SMALL BUSINESS ID THEFT AND FRAUD

DATA BREACH RISK MANAGEMENT BEST PRACTICES GUIDE FOR SMALL BUSINESS

NO ONE COMPANY CAN PREVENT
ITSELF FROM EVER HAVING A DATA BREACH EVENT

Mark Pribish – VP & ID Theft Practice Leader, Merchants Information Solutions, Inc.

eBook sponsored by:
MERCHANTS INFORMATION SOLUTIONS
ID THEFT ADVISORY BOARD

TABLE OF CONTENTS

WHAT IS A DATA BREACH	3
DATA BREACH EVENTS ARE AN EMERGING RISK MANAGEMENT ISSUE	4
VERIZON 2012 DATA BREACH INVESTIGATIONS REPORT	4
SMALL BUSINESS DATA BREACH RISK FACTORS	5
DATA BREACH RISK MANAGEMENT	5
WHAT CAN A SMALL BUSINESS DO	6
DATA BREACH RESPONSIBILITY IS ON THE DATA OWNER	7
CREATING A DATA BREACH INCIDENT RESPONSE PLAN	7
DATA BREACH RISK MANAGEMENT RECOMMENDATIONS	14
CONTRIBUTING AUTHORS	15

Is your Small Business Prepared for a Data Breach Event

WHAT IS A DATA BREACH?

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data. However, not all data breaches are so dramatic. If an unauthorized hospital employee views a patient's health information on a computer screen over the shoulder of an authorized employee that also constitutes a data breach. If an employee steals another employee(s) personnel files containing PII or PHI that also constitutes a data breach.

A data breach can be malicious or accidental. Malicious obviously applies to a perpetrator with the objective to access information that could be resold in the black market or utilized to transact an identity fraud event. An accidental breach is much less obvious. A number of industry guidelines and government compliance regulations mandate strict governance of sensitive or personal data to avoid data breaches. Within a corporate environment, for example, the Payment Card Industry Data Security Standard (PCI DSS) dictates who may handle and use sensitive PII such as credit card numbers, PINs and bank account numbers in conjunction with names and addresses. Within a healthcare environment, the Health Insurance Portability and Accountability Act (HIPAA) regulates who may see and use PHI such as name, date of birth, Social Security Number and health history information.

If anyone who is not specifically authorized to do so views such information, the corporation or healthcare organization charged with protecting that information is said to have suffered a data breach. If a data breach results in identity theft and/or a violation of government or industry compliance mandates, the offending organization may face fines or other civil or criminal prosecution.

Data breach events are an emerging risk management issue for all businesses in general and small businesses in particular. Based on the numerous and persistent trend of data breach events, no one company can prevent itself from EVER having a data breach event.

That said, small businesses today are managing more customer, employee and proprietary information than ever before. The safeguarding of this customer, employee and proprietary information is now a priority for small business owners along with managing the risk and total cost of a potential data breach event.

In addition, the effective safeguarding of information could determine the success or failure of a small business as identity thieves are targeting and stealing customer and employee information, business assets, business credit information, and even the business branding and reputation for financial gain. In recent years, identity thieves have learned that small business owners are an easier target than big companies as big companies have more resources and have become better at protecting their assets.

The Verizon 2012 Data Breach Investigations Report found that small businesses getting attacked are one of the two big trends in its annual study of security breaches. The Verizon Data Breach Investigations Report also found that nearly three-quarters of data breaches analyzed last year were businesses of 100 employees or less.

For example, most small business owners are focused on selling products/services, growing revenue/profits, and increasing the company's brand image – while many of the same small business owners are ignoring basic information governance and security standards and regulatory requirements.

Small business owners – regardless of the size of the business and number of employees – should consider taking a proactive Enterprise Risk Management (ERM) approach in supporting and protecting their business.

Small business data breach risk factors include people, processes and technologies:

- People – the insider threat, whether accidental or malicious, can include current and former employees, customers, associates, vendors, and independent contractors.
- Processes – including information technology, enterprise risk management, marketing/sales and human resources need to be aligned, defined, and documented.
- Technologies – that are relied on to conduct and grow your business are also being used to identify vulnerabilities and cyber threats on your business.

Data breach risk management can be supported by incorporating basic risk management concepts including pre-employment background screening, even if there are only one or two employees; information technology security including the use of firewalls and perimeter controls, anti-virus/anti-malware solutions, database security tools, and endpoint security solutions; collateral security to isolate and protect hard copy employee, patient and customer files; information governance including a comprehensive security assessment; and vendor management including the due diligence review of all vendors and their security standards.

What can a small business do? The first action item is to complete a data assessment of the type of information that is being collected, used, stored and transmitted by asking the following questions:

- What type of data (e.g. current and former employee / customer / patient information) is in your electronic and hard copy files?
- What type of Personally Identifiable, non-public Information (PII) is included in your business data (e.g. name, address, social security number, driver's license, bank account information, credit/debit card, medical plan information)?

- What percentage of your data involves the collection, storage, usage, and transmittal of current and former PII?
- What aspects of your business products, services and technology are performed within and outside your business?
- What is the value of your data assets if they were stolen and made public?
- Is data that you store subject to civil fines and penalties if breached?
- What is your overall financial risk if data you control is breached?
- Which states does your business conduct business in and what states are your customers / employees / patients domiciled?
- Could a data breach damage your brand and if so what is the potential impact?
- Does your business insurance include cyber/network liability insurance?

Data breach responsibility is on the data owner whether the business data is accidentally lost or it is stolen with malicious intent. Any business that experiences a data breach should work with legal counsel to determine regulatory requirements including but not limited to state breach notification laws, the FACT Act Red Flags Rule, the HIPAA HITECH data breach requirements, the PCI Data Security Standards, and the COPPA (Children's Online Privacy Protection Act).

Based on current and future privacy and security laws, your business may have responsibility to notify affected individuals of a potential security breach to their personal information – and according to the March 2012 **Ponemon Institute Cost of a Data Breach Report**, a data breach could cost your business up to $194 per lost record. So a question for every small business is: "Have you budgeted $194 per individual record that resides in your database (customer or employee) in the event of a data breach?"

Creating and implementing a data breach incident response plan can assist a small business in several ways:

- **Planning** will significantly reduce costs related to breach response and help mitigate its effects through efficient and timely notification.

- If a **professional breach remediation resource** is not pre-determined an actual Breach event could create an adverse situation through the haste of engaging a Breach response provider.
- **Proper notification**, planning, and professional execution of the plan will help mitigate possible fines, penalties, class actions, brand damage, and loss of revenue.

While each small business is unique to its industry group or business sector, the foundation of a small business data breach incident response plan should include the following tenants:

- **Determine Breach Source** – and make sure the data compromise is isolated and access is closed. If you cannot determine the source of breach you should engage a forensic investigation company.
- **Breach Assessment** – to determine the scope of the data breach event and the privacy and data security regulatory requirements associated with the type of records in addition to the state of domicile.
- **Response Plan** – including internal employee education and talking points; public relations press releases, customer education and resources; the small business or consumer solution(s) to be considered; and the content and timely release of notification letters.
- **Protection Plan** – including the small business or consumer protection services to be offered to the compromised record group; and the confirmation of professional call center and recovery advocate support services.
- **Breach Victim Resolution Plan** – providing access to professional certified identity fraud recovery advocates that will work on behalf of the victims to mitigate and resolve the issues caused by breach. In order to provide the best level of consumer satisfaction make sure you select a provider that performs resolution through a limited power of attorney. If a breach victim thinks their data has been used to transact identity fraud the advocate will conduct data base searches to help surface data that has been exposed but not initially discovered. The advocate will also conduct credit history research and discovery. Credit monitoring provided in conjunction with this resolution service will also help provide detection. The

advocate will file disputes and require resolution from the entities affected by the identity fraud event. This is all done until all of the discovered events are resolved.

Data Breach Victims Face a Real Risk that is not resolved through Traditional Breach Response Programs

It is a known fact that an individual's data records compromised in a breach typically are resold and aggregated several times on black market Internet trading sites. This information is also warehoused for time periods exceeding 12 months and may even take several years before the data is actually used to transact an identity fraud event. There is a significant amount of profit in selling this data alone. These black market Internet trading sites are high volume fencing operations for data brokers supported by organized crime, international terrorist groups, and individual criminals.

Traditional Breach Victim Response Programs create a Significant Risk Management Gap

There is a significant risk management gap in traditional breach event victim response services in today's world. This risk management gap stems from the fact that traditional breach victim response programs only provide detection and remediation services access for 12 months. Unless the data breach perpetrator does not follow the typical modus operandi, the breach response services offered through the breached organization are useless. In addition to the traditional time period providing victim access being insufficient, some of the breach response services require victim registration and authentication.

Registration requires that the compromised individual must enroll typically through an online portal provided by the breached organizations response service provider. If the individual does not register and enroll they cannot access the benefits provided.

Authentication requires both registration and enrollment first. Once the first step is taken, credit monitoring activation for example, is done online through authentication which is a process that validates the individual's identity and allows access to credit monitoring and alerts.

Victim response programs offered today provide all, none, or some of the following victim identity fraud detection and remediation benefits …

- **Victim Notification** – A letter communicating the breach event with information regarding the data compromised with response program services access options available to the compromised victims.
- **Assisted or Fully Managed Identity Fraud Resolution** – Provides the victim with access to identity theft recovery service professional certified advocates to file disputes and resolve. The breached organization usually will send a limited information secure file specifying the breach victims so the victim solution service provider can maintain a data base allowing the breach victim to directly contact the service provider to activate services if an event occurs that makes them think they are a victim of identity fraud. **Registration and Authentication are usually not required.**
- **Credit Monitoring** - Will monitor consumer's credit reports for activity and alert them to changes to their accounts. If an alert is generated that is not the individuals being monitored the change may be identity fraud. Credit monitoring is usually provided to victims that utilize the fully managed recovery service at no cost to the victim or breached organization. **Registration and Authentication is required.**
- **Credit Reports** - An amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies provide a consumer with a free copy of their credit report, at their request, once every 12 months. In addition, individuals that think they are a victim of identity theft they can notify one of the major credit repositories and receive a credit report in addition to filing a credit alert. (This is a FREE service if you go directly to one of the credit repositories. This will also be included with most fully managed recovery services at no additional expense). **Registration and Authentication is required if the service is included as a breach victim response service.**
- **Fraud Alerts** – Free service provided by the major credit repositories if a consumer thinks they are a victim of identity theft. A fraud alert places a statement on a consumer's credit report. If an imposter attempts to obtain credit in the consumer's name, the creditor will check credit and will encounter a statement that says something to this effect: "I may be a victim of fraud. Call me at my phone number 123-456-7890 before extending credit." An initial fraud alert lasts 90 days. An identity theft victim can request an extended fraud alert that remains a part of their

credit files for seven years. (Placing a fraud alert is usually recommended by most fully managed recovery service providers at the initial point of contact) **Authentication is required and can be completed by phone or online by the victim.**

- **Internet Monitoring** - Monitors internet black market websites, chat rooms, etc. for personal credentials, such as name, SSN, credit cards, driver's license, etc. In the event that a monitored personal credential surfaces on one of these internet sites an Alert will be sent via email or text message. **Registration is required in order to monitor. The process includes victim input of the personal credentials.**
- **Identity Theft Expense Reimbursement Coverage** – Reimburses for expenses related to identity theft resolution including lost wage and legal fees and expenses. The victim is usually responsible for compiling receipts eligible for claim reimbursement and submitting them to the underwriter at the end when all identity fraud issues are resolved. **Registration may be required in some cases. When fully managed recovery service through a limited power of attorney is activated specific registration for expense reimbursement insurance is not required. The true fully managed recovery service also incurs all or a majority of the expenses that are scheduled for reimbursement under the expense reimbursement insurance making the real value of having such coverage benefit incidental.**

Time period access for traditional breach response services is 12 months

All, some, or none of these traditional services may be provided at the expense and discretion of the organization in which the breach event occurred.

The usual time period a breach victim can access traditional services is up to 12 months. The time period available for breach victim access is limited because the business that was breached is responsible for the cost of providing these services.

The cost of the breach response services may be partially covered in breach liability insurance policies. The reason only a portion of the cost is covered is due to coverage deductibles, policy limits, and coverage exclusions. Most breach liability insurance policies do not include solution

service providers. "Solution Service Providers" are the organizations that actually execute the breach response plan, Program services delivery, and victim support.

Some breach policy underwriters provide access to breach solution service providers however their services are engaged and billed to the breached organization separately. Then reimbursement claims are filed with the breach liability insurance provider to "partially" reimburse for covered losses.
48 states have some type of breach notification requirements. While there is some continuity in each states requirement there are differences that need to be properly addressed for compliance purposes. Certain types of organizations also have to comply with specific regulators that oversee their type of business of profession.

The Issue "If the stolen data is monetized through reselling, aggregating, warehousing and typically not used to transact identity fraud for several years, what benefits do traditional response plans provide?" NOT MUCH

Identity fraud experts realize that there is a significant risk management gap in traditional breach response services due to the fact that are victim access is usually provided for a 12 month time period. Some traditional response and monitoring services may have a nominal benefit in the first 12 months subsequent to a breach however, access to those services usually expire after the 12 month period when they are really needed.

To make matters worse a majority of the breach response benefits require registration and authentication. If the breach victim has not registered and authenticated then any monitoring service or expense reimbursement coverage that has not been activated is totally useless.
Breach response resolution and monitoring services can also carry a very high price tag. The larger the volume of compromised records the greater impact it has on the breached organizations bottom line.

The compromised organization has to balance out the cost of providing breach response services to mitigate brand damage and loss of revenue with its public relations benefit. Most guidance and

regulation directives provided by government consider providing breach response services for 12 months acceptable. A majority of consumers that don't know the risk they face also see the 12 month breach response service access as acceptable.

If a consumer understood the actual LONG TERM and SHORT TERM effects that a Breach could have on his/her life, there would be more class action lawsuits and the demand for more regulation would follow. Organizations that have and will suffer a breach event stand to experience a negative impact unless they take a proactive approach.

The proper risk management response solution for the LONG TERM and Short Term effects of a breach event should include:

1. Provide access to breach response services for more than 12 months. In fact, up to 5 years is a better way to go.
2. Provide breach remediation services that can be accessed anytime during the access period that does not require registration or authentication.
3. Balance out the cost of providing the services over a longer period of time by eliminating high cost services such as Credit monitoring and expense reimbursement. In the course of the consumer and regulators "Real Effects" awareness transition phase it is suggested at least some form of monitoring for 12 months.
4. The cost of providing the most comprehensive risk management breach response benefit can also be the least expensive depending on the service provider. The most comprehensive and effective breach response benefit that can be provided to victims is fully managed identity fraud recovery. The gold standard of the industry provides recovery and remediation through a limited power of attorney.
5. Internet monitoring is also an efficient and effective way to help alert victims to data that is exposed on black market internet sites, however it does require registration.

Industry experts will all agree that **Fully Managed Recovery Services** provided by experienced professional recovery advocates will be more effective and efficient cost wise than any other breach

response service known today. In fact an organization that makes the decision to provide fully managed recovery services for a 5 year time period will pay less that they would for 12 months of credit monitoring services.

Why does Fully Managed Identity Fraud Recovery Services make sense from a Risk Management standpoint?

In most cases the source of the identity fraud event cannot be detected. So for example, three years down the road how can the victim really know that the breach source was the organization that had some of their personal data subjected to a breach event? The best fully managed recovery service providers will cover any type of identity theft and not require evidence regarding when the event occurred. They will provide remediation and resolution until completed without a time limit. The fact that this benefit can be accessed at any time during the benefits period without registration or authentication makes this a consumer friendly option.

When the breach victim's access time period extends to 5 years or more the fully managed recovery remediation and resolution solution will continue to provide more value from public relations and risk management standpoint.

As consumer awareness regarding the "Real Effects" of breach continues to gain exposure and attention, hopefully government lawmakers will also understand how they should regulate and provide proper guidance to organizations that control and maintain personal non-public data. breach response risk management solutions that benefit victims for the "Long Term and Short Term" effect of identity fraud is a solution that can be provided now.

If your organization suffers a data breach, make sure you access a breach resolution service provider that is consultative and not just offering "turn-key" breach response package options for profit. There is nothing "turn-key" about a breach. Each one is unique and properly responding to a breach event can help mitigate its effect on brand damage, loss of customers, regulatory issues, and financial loss.

Make sure you have a breach response resource in place in advance so that the proper due diligence can be conducted at your convenience, as opposed to the haste associated with no plan.

To do the right thing for victims of a breach event for a longer period of time does not necessarily cost more than the traditional approach to breach response. It is important to consider how consumer awareness will evolve and how your organizations breach response solution will impact your brand image.

Small Business Data Breach Risk Management Recommendations

- Know your organization's strengths and weaknesses.
- Monitor your business credentials to help provide early detection.
- Schedule periodic assessments and test your small business security vulnerably strengths and weaknesses. Have appropriate dual controls in place for access to sensitive data and financial transactions and audit that access at least annually.
- Perform periodic social engineering testing of staff and vendors who have access to your data. This could include sending emails that look legitimate that include links. Track who has clicked on the link and follow up with them on the risk and violation of policy.
- Increase employee information governance and security awareness through education including written communications and meetings. If you perform transactions or communications via TTY devices ensure there is a second level of authentication review. Make staff aware a large number of small business and personal breaches occur because of use of open Wi-Fi connections especially in vacation and conference settings.
- Implement baseline safeguards and controls such as securing sensitive business, employee and customer information including electronic and paper files. Ensure you have the ability to wipe data from employee devices remotely if reported missing or an employee is terminated.
- Keep your technology current including the use of a firewall, anti-virus software, encryption, and a strong password management policy. Ensure malware software and firewalls are up to date and maintained on employee devices. If you allow your employees to use their own devices, both mobile and laptop, consider having a third party application to secure

connections. These are available from most major mobile carriers or can be managed on your own enterprise network.

- Vigilance including annual pre-employment screening and limitation or restriction of certain data related to employee responsibility.
- Stay current on ID Theft and Data Breach related events/trends – especially in your industry group and the states you conduct business. Education and awareness can help you prevent business and personal identity fraud losses.
- Determine how much financial risk your firm can fund and evaluate the need for cyber liability coverage if you have not done this already.
- Understanding your business owner insurance policy including the cyber/network liability coverage – and, consider adding a cyber/network liability endorsement if the current business owner policy does not include said coverage.

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:

Kent Ailes
Vice President of Risk and Cards
Arizona Federal Credit Union
www.arizonafederal.org

Mark Pribish
VP & ID Theft Practice Leader
Merchants Information Solutions, Inc.
www.merchantsinfo.com

Scott Smith
NXG Strategies, LLC
Managing Partner / Co-Founder
www.nxgstrategies.com