Merchants
INFORMATION SOLUTIONS, INC.
Delivering World-Class Identity Theft &
Background Screening Solutions

Small Business ID theft and Fraud

An **Information Governance** Best practices Guide for Small Business

**It is not a matter of "if" but "when" an intrusion
will be attempted on your business computer system
in an effort to steal your customers' personal information**
John G. Iannarelli – Assistant Special Agent in Charge (ASAC) Phoenix FBI

eBook sponsored by:
Merchants Information Solutions
ID Theft Advisory Board

Small Business Information Governance Best Practices Guide

TABLE OF CONTENTS

Protecting your business means protecting your information

If you worry about your business becoming a victim of theft of sensitive information, you probably are concerned with some foreign hacker, sitting alone at a local cyber café in a faraway country, sipping on a latte while trolling for your company's internal secrets. Worse yet, perhaps you fear a hack being committed by a professional, sponsored by some rouge nation whose goal is to disrupt commerce within the United States, upsetting our economy while putting you out of business and Americans out of work. In the cyber world these types of hacks are attempted each and every day. However, the hack that you may worry the least about is the one most likely to occur. The computer intrusion your company will probably face is the one that will be committed by the hacker you already know.

Many of the computer intrusions against small to mid-size businesses come not from the foreign hacker, but rather the business competitor. In many of these instances the competitor hacker has obtained his advantage by hiring away one of your trusted employees who has insider knowledge. Or perhaps, it is one of your soon to be former employees who have decided to go into business for themselves. In either event, to guard against this danger there are steps you must take to not only ensure the hacker can be prosecuted, but also to make sure you are not forced out of business. Preferably your goal should be to stop the attack before it occurs.

Title 18, United States Code, Section 1030(4) (Fraud and related activity in connection with computers), provides that "Whoever knowingly and with intent to defraud, accessed a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the subject of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period". Therefore, to obtain law enforcement action if your computer system has been illegally accessed, you will need to be able to prove the element of intent as well as prove your system was "protected". While this is far less complicated when the hack is committed by a foreign third party, showing intent to commit a crime committed by a current or former employee can be far more difficult. Nevertheless, by putting into place some basic precautions the element of intent can quite easily be demonstrated. This is where a sound and implemented information governance policy can be the key.

Information governance is a set of multi-disciplinary policies, procedures and controls that authorizes and restricts your employees' use of the company computer, as well as their access to sensitive information. More importantly, without an information governance policy in place, it is virtually impossible to prove intent. When the FBI is contacted after a computer intrusion or theft of proprietary information has occurred, one of the Bureau's first questions will be "was your employee entitled to access the information in which they did"? If the answer is no, then the Bureau's next question will be "how can we prove it".

Information governance consists essentially of five areas—Data Governance, Information Technology Governance, Information Security Governance, Physical Security and Responsible Information Management.

Data Governance is the manner in which a company exercises control over the processes and methods of handling information. Does your company's policy restrict an employees' computer use, to include whether or not they are allowed to access the company system from the privacy of their homes? Are your employees permitted to log on whenever they like, or are they restricted to only certain hours of the day? In the reality of today's 24/7 work world your employees may need access at all hours, which will mean occasionally working from home. After all, time is money, and in today's competitive business world you need any edge you can get on the competition. However, by spelling out a specific policy of the dos and don'ts, you can more easily monitor your employees' use of your information, and spot obvious violations that may provide clues to nefarious intent. A specific process of Data Governance not only will hold employees accountable, but in the long run will ensure the organization is operating efficiently, as both leadership and employees understand the boundaries which they must work within.

Information Technology Governance focuses on ensuring that all of the stakeholders within the organization have the necessary input in the decision making process. Information Technology (IT)

can no longer be in a "black box", meaning decisions regarding how information is handled technologically can no longer be relegated to the IT personnel alone. By all interested parties coming together to ensure the proper governance steps are taken everyone's interests will be properly met. Also, as a byproduct, no longer can IT personnel be held solely responsible for decisions deemed to be poorly made. Leadership's role and vested interest in the decision making process will give them accountability as well, thereby freeing all parties to institute policies that are in the best interest of the company without fear of mitigating blame. Furthermore, Information Governance is becoming more recognized corporately and legally as a fiduciary responsibility of leadership, much like present day accounting and human resource systems.

Information Security Governance focuses on the information security systems to offer protection against unauthorized access. It is not just the computer hack that the company needs to be concerned about, but also what will happen to the information if it is compromised. Companies need to examine their in place protections to ensure against improper disclosure, as well as protect against modification or destruction of sensitive information.

Physical Security focuses on an organization's physical security system and policies. Physical security is any and all necessary requirements that once implemented are designed to prevent, deter, inhibit or mitigate threats that face the safety and security of persons, property and information. While many information security governance practices are driven by legislative requirements for tighter requirements, physical security standards including closed circuit television monitoring and ancillary components typically have fewer legal requirements for its expansion and use.
Small Businesses should not wait for legal mandates to provide adequate physical security standards to protect the small business and its data. In coordination with the Information Governance protection procedures and policies, physical security policies can provide enhancements by adding another layer of protection.

Through a collaborative process – every small business, regardless of size, should involve employees in the assessment process of identifying internal threats. This process can create a strong and healthy work environment while strengthening the information and physical security policies. Generally speaking, physical security components are made up of **Access Controls** including **Bio Metrics, Alarm Monitoring** and **Closed Circuit Television** (CCTV). All three components along with a moderately sophisticated physical security function – that is strategically aligned to a common set of security policies – can harden a target from the internal threat, whether it is information misappropriation or criminal in nature.

The **Access Control** components of the physical security program are used to grant or deny physical access to specific buildings or rooms within a structure. Additionally, access control can also be linked to information access points as needed to control and track the location of an employee.

Alarm Monitoring is designed to inform the monitoring center of an intrusion, panic, and/or threat event. It can also be used with the access control components to audibly notify an employee of a breach when an individual does not have authority to be in an office or virtual location.

The **Closed Circuit Television** (CCTV) component of a physical security program including digital recording with video analytics can warn the monitoring center of unusual actions that an employee is demonstrating while at work. Video analytics is the software program in a video system that is adjusted based on a set of normal human actions and behaviors in a given environment.

Since most inappropriate actions or criminal acts are preceded by abnormal behaviors and actions, the video system is programmed with analytic software that can alert the monitoring center of these abnormalities. This allows the control center operators to focus its attention on those abnormal behaviors and actions and then notify the small business owner and/or leadership for proper follow-up, investigation and intervention.

When a small business focuses on both information and physical security, a small business will have greater opportunities to improve its risk management objectives and successfully prevent, deter, inhibit, and mitigate internal and external threats to the small business.

Finally, **Responsible Information Management** goes to the core of the organization's values and ethics in protecting sensitive data. Many of these decisions will be driven by legislative requirements, such as the Red Flag rules and Sarbanes-Oxley. However, companies need to engage in these discussions so that they can not only adhere to the law, but also balance the societal and economic significances involved. All companies want to be seen as good partners in society, but have to take into account the financial bottom line. This balancing test needs to be openly discussed and incorporated in the operations of the company. Corporate leadership is responsible to steward their organization and governing their information has become a major focus of many large and small companies.

Using the five components of Information Governance—Data Governance, Information Technology Governance, Information Security Governance, Physical Security, and Responsible Information Management—organizations can then objectively examine the potential threats or possible damage to a company's protected data. Threats can be in the form of malicious code, a web compromise, an insider compromising trade secrets, or the criminal engaged in social engineering. But regardless of the threat, one thing is certain—you must have established Information Governance policies in place.

A written Information Governance policy, reviewed and signed on an annual basis by every company employee (and again, regardless of the size of the business) will document the needed element of proof showing intent, thereby then shifting the burden to the employee or hacker to prove their actions were not criminal in nature. Additionally, when an employee leaves your company, ensure that their access to the business data is quickly terminated and their access password has been removed. If you are able to show intent a law enforcement investigation and prosecution are far more likely to occur. Likewise, a successful prosecution will likely assist in your obtaining restitution for whatever damage occurred, as well as be a loud and clear message to others that your company will deal seriously with other would-be thieves of sensitive information who might contemplate trying the same.

It is not a matter of if, but a matter of when your company will become the victim of someone attempting to probe your business information. The key to ensuring that you are prepared for such is to minimize the potential for the hack by having in place a comprehensive Information Governance plan, to understand what needs to be done to ensure the necessary evidence is available to seek judicial remedies, and to have mechanisms in place so that your data is backed up off-site, and easily retrievable to keep your business going. Having a full and managed Information Governance policy is responsible leadership to your company, your sensitive information and your clients. Failing to have an Information Governance policy leaves your organization vulnerable to unnecessary risks.

Notice and Disclosure

This eBook is not intended to offer professional consulting services or legal advice. This eBook is intended to provide basic direction, guidance and concepts for small business owners and small business executives.

No one company can ever prevent itself from having an ID Theft, data breach or fraud event. Merchants Information Solutions, Inc. (Merchants) and its Advisory Board recommends all companies and organizations seek professional consulting services and legal advice regarding the content of this document.

This eBook is a working document and will be updated to reflect Small Business ID Theft and Fraud trends and regulatory/compliance updates on an ongoing basis.

Contributing Authors:

John G. Iannarelli
Assistant Special Agent in Charge (ASAC)
Phoenix FBI
http://www.fbi.gov/phoenix

Michael O'Shaughnessy
President & CEO
Guardian Pro
http://guardianpro.net/

Alan Saquella, CPP
Risk Management/Security
Asset Preservation
COX
http://coxenterprises.com/