SMALL BUSINESS ID THEFT AND FRAUD

IT SECURITY RISK MANAGEMENT BEST PRACTICES GUIDE FOR SMALL BUSINESS

"WITH HIGH PROFILE SECURITY INCIDENTS TAKING PLACE EACH WEEK, IT SECURITY IS NO LONGER ABOUT RELYING ON THE IT TEAM PLAYING THE ROLE OF POLICE OFFICERS. RATHER, EVERY EMPLOYEE HAS A RESPONSIBILITY TO KEEP THE COMPANY SAFE."

Steve Phillips – Senior Vice President and Chief Information Officer, Avnet, Inc.

eBook sponsored by:
MERCHANTS INFORMATION SOLUTIONS
ID THEFT ADVISORY BOARD

TABLE OF CONTENTS

IT Security Risk Management for your Small Business

Information technology security and risk management – at first glance – appear to be two distinct and separate functions within any small or large business.

However, the breathtaking pace of changes in technology combined with the large amounts of data used and stored digitally by small businesses require a more comprehensive approach to managing technology and data.

That said small businesses today need to utilize a risk management approach in assessing and addressing their network, technology devices and vulnerabilities.

In assessing security risks and vulnerabilities, it is important to look at both:

- **Insider Threats:** While most employees behave with integrity, there is always the potential that an employee could significantly impact IT security if they simply become careless or even "go rogue." This could include unsuspectingly downloading a virus or malware, stealing data, deleting business-critical files, or even sabotaging computer systems. This type of threat is often the most difficult to detect since employees already have system access, and it can be challenging to distinguish normal behavior from a potential security issue.
- **External Threats:** It seems like there is no limit to the number of outside forces that could potentially harm even the most protected IT system. These external forces include computer equipment thieves, contractors, hackers, former employees, and organized crime. They have a wide-variety of ways to attack small businesses, but some of the common techniques they use include Denial of Service (DoS) attacks and phishing.

Both these internal and external forces can exploit IT security vulnerabilities in variety of different ways, and key areas that small businesses should vigilantly monitor include:

- **Cloud Computing Platforms:** While cloud computing offers significant benefits for small businesses, it is important to keep in mind that you are providing a third-party with your data, and potentially very sensitive data. If a cloud vendor's security is breached, there is the potential that your data will also be breached or a "back door" could be opened into your systems. When working with any cloud vendor, small businesses should extensively validate the cloud vendor's security practices to make certain they trust the cloud vendor to protect and secure hosted data like it is their own. A good practice is to ask if the cloud provider engages an outside party to perform an audit of their security and control practices such as a Service Organization Controls Report.
- **Cyber Threats:** This most commonly includes Advanced Persistent Threats (APTs), malware and viruses that seek to harm or gain access to data stored on web servers, behind firewalls, encrypted, and transmitted via mobile networks.
- **Physical Assets:** With wide-spread adoption of laptops, smartphones and tablets in the business world, a data breach can occur if even one of these devices is stolen or lost. Small businesses should explore ways to protect any sensitive company data housed on mobile devices. This is especially relevant today with the BYOD (bring your own device) movement, where employees are increasingly using their own personal devices for work purposes.
- **Social Engineering:** This technique focuses on manipulating people into sharing confidential information or circumventing security. This is often done to gather information, commit fraud or gain computer system access from an unsuspecting person.
- **Regulatory Requirements:** It is critical that small businesses understand privacy and security laws, such as state breach notification laws, FTC Red Flags Rule, and the HIPAA-HITECH data breach requirements. Additionally, small businesses should pay close attention to Payment Card Industry (PCI) regulations associated to credit card transactions, especially as more small businesses use mobile devices to "swipe" credit cards. Failure to comply with these regulations could have a significant financial impact on a small business.

Once a small business has a better understanding of the security risks and vulnerabilities related to technology – it can implement and support a best practices policy to help protect its business, employees, customers, partners and suppliers.

An information technology security assessment is an example of an information technology best practice that can be used for your small business.

An information technology security assessment (IT Security Assessment) is an opportunity for any organization, including small businesses, to identify potential information technology related vulnerabilities and risks.

A common misperception is that a small business does not require a comprehensive information technology assessment simply because the business is a small business with a small database. However, and quite the contrary, most small businesses – especially those with a database including Personally Identifiable Information (PII) – are at risk of being targeted by identity theft criminals and hackers. And, the bottom line is that it only takes one device to breach any company's defenses regardless of the organization's size.

The standard assessment will deliver practical guidance and advice – whether your business is a one person company or a 100 person company. The assessment begins once the small business agrees to grant access to its physical location to a reputable third-party IT security expert, provides network access, and outlines detailed information about the small business network infrastructure, etc.

All parties understand that the goal is to study security and identify improvements to secure the systems. An assessment for security is potentially the most useful of all security tests.

The following outline is an example of an information technology security assessment:

- Requirement study and situation analysis
- Document review

- Risk identification
- Vulnerability scan, including wireless networks
- Social engineering testing
- Data analysis
- Report & briefing

Based on the above, the security assessment report will include the following information/assessment:

- Introduction/background information
- Executive and Management summary
- Industry benchmarking of overall security posture against other similar industries or company sizes
- Industry benchmarking associated to the risk level of each vulnerability
- Assessment scope and objectives
- Assumptions and limitations
- Methods and assessment tools used
- Current environment or system description with network diagrams, if any
- Security requirements
- Summary of findings and recommendations
- The general control review result
- The vulnerability test results
- Risk assessment results including identified assets, threats, vulnerabilities, impact and likelihood assessment, and the risk results analysis
- Recommended safeguards

Once complete, your small business will most likely have an advantage over the competition as your security assessment will be a valuable marketing and due diligence tool to show how your small business is able to support a trusted vendor relationship.

The last recommended priority action item is the creation of a **small business continuity plan** (**BCP**) which will help identify potential exposures related to internal and external threats and provide key prevention and recovery action items.

A small business continuity plan will also help a small business owner remain open for business under an unexpected and adverse condition (e.g. a data breach event, an employee injury or a physical loss of property).

Finally, your new business continuity plan should be used as a working document that will change and evolve along with your business strategies and objectives.

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:

Lisa Daniels
Managing Partner
KPMG LLP
www.kpmg.com/

Christine N. Jones, Esq.
President
CNJ Management
cnjmanagement.com

Steve Phillips
Senior Vice President and Chief Information Officer
Avnet, Inc.
http://www.avnet.com/