CYBER SECURITY PLANNING GUIDE

New York Small Business Development Center

Funded in part through a cooperative agreement with the U.S. Small Business Administration. All opinions, conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of the SBA.

CYBER SECURITY PLANNING GUIDE

CONTENTS

ACKNOWLEDGMENTS

Contributing Author:
Thomas Morley, Director, Rockland Regional Center NY SBDC

Contributing Editors:
Darrin Conroy, Director, New York SBDC Research Network

David Carnevale, Publications Director, New York SBDC

Design/Layout/Editing:
David Carnevale, Publications Director, New York SBDC

* Special thanks to **Dave Powalyk**, Chief Information Officer, SUNY System Administration, for his contribution to the content of this guide.

INTRODUCTION

We hear much about cybersecurity these days including how important it is, how difficult it can be, how significantly a breach can impact a business and much more. Sometimes it can all seem a bit overwhelming or too challenging to achieve or, for many small businesses, far too expensive. Our objective in this guide is to provide some pathways to achieve a level of data protection appropriate for your small business. The data security needs of a small restaurant will be vastly different than those of an engineering company so we'll try to include examples throughout that will hopefully illustrate a plan that makes sense for your business.

An attitude adjustment can help as we deal with cybersecurity. How our attitude towards our information and vulnerability shapes our response is significant. All businesses have information that is valued in many ways; recognizing and categorizing that value is important. From simple recipes to complex chemistries, all businesses rely in myriad ways on information. Any business can be the victim of an attack that breaches or damages the information we rely on. Whether the threat is internal or external, we are all potential targets.

A good first step for all businesses is to view information and data in much the same way as other assets of the business – as something valuable and deserving our attention and protection. While the double-top-secret research data of a tech firm might seem an obvious high value information asset, the Human Resource records of a three-person rural business are also of value, albeit to different rogue elements and for different reasons. Further, we should also view data as potentially costly if breached. For example, the loss, or external theft of, certain data (like Social Security numbers or credit card numbers) might mandate paying for credit monitoring, litigation, fines or such.

Not all firms are targeted. Often small businesses are simply stumbled upon as part of sequential probes that are computer driven. Remember the bad old days of telemarketers who simply dialed phone numbers in sequence? Well, in this digital age there are 'bad actors' or 'rogues' - digital thieves who are simply trolling IP addresses (your company's digital 'address'), looking for a weak spot.

When they find one, 'hackers' will 'penetrate' a system and look for any data of value. They will interpret that value in the context of the global bazaar of money for data. Examples include holding your data hostage via encryption [ransomware], selling the Social Security numbers of employees found in a spreadsheet, selling credit card numbers stored within an ecommerce website, stealing design plans for the newest product, and so on. More often lately, a 'ransom' is demanded, forcing you to purchase your own information which hackers have encrypted, preventing you from using your own data which will be destroyed if you fail to pay.

A chilling example of this risk: for more than a week, hackers shut down computer systems at Hollywood Presbyterian Medical Center for a ransom of 9,000 bitcoin, or almost $3.7 million, by encrypting the hospital's data, preventing use of their own data and threatening to never enable the hospital to regain access. The hospital said patient care was not compromised, but the 'ransomware' attack forced the hospital to revert to paper registrations and medical records, and to send emergency patients to other area hospitals. This greatly increased operating costs, not to mention the millions paid in ransom. Small businesses are often hit with attacks demanding 20 to 100 bitcoin – trading at this 2016 writing at US $580.95 – to get your own data back!

Sounds farfetched? It's not. Data thieves can make significant money selling your data. For example, 'Fullz,' dossiers of credentials for a single identity theft, sell for an average of $30 each (a $5 increase from 2013 prices) while 'Kitz' (which includes healthcare data with identity information and related documents) can sell for upwards of $1,000.

Data reports show just how much some data can be worth:

a. Social Security number (as part of 'Fullz' dossier) - $30

b. Date of birth - $11

c. Health insurance credentials - $20

d. Visa or MasterCard credentials - $4

e. American Express credentials - $7

f. Discover credit credentials - $8

g. Credit card with magnetic stripe or chip data - $12

h. Bank account number (balances of $70,000 to $150,000) - $300

i. Full identity 'Kitz' - $1,200 to $1,300

Despite these values, data theft is becoming less the target. Data kidnapping (ransomware) has become more and more prevalent. The threat vectors originate from many sources including cyber-terrorism, criminal activity and state sponsored or rogue actors. It's important to remember that threats can be external or internal and even originate from inadvertent events like a lost laptop or USB key.

The 'why' of data attacks and breaches are converging. E-espionage (attacks seeking information for its own sake) and financial (attacks seeking theft of specific values) clearly showing the increasing value of information, often the lifeblood of small business.

The 'how' of threats and attacks runs a gamut of aptly named tactics like replicated credentials, key-loggers, ransomware, RAM scrapers and C2 backdoors and more. We don't need to understand how each of these work, just how to stop them and avoid what many studies show as costing small businesses an average of more than $180,000 to cover data repair and active response – not to mention the potential or opportunity cost of confidential product or process breaches that can dramatically diminish a competitive edge in the market.

The numbers – or what we should more accurately call the 'why you should do something' – are alarming:

- 72% of successful data breaches occur in small businesses
- 71% of small business owners lack confidence in their data security systems
- 65% of small businesses have no cyber insurance
- 83% of small businesses have no cyber security plan
- Almost 65% of victimized small businesses are forced out of business within six months of a successful attack

The costs of a data breach often go beyond direct expense. The cost to a business' reputation, the loss of customer or supplier confidence, the 'black eye' of being the breached company in the news, employees losing trust, proprietary product or data no longer being proprietary, subtle or overt alteration or disruption of digitally controlled systems or manufacturing processes and more. Just like other assets in your business, information is valuable and needs to be protected. The loss or misuse of your data can quickly put you out of business.

Of further concern to small business is a recent trend resulting from the rise of targeted attacks and more advance threats, and deep concerns about data protection, greatly raising the significance of third-party relationships, such as suppliers and partners. More potential vulnerabilities are being exposed along supply and data chains at the same time that regulators, customers and business' scrutiny of these are at an all-time high.

Small businesses will be increasingly required to comply with data policies and protection requirements of upstream partners like large retailers or distributors, and downstream partners like suppliers and contractors. Regulators in the US, Canada, the UK, France, Germany and other trading partner countries are looking ever more deeply at where breaches can and do occur. This results in the strengthening of the protection requirements, regulations and penalties, ratcheting up the pressure on small businesses to have better and better cyber protections in place.

What can you do to protect your business from a data breach? We'll try in this guide to outline some ways you can protect your business data. It's often easier and cheaper than you think - certainly cheaper than the cost of repair. Small businesses may also want to consider insurance to cover a data breach or intrusion. Often, insurance companies will be very helpful to small businesses as they plan data protections and backups.

Small businesses create, use and store information and employ many technologies (across the enterprise) in finance, manufacturing, design, human resources, healthcare, research, sales and more. Many small businesses interact digitally with big business, government and critical infrastructure technology elements like banking, shipping, supply chain management, insurance, compliance and even tax agencies. This extensive interaction makes small business an attractive target as the easier entry and/or end point of an attack.

Threats to your business data are not just external. Often an employee, disgruntled or otherwise, might seek to derive from or deprive you of the value in your data. Customer lists, sales plans, market strategies, research, recipes, manufacturing procedures - all the skills and know-how accumulated in your business may be at risk. Most importantly, these need effective protection in much the same way as cash, inventory and other valuables in one's business.

We haven't set about to scare, rather to raise awareness and to outline steps a small business can take to implement effective, viable and appropriate protections. Some steps are relatively easy and already available for many small businesses. Windows, for example, includes a file encryption function that makes sense for many while others may need a more robust cloud-based system. We'll try to help you determine which makes the most sense for your business. Data parsing, such as storing key data elements separately or creating employee numbers instead of using Social Security numbers, can often be easily and cost effectively implemented in a small business.