaviors were generally developed in an adhoc way over time and continued unchecked because the need of the business

function greatly overshadowed the need for security. Small businesses must recognize that information security is as important to the business as managing its finances, for lack of this recognition could literally lead to its demise.

So, the first behavior that must be incorporated into the business is the consideration that information security is an integral part of the business operation. Improving the company's security profile starts with asking and answering the Who, What, Where, When, Why and How of technology usage and information access and must be constantly considered in the daily business operations. The following are some questions that should be asked and answered to begin the process of creating an information security program for your business.

Who
- *needs to have access to our information?*
- *has been accessing our information?*

What
- *is the security profile of the technologies we need to run our business?*
- *information needs to be accessed?*

Where
- *is this information going to be stored?*
- *are the people that are going to be accessing our information?*

When
- *will our information be accessed?*
- *will the need for this information begin and end?*

Why
- *does someone need to access our information?*
- *are we allowing access to our information?*

How
- *will someone gain access to our information?*
- *could someone penetrate our security architecture to gain access to our information?*

Once these questions have been addressed, the small business is now ready to begin the process of changing the organization's behavior. One way to effect change in the behavior of a small business is by simply defining and implementing an Acceptable Use Policy (AUP), ensuring that all employees are aware of and have accepted this this policy as well as implementing technical controls that can enforce the AUP. Implementing an AUP can deter, prevent, and protect against a lot of internal technology and information usage behaviors that could weaken a small business' overall security profile. There are many templates for AUPs on the internet that can be downloaded and tailored to address the particular and specific needs of the business. This activity can be completed at almost no cost to the business. However, implementing an AUP is not enough. An equally important part is the enforcement of the AUP. The AUP will never have the effect of changing behavior if the AUP is not constantly enforced. Lack of enforcement sends the message that the leadership of the business is not serious about their information security concerns and therefore, the behavior that has created the information security concerns in the first place will never change. It is the business' leadership that is responsible for establishing and setting the tone of the culture in the business and part of this culture must include enforcement of policies such as the AUP that will bring about the expected change in behavior.

Changing the business' behavior leads to an increased sense of awareness of the threats and risks against the business' digital infrastructure and how the business' behavior reduces or increases its vulnerability to those threats and risks.

Technology

The second part of the framework is implementing security countermeasures that can enforce the AUP and protect the small business' digital infrastructure from both internal and external cybercrime threats. Security countermeasures such as small office firewalls, intrusion detection software/systems, virus and malicious code detection software, data backup and restoration solutions as well as event monitoring are all important to protecting the small business' digital infrastructure. All of these technologies can be implemented for less than a few hundred dollars and, in some cases such as the intrusion detection software, can be acquired at no cost but can significantly increase the overall security profile of the small business. However, some of the security technologies mentioned here will require some skill to configure and manage. The good thing about the internet is that you will find information, and even training videos on Youtube, that will provide information on how to configure and manage these devices or software.

User account and password management as well as operating system and application patch management also play a significant role in protecting the small business from cybercrime related activities. Implementing strong password standards as well as requiring passwords to be changed frequently can help to minimize unauthorized access to systems, applications, and information. Solutions such as password tokens or Bio-password software can provide inexpensive ways to implement strong password management functions and help to change the behavior of weak password management in a small business. Also, ensuring that servers and desktops have the minimum number of user accounts enabled on them and regularly auditing the access logs for those user accounts is a necessary way to track system and application usage, at least for those critical servers and desktops. Operating system and application patch management can help to ensure that any known security vulnerabilities are closed. Patch management can be done at no cost to the organization just by simply downloading and installing software patches created by the software manufacturers. This should be done on a regular basis.

Event Monitoring

One of the most often overlooked and underutilized security countermeasures for protecting a digital infrastructure is…….MONITORING. One of the other contributing factors for cybercrime related activities is that most businesses have no clue what's really going on in their digital infrastructures. Being able to know who is doing what both internally and externally to the small business digital infrastructure is paramount to protecting the business. Implementing the function of monitoring will provide the business with the capability of knowing who is accessing the business' data, applications, and systems at all times. Being able to determine if that access is

authorized or unauthorized can allow a business to mitigate any threats quickly. Most incidents don't happen overnight. Most of the incidents that do occur take time to execute. Reconnaissance is key to effecting malicious activity within the digital infrastructure of the business and that can take days, even months to conduct. It is highly likely that the business can detect such reconnaissance activities if it has some type of event monitoring function deployed. If a business can identify suspicious activities in its infrastructure early on, that positions the business to prevent that activity from having a negative impact on its operations.

Monitoring can be implemented by simple downloading and reviewing the logs from critical devices such as internet routers and firewalls, intrusion detection systems, servers, and some critical desktops that are central to the business' digital infrastructure. This can be achieved by exporting and loading these device logs into a spreadsheet tool such as Microsoft Excel and looking for IP addresses or port numbers that look out of place. If suspicious IP addresses or port numbers are found then access rules can be implemented in the Firewall and Intrusion Detection System to prevent further access from these suspicious IP addresses and port numbers, for example. Reviewing device logs can take some time to do but it will at least provide some insight into the activities happening within the company's digital infrastructure. A quicker, more efficient way to accomplish a log review could be to purchase log aggregation and correlation software known as Security Event Information Management or SEIM that can quickly provide a clear picture of transactions occurring both internally and externally from the company's network. SEIM software is inexpensive these days and can enable a company to effectively manage its digital infrastructure and detect and prevent potential cybercrime related events.

Incident Response Planning

What are you going to do should your business experience a security breach? Incident Response Planning or IRP helps to answer that question. Monitoring and Incident Response Planning go hand in hand and as with Monitoring, IRP is often neglected. Most of the attention in implementing and managing the small business' security profile focuses on the technology aspect but often neglects some important processes that help to prevent a security breach or minimize its impact on the company. IRP can help to minimize the negative impact of a security breach and can help the small business restore operations quickly. IRP focuses on defining the particular incidents that could have the most negative impact on its operations and defines plans for responding to those incidents. Having these pre-scripted and tested plans in place can mean the very survival of the business after an incident has occurred. To create these plans requires an understanding and definition of the small business' critical path, meaning, what business functions do we absolutely need for the business to operate daily? Once this critical path is defined, then the technology that supports the critical path can be identified. A general threat assessment can then be conducted for the technology the supports the business' critical path. Now don't get overwhelmed by the words "threat assessment". That just simply means asking the question "What events could cause these systems, applications, and information to suddenly become unavailable to the business?" Once those potential

events have been identified, the IRP should start with those potential events that have the highest probability of occurring and the plan should basically cover the following:

- **Who should be involved in the incident response process?**
- **How to communicate about the incident and to whom.**
- **How to collect data (evidence) about the incident.**
- **How to restore the affected systems and business operations.**
- **Conducting vulnerability remediation that led to the incident.**
- **Post review of the incident to improve the security profile and business operations.**

Once these basic parts of the IRP are completed, the small business will be well positioned to handle security incidents.

Internal vs. External Threats

Generally, most organizations focus on protecting themselves from the external threats, but the biggest threats that exists to their business are from the internal. Think about it…. those within the business have the most access and can do the most damage if they chose to. Research conducted over the years has consistently shown that approximately 80% of the security related incidents companies deal with occur as a result of employee behavior. Most organizations don't want to take the position of mistrust of their employees but this often leaves the organization extremely vulnerable to insider related security breaches. A number of the security countermeasures briefly mentioned above can be used to protect a small business from the internal threat as much as it can the external threat. Some of the strategies like monitoring and user account auditing can be used to mitigate this threat but listed here are some other ways that the small business can mitigate the insider threat.

- **When terminating an employee, deactivate all of their access and login credentials before terminating them.**
- **Implement compartmentalization strategies to minimize the sharing and unauthorized access of information. Compartmentalization requires approval to be granted before information can be accessed.**
- **Conduct regular log audits to track usage attempts and patterns of employees. This also helps to enforce the AUP.**

The insider threat can't be completed mitigated but it can be made very difficult to act on with these simple strategies.

CONCLUSION

There is really no secret potion, magic bullet, or pill that can be used to mitigate security threats to a small business. The business has to first realize that managing information security is as important and critical as managing the finances of the business. With this mindset, an organization is best able to take the next step in changing its behavior related to how technology and information is used. Lastly, the small business is then ready to implement the necessary technology to properly enforce appropriate behavior and protect the business' digital infrastructure. But it must first start with changing the mindset and behavior of the business. As I have always said….You can implement a Billion dollar security system but all it takes is one person within the business to give away the password to that system to render that Billion dollar system…useless!

For more information on our solutions, please visit our website at www.data-Defenders.com. Customer can also follow us on Facebook at http://www.facebook.com/pages/Data-Defenders-LLC/129964020394790 and Twitter at @DataDefenders.com.

WE ARE THE DEFENDERS OF YOUR INFORMATION WORLD! ™

Data Defenders®, LLC.

Corporate Headquarters:
University Technology Park at IIT
10 W. 35th St. Suite 9F5-1
Chicago, IL 60616
(WEB): www.data-defenders.com
(EMAIL): info@data-defenders.com

(MAIN): (312) 224-8831
(FAX): (312) 242-1795