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, FBI Phoenix Division

Small Business ID Theft and Data Breach

Safeguarding Information and Managing the Cost and Risk of a Small Business ID Theft and Data Breach Event

February 2015

Written by:
Mark Pribish, Vice President and ID Theft Practice Leader
James Collard, Vice President for Operations and Small Business ID Theft Services

Table Of Contents

Contents

Executive Summary

For years, most small businesses were an unlikely target for cyberattacks, data breaches and ID theft because of their small database of customers and employees, small revenue and profits until now.

However the dam has broken for small companies when it comes to security. Jeremy Grant, an adviser at the Department of Commerce's National Institute of Standards and Technology, stated that in the past two years he has seen "a relatively sharp increase in hackers and adversaries targeting small businesses."
Jan 2014, Web - http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html

The impact of small business ID theft and data breach is an emerging risk management issue for small to medium businesses or SMBs.

The premise of this small business ID theft and data breach whitepaper is based on three principles:

1. No ONE COMPANY can PREVENT any individual from becoming a victim of ID Theft
2. No ONE COMPANY can PREVENT itself from experiencing a data breach event
3. SMBs are the NEW TARGET for cyberattacks, data breaches and ID theft

Based on the above, this whitepaper will offer risk management and information governance concepts to support a proactive approach for small businesses in preventing and managing the risk of an ID theft and data breach event.

Small business ID theft and data breach events can take many forms, but in each case, business account information and/or employee or customer account information is lost or stolen through an accidental release or an intentional, illegal act.

This breached information can be used to initiate unauthorized activities that appear to be in the name of the business or to commit identity theft from the Personally Identifiable Information (PII) of current and former employees and customers.

According to a 2012 National Cyber Security Alliance (NCSA) and Symantec Survey, U.S. small business owners have a false sense of cybersecurity as more than three-fourths (77 percent) say their company is safe from cyber threats such as hackers, viruses, malware or a cybersecurity breach, yet 83 percent have no formal cybersecurity policy or contingency plan.
October 2012, Web http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

One of the most common causes of small business ID theft and data breach is the insider threat as reported by SpectorSoft's 2014 Insider Threat Survey – where 23% of enterprise respondents reported that their organization had suffered from an insider driven data breach and that 47% of enterprise respondents reported that former employees took information with them before they left the company.
Aug 2014, Web - http://downloads.spectorsoft.com/resources/infographic/spectorsoft-2014-insider-threat-survey.pdf

Another reason small businesses are targeted by cyber attackers is technology where email, websites, webinars, laptops, iPhones, iPads, and more have become a great technological resource for cyber criminals to increase the threat environment for cyberattacks.

This white paper will help small business owners and executives better understand their threat environment and the pre-breach planning and post breach actions that are necessary in responding to a data breach – whether it is from the outside through a hacker or an internal event through a current or former employee, vendor, customer, or organized crime.

Small Business ID Theft in the News

One of the big challenges facing small businesses today concerning information security and governance is the constant barrage of data breach news and headlines – what is commonly known as "breach fatigue," where most people including small business owners and executives begin to ignore the threat of a data breach.

To help every business owner understand the current threat environment, listed below are recent examples of headline news stories:

Data breaches increased 49 percent in 2014 to 1 billion data records compromised, with cybercriminals targeting identity theft as top breach category - Gemalto, a leading digital security firm released the latest findings of its Breach Level

Index, revealing that more than 1,500 data breaches led to one billion data records compromised worldwide during 2014. These numbers represent a 49% increase in data breaches and a 78% increase in data records that were either stolen or lost compared to 2013.
February 2015, Web - http://www.darkreading.com/gemalto-releases-findings-of-2014-breach-level-index/d/d-id/1319085

Is any business safe from Cyberespionage? - The simple answer is no. Even the smallest businesses can be directly targeted for the sensitive or valuable information they hold – from customer banking details, to supplier information or even data that can be used to help stage an attack on a larger enterprise.
November 2014 - http://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf

The Fourth Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management - Small and midsize businesses increasingly realized that they are highly vulnerable. Information security risks have become a risk management focus for more organizations. Thanks largely to a number of high profile retail breaches, 2014 also has been the year that executives and board members began to view cyber risks more seriously.
October 2014,Web http://www.zurichna.com/zna/media/news-releases/current-releases/advisen-cyber-security.htm

Attackers set their sights on medium-sized businesses - Small and medium-sized businesses (SMBs) are key prey for attackers, and this year demonstrated no exception to the trend. In 2013, SMBs collectively made up more than half of all targeted attacks at 61 percent – up from 50 percent in 2012 – with medium-sized (2,500+ employees) businesses seeing the largest surge.
April 2014, Web - http://www.forbes.com/sites/symantec/2014/07/24/the-2014-internet-security-threat-report-year-of-the-mega-data-breach/

The fact is small businesses need to be aware of and understand the data breach environment including the headline news in order to be proactive in protecting their businesses from ID theft and data breach events.

Information Security Is More than Information Technology

If a small business has a data breach event where the owner(s), partner(s), agent(s), and/or senior management do not already know what to do or who to call after a breach event - then it is usually too late for the business to respond quickly with an efficient and well organized plan that will minimize the negative impact on the business.

At the same time, a small business that plans for a breach event can expect their business to respond with a positive, well prepared, and proactive plan that will maximize public relations and goodwill along with the potential to actually increase new business revenue, sales, branding, and the company reputation by its proactive and responsive actions.

So what is the answer for small businesses – especially those businesses with limited financial resources? The simple answer is to do what is right for your business and customers by **implementing internal and external business policies and best practices.** This decision is no longer a "nice to have" but is critical to the survival of the business.

Every small business should understand that while technology has the potential to increase productivity, revenue and profits – technology can also create gaps in information security based on the following:

- **Small businesses handle sensitive employee and customer information (e.g. social security numbers, bank account information, driver license numbers, and birth dates).**
- **Small businesses rely on electronic networks including the information, data and the e-records within and outside these computer networks.**
- **Small businesses use e-mail, computerized accounting, electronic procurement, and/or store electronic employee and customer information.**

And based on the above, **small businesses need to know that**

information security is more than just information technology.

Information security requires commitment and input from every aspect of a small business, whether the business is a one person company, a 10 person company, or a 100 person company and should include the following:

- Senior Management – safeguarding business and customer information has to be a priority.
- Information Technology – needs to respond to hackers, malware and structural vulnerability.
- Human Resources – where current/former employee information; current/former employees; and careless employee actions should be included in the risk equation.
- Marketing/Sales – where current/former customer information; current/former customers; and careless

customer actions should be included in the risk equation.

- Physical Security – by knowing the security risks related to the home office, branch offices, remote offices, and equipment (computers, laptop, cell phones, PDAs, etc.).
- Finance, Legal and Risk Management – requires a clear understanding of corporate responsibility and regulatory requirements (e.g. state breach notification laws, Red Flags Rule, HIPAA information security requirements, etc.)
- Vendor Management – you need to understand your business relationships and the need for a formal due diligence process for every vendor or business partner – based on the risk associated in doing business with each vendor/partner.

By including the above points in a formal document such as an information governance plan, a small business will be able to identify risks such as gaps in security and benchmark exposures to create a foundation for a data breach response or incident response plan.

Regulatory and Compliance Drivers

Examples of regulatory requirements for small businesses could include the Federal Trade Commission **(FTC) Red Flags rule.** The FTC's Red Flags rule requires any size business that falls under the FTC's broad definition of "creditor" that has "covered accounts" to have an ID theft "prevention, detection and mitigation" plan in place if the breach of customer information could lead to potential ID theft events related to the customer information.

The **Health Information Portability and Accountability Act (HIPAA)** includes the **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** that requires a data breach notification plan for business associates. Business associates are companies like accounting firms, billing agencies, law firms and/or other businesses that provide services to entities like hospitals, medical groups, dental groups, pharmacies, and other healthcare related companies.

A third regulatory and compliance driver for small businesses are the current **47 state Security Breach Notification Laws, the District of Columbia, Puerto Rico and the Virgin Islands.** In each instance, each state breach notification law requires your business – regardless of size – to notify any employee, customer and/or member of a data breach event where employee, customer and/or member information may have been lost or stolen.

Managing the Risk and Cost of Small Business ID Theft and a Data Breach

According to the Ponemon Institute's 2014 Annual Study: Cost of a Data Breach -- the Ponemon Institute's benchmark study concludes

the average cost of a data breach is $201 per lost record

based on direct, indirect and lost opportunity costs. Has your small business created a budget of $201 times your total number of current and former employees and customers? **May 2014, Web -http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis**

Your small business needs to understand that the data your small business uses, stores, and transfers has a street cash value. You can manage the risk of your data and a potential ID theft or data breach event by completing **an information governance assessment of your business data assets** and answering some of the following questions:

1. Your cyber assets – what are they worth?
2. Your current and former customer data – what is it worth?
3. Your current and former employee data – what is it worth?
4. Your current and former vendor relationships – how secure are they?
5. How many current/former employees and vendors have had access to employee and customer data?
6. What is your pre-employment screening policy and process?
7. What is the risk equation in signing up new business clients and taking on sensitive customer information?

Since today's small business computer servers contain business data, employee data, and customer data, these computer servers are like financial institutions where ID theft criminals and hackers target databases for profit.

So what can be done? Every small business should support its **information governance** plan by completing the following action items:

1. Implement an information governance policy.
2. Develop an incident response plan.

3. Require annual information security training and education.
4. Understand what type of employee, customer and/or member data is being collected, stored, and protected?
5. Constantly assess and test your organization's needs and requirements.
6. Know your organization's strengths and weaknesses.
7. Implement baseline safeguards and controls.
8. Vigilance including annual pre-employment screening.

Each small business has unique risks by industry group, size of business, and types of business along with the employee and customer data that is being collected.

The initial goal in creating an information governance plan is to be deliberate and take your time in assessing and understanding ALL potential risks related to your business.

About SmartIDentity for Business

Merchants Information Solutions, Inc. (MIS) provides a wide variety of sponsored and consumer-paid strategies for identity theft and data breach detection and recovery, utilizing the highest quality, high-touch services and state-of-the-art technologies. SmartIDentity for Business is designed to provide a small business with the following three benefits:

- **Data Breach Planning and Preparedness** by supporting a threat assessment, risk profile and customized response plan.
- **Data Breach Response Services** for an accidental or malicious incident that results in the loss of consumer non-public personal information including breach notification.
- **Personal Identity Theft Recovery Services** for all principal owners of the business and their titled officers if identity theft strikes their individual name.

The SmartIDentity Business solution is supported by MIS' professionally-trained, Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transaction Act (FACTA) recovery advocate service.

About Merchants Information Solutions, Inc.

Founded in 1912, Merchants is a leading provider of low-cost identity theft protection and recovery solutions, helping to support the risk management objectives of financial institutions, associations, employer groups, and the automotive industry – by offering revenue opportunities through fee-based subscription services. Merchants also has a robust line of on-demand background screening solutions empowering pre-employment, tenant screening and behavioral psychological assessments for clients to instantly assess candidates in minutes. For more information, visit www.merchantsinfo.com.

About the Authors

Mark Pribish, Vice President and ID Theft Practice Leader – Mark Pribish has 25 years of experience in working with financial institutions, associations and Fortune 500 companies throughout the United States. His background includes the sales and marketing of identity theft, cyber insurance, and data breach response solutions through affinity marketing and risk management programs. Prior to joining Merchants in 2005, Mr. Pribish was Senior Vice President for Aon Risk Services of Arizona, Inc., National Sales Manager for AIG Life and the AIG Environmental Banking Group, and a regional sales executive for Affinion.

James Collard, Vice President of Operations and Business ID Theft – Jim Collard has over 30 years of senior executive experience in Business Credit, Financial Management and Operations. Before joining Merchants in 2005, Mr. Collard served as a General Manager, Chief Credit Manager, and Chief Financial Officer for a number of regional and national companies where he supported business credit fraud and fraud risk management. Mr. Collard also held the position of President of the Credit and Financial Development Division of NACM (National Association of Credit Management) and was Chairman for the Phoenix Area Credit Executives.

End Notes

Why Your Business Might Be a Perfect Target for Hackers
Jan 2014, Web - http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html

New Survey Shows U.S. Small Business Owners Not Concerned About Cybersecurity; Majority Have No Policies or Contingency Plan
October 2012, Web http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01

An overview of the insider threat landscape and key strategies for mitigating the threat challenge
Aug 2014, Web - http://downloads.spectorsoft.com/resources/infographic/spectorsoft-2014-insider-threat-survey.pdf

Data breaches increased 49 percent in 2014 to 1 billion data records compromised, with cybercriminals targeting identity theft as top breach category.
February 2015, Web - http://www.darkreading.com/gemalto-releases-findings-of-2014-breach-level-index/d/d-id/1319085

Is any business safe from Cyberespionage?
November 2014, Web - http://media.kaspersky.com/en/business-security/kaspersky-cyber-espionage-whitepaper.pdf

The Fourth Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management
October 2014, Web http://www.zurichna.com/zna/media/news-releases/current-releases/advisen-cyber-security.htm

Attackers set their sights on medium-sized businesses
April 2014, Web - http://www.forbes.com/sites/symantec/2014/07/24/the-2014-internet-security-threat-report-year-of-the-mega-data-breach/

Ponemon Institute Releases 2014 Cost of Data Breach
May 2014, Web - http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis