AMERICA'S SBDC NEW YORK

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.

CONTENTS

ACKNOWLEDGMENTS

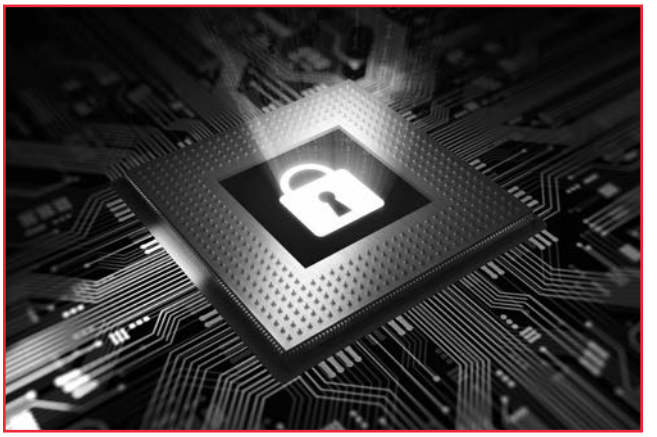
Contributing Author:
Thomas Morley, Director, Rockland Regional Center NY SBDC

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.

WHAT ARE THE LEADING CAUSES AND RISKS IN CYBERSECURITY?

There are many causes of data breaches, some obvious, some less so. To be secure it's sometimes necessary to approach a situation from a very different perspective than many of us are accustomed to. While we may think that our employees would never intentionally misuse company data or would never copy employee records, it just isn't that easy or simple. Let's take a look at some of the leading causes of data or cybersecurity breaches and general strategies for dealing with each.

Hacking and malware likely top our list of perceived threats. This refers to unauthorized access to your systems during which information may be viewed, copied or corrupted and during which additional software may be written to your systems [viruses and malware] which can do a host of unpleasant, costly things. Examples include 'keystroke recorders' (exactly what they sound like, they record every key stoke you make on your keyboard including passwords and such) and viruses that erase files. Sometimes this can be the result of inadequate or poorly configured 'firewalls' (the first line of electronic defenses keeping intruders out of your systems) or weakening anti-virus programs (from off-the-shelf solutions like Norton, McAfee or Kaspersky). Many systems now require increasingly robust hardware/software, network and endpoint protection systems like Sentinel One, Carbon Black, Cylance, or Barracuda. In any case, however, it's essential to data protection that you continue to update your protection, that you avoid the obvious like weak or repeated passwords, and more. Be sure to keep an eye on – and a lock on – the front, back and side doors of your data house.

Ransomware is software maliciously loaded onto your system that locks or encrypts your data, effectively preventing you from using it. Ransomware is now the fastest growing class of malicious software according to many experts and law enforcement. In recent years it has moved from simple screen blockers demanding payments to far more dangerous threats and higher ransom demands.

Ransomware attacks fall into two main categories: scareware and lockers. Scareware is a social-engineering attack that displays an official-looking notice of a fine, often for the PC having allegedly been used to view pornographic or other illegal material. Much more insidious, however, are locking or encryption attacks, which encrypt files, operating system kernels or a master boot record, then threaten to throw away the encryption key unless users or businesses quickly pay a ransom.

Unintended or accidental disclosure is not often thought of as a leading cause but in fact is one. These include postings on social media with too much information, lost or stolen tablets, laptops left running in hotel rooms, emails with sensitive data, attachments that go astray or to the wrong address, and password lists taped to monitors or desktops. You can take procedural preventive steps in this area with good employee awareness (training and periodic reminders or updates), a clear, written data policy for employees that includes strong, frequently updated passwords, social media and web browsing policies, email procedures and risk awareness training. Employees should be encouraged to trust but verify. If an unusual request is received by email, place a phone call to verify the sender and the activity. Use one of the many low cost email encryption and verification systems that are readily available (this doesn't change your email provider or address, just how you interact with your existing email). Consider using file encryption and file expiration software if you routinely send sensitive information (like tax returns, financial data or product designs).

Credit and payment card fraud is an area we often hear about in the media when it is on a large scale but that is often the tip of the iceberg. Small businesses are making increased use of card payments from websites to parts sales at industrial companies to invoice payment. Fortunately there are some good procedures, like PCI compliance which is promulgated by the payment card industry to software for use on your website to the

simple step of physically examining your credit card terminals for skimmers and such. Not to be ignored is the cost to your business for not being vigilant in the form of higher processing, settlement and monthly fees. We never want to think there are bad actors among our employees or the companies supplying our merchant services, but it does happen and awareness is effective and cheap.

Lost, stolen or discarded paper, portable devices and PCs are a constant weak spot in cybersecurity. From laptops to smartphones to PCs to USB drives to old paper files we are constantly replacing or losing or tossing out hardware that contains data. Think about it: have you ever lost a cell phone, or couldn't find that USB that was in your pocket, or replaced the PC on your desk with a sleek new one? Whether separately or as part of your company's overall data policy, it's important to have procedures in place to handle loss or disposal properly. Using readily available file encryption (it's included in many software systems like Windows or Apple OS), good inventories of hardware and shredding of paper files (often available on-site at a business for hundreds, not thousands, of dollars) to taking a hammer to that old hard drive (yes, physically breaking the hard drive does work), there are good procedures that can be cost effectively implemented when you're aware of and committed to protecting your data.

Bad employees are something that many of us don't want to think about or face but the reality is simple and the evidence is there. Employees are sometimes the root of the problem. It is important to be aware of the reality and some simple steps can be taken to help prevent theft or misuse of data by employees. Things like periodic inspections looking for skimmers, or audits looking for patterns and improper activity to digital controls like access logs, can help you take steps to know what has happened and who did it. (An access log is a list of all the requests for individual files that anyone may have requested or copied from servers or websites that get transmitted or used.) The access log (sometimes referred to as the "raw data") can be analyzed and summarized to keep you aware of what is happening in your business.

Cybersecurity for your business goes beyond good practices. It's about taking a consistent, committed approach to understanding the value of data and the costs of compromises to your data. It's about developing, implementing and updating policies, practices and procedures. It's about ongoing vigilance. It's about insurance (yes you can buy insurance for data protection). Above all, it's about common sense and appreciating the importance of cybersecurity to the health, profitability and long term survival of your business.

INFORMATION AS AN ASSET, IDENTIFY YOUR INFORMATION

A great first step to take is to identify and catalog the information in your business so you can begin to define effective strategies to protect and isolate. As noted, this is not a one-size-fits-all set of solutions. Each business needs to know what they have, why they have it and define strategies to protect it. We would never let all employees have the combination to the safe with the cash, checkbooks and corporate jewels, so we must create or strengthen the safe that will protect our data.

Start with an overview of all the information or data in your business. List all the types of information your business collects, uses, develops and stores; the ways in which you do it; the processes in place; and any regulatory or other compliance controls that affect or impact it. Knowing what you have is essential to defining your protection needs.

You might want to map out a table and include the following information to get started:

1) **Data Area** - A quick description of what kind of data
   Example 1: HR Information
   Example 2: Sales and quotes

2) **Information** - What is being stored, held or used?
   Example 1: Names, addresses, Social Security numbers, insurance information, salaries
   Example 2: Customer names, sales history (product & pricing), credit card data

3) **Where/What Form? -** Whate are the physical/electronic locations of the data, and what form is it in?
   Example 1: Filed paper from applications; scanned backups and Quickbook data files from payroll stored on department PCs
   Example 2: CRM files, QuickBooks export files, MS Word files for quotes, Excel for take-offs, paper copies, all PCs in sales

4) **Who Accesses?** - Who in the company can regularly access the data?
   Example 1: HR staff, finance/payroll clerk, insurance administrator, shop steward
   Example 2: All sales people, production staff

5) **Why?** - Why does the data exist in all the locations, and how does each person use the data?
   Example 1: HR as control and for insurances, Finance for Payroll, Insurance Administrator for benefits, Shop Steward for union issues
   Example 2: Ongoing sales & marketing, production planning

6) **External Factors** - Laws, regulations or policies applied by agencies, industries or government
   Example 1: HIPPA (laws regulating the use and storage of SS #'s, insurance/benefits, COBRA, etc.), State Tax Authority
   Example 2: Competitive, PCI compliance

You should list all information that is dealt with in the company. What may seem trivial could be a lynchpin to a secondary process. For instance, the use of a particular coatings supplier could give a competitor valuable information; storage of employee names and addresses with Social Security numbers in a spreadsheet on an owner or manager PC could lead to identity theft or employee poaching if compromised; not complying with PCI (Payment Card Industry) standards can lead to higher credit card processing fees and breach risks or a competitor who gains access to your warranty or service histories could improve their market strategies.

Next, we should evaluate how much and which information is really needed by all who have access. For example, does Marketing & Sales really need the detailed CAD presentation of a product for a marketing piece or product manual when a less detailed sketch, disclosing far less, would suffice? Does everyone in sales really need complete sales histories on all customers with access to credit card numbers or can you limit credit card access to fewer people? Yes, they might then need to get someone else involved in a transaction, but how many transactions does your company process weekly or monthly? Most common office software applications will permit security controls to limit who can view, edit or copy information. Fairly easy to use file encryption can be used to ensure that stored data is of no use if maliciously or inadvertently copied. It is important to review access requirements annually as requirements change routinely; it's not rude to change employee or contractor access, it's prudent.

STRATEGIES TO CONSIDER AS YOU ASSEMBLE A SUMMARY OF YOUR DATA

Parsing Information

You can separate or swap some data, e.g., use an assigned employee number instead of Social Security numbers on timecards or timesheets (a legal requirement for some), remove credit card numbers from CRM or sales reporting systems, use separate networks for critical functions like R&D or MRP; and if you provide open wireless for visitors use a separate Internet access path instead of the company's "regular network".

Procedures

You can modify how things are being done with information, e.g., require that all laptops used in the company use file encryption to prevent data loss if the laptop is lost; require that all CNC or other machine control code be stored off-line with backups physically secured in a cost-effective, fireproof container available at your local office supply store; if you have an IT person, staff or department can you require that all tablets, smartphones and laptops be brought in to the company routinely for anti-virus scanning, verification of updates, and installation of any new dedicated controls; not to mention the simple physical act of inventorying the equipment itself (you should always know where all of your equipment is).

Isolating and parsing information not just in files but in procedures is an effective strategy to limit the opportunities for misuse, theft or compromise. While this can be challenging in very small companies where "everybody does everything," taking a critical look at how data are used is an important step. If the inventory clerk doesn't process credit card sales, they shouldn't have access to credit card numbers. While engineering stores and uses information on current products and upcoming efforts, does product really need access to all of the information, or can that be separated until needed? Again, the strategy here is to think critically about who needs what.

Work Habits

This is an area where a little effort and attention to detail can go a long way. Be sure to train and re-train employees for specific procedures and for data awareness, data appreciation and data notification. Smart employees are a great resource in the battle for data protection and security.

The fewer copies of sensitive data that exist the simpler it is to control it. Many companies now use network printers and centralized copiers. How often have you gone to the printer to fetch your print job and found all or part of a previous print or copy job still there? Locate a cost effective shredder next to the printer/copier and have a procedure to shred anything that is left behind. Have a chat with the staffer who left it, the cost of an occasional reprint job will be minor compared to the potential cost of losing or disclosing sensitive information. And, while we're talking about printing, include in your data and information policy some guidelines for printing and following up with that which is printed. Depending on your business it might not be a bad idea to shred all paper documents when they are no longer useful and prior to recycling.

It's a good idea to include in your data policy (which should be part of every employee handbook and you should get a signed acknowledgement that the employee has received it) sections dealing with technology, data, remote or offsite work and the tools used like home computers, USBs, CDs or emailed files. Good practice dictates having some kind of checklist for any hardware device that contains data, e.g., all files must always be encrypted when being sent or carried, or the device must be inventoried and 'signed-out' (it's tough

to know what we may have lost if there's no records of the device and its contents). There are a number of simple steps, some already included in many PC operating systems, to help control/record data inventory. Windows, for example, lets you create and 'sync' files to a 'briefcase'. You can then routinely 'sync' the files in the briefcase with the files on your PC; and, you can encrypt the briefcase.

File encryption is another achievable procedure that is included in popular operating systems. From Apple's File/Vault to Microsoft's Bitlocker, data encryption is already at the fingertips of virtually all small businesses. Though not foolproof these are some easily achieved steps that can prove effective in many small business circumstances. Encrypted data cannot be readily read or recovered by anyone except the author, rendering a lost or misplaced USB or the email that goes inadvertently astray essentially useless. Using steps like this as part of our data or information 'procedures' can go a long way toward helping to secure access to and control of the information in our small businesses.

If your organization permits work at home consider using a VPN, controlled by the business, to ensure that access and file transfers are controlled, logged and encrypted. It's also a good idea to provide the hardware that remote workers will be using. This permits your business to configure and control the device(s) and its ability to access your network and data. It permits you to utilize appropriate software and systems to regulate the device. Again, the effort is to control the ability of others to see, copy, corrupt or use your sensitive information, or, information that puts you at risk.

Many companies, particularly those with highly sensitive information, may wish to establish policies preventing the use of USB storage devices. In some cases, it may even make sense to use software that precludes or prevents data downloads. It's an effective protection to implement that still allows employees to work with data. They just can't copy the file(s).

ENCRYPTION

Encryption comes in many forms. From advanced systems to literally a few clicks in Windows (right click the file/folder, select security, select advanced, select encrypt, done) or in Apple (click the folder, select encryption, choose your options or use the file/vault feature). Keep in mind that these features require you have a log in for the computer to identify the user and enable access. Don't set up file encryption and then leave the front door wide open. Encryption is especially important for cloud storage users. While your cloud provider is likely using an advanced encryption system while storing, your data are exposed during transmission or could be exposed if your cloud provider were to be breached. You'd be much more comfortable knowing that even if there's a breach, you still have some protection in place.

For many small businesses achievable encryption like this is an easy and effective step to protect and parse digital information. This, in conjunction with establishing 'users' on your company's computers, is an effective way of keeping Joe out of Mary's data. It also prevents data loss if your system is compromised from outside and data are copied, as the copied data will be useless to all but the most determined or advanced hackers.

For more sensitive or high value business situations it may make sense to utilize a commercial file encryption system. These are software systems that generally provide a level of encryption beyond File/Vault or BitLocker and will work across many platforms including cloud storage. Often these systems can be configured to encrypt data essentially anytime you're not actually using it, such as during transmission, storage, attachments to emails, etc. Again, it may sound complex but is achievable in many small businesses. With off-the-shelf encryption systems ranging from about $40 to $200 and available from well-known companies like Symantec or McAfee, encryption is not an expensive investment for small businesses that have valuable data.

You may hear about the Advanced Encryption Standard and its applicability. For some small business users it may be necessary or advisable to utilize a system that meets this standard. The origins of AES date back to 1997 when the National Institute of Standards and Technology (NIST) announced that it needed a successor to the aging Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks. This new encryption algorithm would be unclassified and had to be capable of protecting sensitive government information well into the next century. It was to be easy to implement in hardware and software, as well as in restricted environments (example: a smart card) and offer good defenses against various attack techniques.

The Advanced Encryption Standard became effective as a federal government standard in 2002.

In June 2003, the U.S. government announced that AES could be used to protect classified information, and it soon became the default encryption algorithm for protecting classified information as well as the first publicly accessible and open cipher approved by the NSA for top-secret information.

Its successful use by the U.S. government has led to widespread use in the private sector, leading AES to become the most popular algorithm used in symmetric key cryptography. AES is more secure than its predecessors -- DES and 3DES -- as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware such as firewalls and routers.

In case you're wondering how AES encryption works, here's a quick summary. AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric or secret-key ciphers use the same key

for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

As a cipher, AES has proven reliable. The only successful attacks against it have been side-channel attacks on weaknesses found in the implementation or key management of certain AES-based encryption products. (Side-channel attacks don't use brute force or theoretical weaknesses to break a cipher, but rather exploit flaws in the way it has been implemented.) The BEAST browser exploit against the TLS v1.0 protocol is a good example; TLS can use AES to encrypt data, but due to the information that TLS exposes, attackers managed to predict the initialization vector block used at the start of the encryption process.

Various researchers have published attacks against reduced-round versions of the Advanced Encryption Standard, and a research paper published in 2011 demonstrated that using a technique called a biclique attack could recover AES keys faster than a brute-force attack by a factor of between three and five, depending on the cipher version. Even this attack, though, does not threaten the practical use of AES due to its high computational complexity.

COMPUTER COMMUNICATIONS IN YOUR SMALL BUSINESS

While we may feel shackled to (or by) the complexities of technology and data communications, there are many options. Some we can do ourselves, while some may require assistance from our web developer, bank or other service provider. In either case, we aren't trying to turn you into a programmer, just an effective manager of information and data who knows what protections are needed. Let's start with a look at some common terms and set the landscape we must all deal with.

HTTPS, Hypertext Transfer Protocol Secure, refers to a data connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The primary purpose of HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data – so we can have a comfort level that we're talking to the place we think we are, are being understood correctly and are not being eavesdropped on.

While HTTPS provides authentication of the websites and servers with whom we are communicating, it also provides some protection against man-in-the-middle attacks through bidirectional encryption of communications between client and server. This protects against eavesdropping and tampering with or forging the data contents. In practice, this provides a fairly reasonable assurance that one is communicating with the intended website as opposed to an impostor, and ensures that the content being communicated between the user and site cannot be easily read or forged or mimicked by a third party.

Historically, HTTPS connections were used for payment transactions on the web, email and for sensitive transactions in corporate systems. In the late 2000s HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private - all features being increasingly demanded by users and customers.

As such, it's important to look at how your business is communicating data. You'll hear terms like SSL (Secure Sockets Layer) and the newer TSL (Transport Security Layer). While it's not necessary to understand the engineering behind these it's important to make sure you are using them when appropriate, and, using the latest versions.

To help understand the context, Transport Layer Security and Secure Sockets Layer are often referred to as 'SSL' and understood as cryptographic protocols for communicating securely over networks. Many versions are used and are generally transparent to actual users. TLS/SSL is used for everything from web browsing, email, Internet faxing, instant messaging and voice-over-IP (VoIP). Many major web sites use TLS/SSL to secure all communications between servers and web browsers.

TLS/SSL are the standard security technologies for establishing an encrypted link between a web server and a browser to ensure that data passing between servers and browsers remains private and with acceptable data integrity. TLS/SSL is an industry standard used by millions of websites to protect online transactions.

For your small business to use TLS/SSL your web server requires a Certificate. When you apply to get it for your server you must answer a series of questions about the identity of your website and your company, thereby enabling your web server to create the private and public cryptographic keys for each session.

Generally, the TLS/SSL Certificate includes your domain name, company, address, city, state and country along with the Certification Authority and the expiration date of the certificate. When a browser connects to a secure site it retrieves the site's Certificate, checks that it has not expired, was issued by a Certifier the browser trusts (included in all major browsers) and that it is being used by the website it was issued for. If it fails on

any of these validation points the browser displays a warning to the user letting them know that the site has a problem, may be compromised and importantly, communication and content are not secured as expected. At this writing we should note your systems should not be using TLS1.0, only versions 1.1 and 1.2.

The primary goal of the TLS/SSL protocol is to provide privacy and data integrity between two communicating computer applications. When secured by it, connections between the client (e.g., your customers or supply chain members) and the server (e.g., your small business) have the following properties:

1. The connection is private because symmetric cryptography is used to encrypt the data being transmitted. The keys for this encryption are generated uniquely for each connection and are based on a secret negotiation at the start of the session, the 'handshake'. The server and client negotiate the details of the encryption algorithm and cryptographic keys to use before any data is transmitted. The negotiation of a shared secret (the keys) is secure because the negotiated secret is unavailable to eavesdroppers and cannot be obtained, even by an attacker placed in the middle of the connection and reliable since any modification of the communications during the negotiation will be detected.

2. The identity of those communicating is authenticated with public-key cryptography. This authentication is optional, but is often required for the server.

3. The connection is reliable, has data integrity, and an authentication code, preventing loss or alteration of the data during transmission.

Additionally, careful configuration of TLS/SSL provides other privacy properties like forward secrecy, so that future disclosure of encryption keys can't be used to decrypt recorded TLS/SSL communications. TLS/SSL, like many software systems, supports several methods for exchanging keys, encrypting data, and authenticating messages. As a result, secure configurations using TLS/SSL involves many options. While not all options will provide all of the privacy-related properties it is important to work with your developers to assess and understand the level of security necessary for your business and your customers. As we might imagine, a local delicatessen publishing an on-line menu has a different security requirement that the local bank or credit union.

Employees

We're not going to get into all of the nuances, requirements and the many other issues associated with hiring and firing employees in this guide. But, be sure your HR systems and applications processes are set up to include background checks, certification validation and policy acknowledgements – always know who you're hiring!

We all know how important it is to handle HR correctly. It's kind of like insurance, often unpleasant to think about and deal with but when it's needed it's great to have it and have it done right. We can't cover all HR eventualities in this guide but here's a few sample things to think about or include in your employee handbook. We can't cover social media policies and other reputational issues in the guide but there are many resources to help your company with these issues.

The following sample text isn't legally approved language. It is a general suggestion to help you define policies that are functional but should be tailored to your company, business situation and the regulatory environment applicable to your business and business locations. Be sure to check with your legal counsel or attorney before defining langauage in any employee policy statement, guideline or handbook.

Policy statements should include a simple stated Objective. It helps understanding and clarity:

[Your Business] recognizes that use of the Internet and e-mail has many benefits and can make workplace communication more efficient and effective, and the company recognizes the importance, value and confidentiality or company information. Therefore, employees are encouraged to use the Internet and e-mail systems appropriately and to comply with all information controls, management and confidentiality requirements. Unacceptable use of the Internet, e-mail or company information can place [Company] and others at risk, may violate laws and can place the company at risk for loss of market share, competitive advantage or research advance. This policy outlines some of the guidelines for acceptable use of technology, the Internet, e-mail and information.

This policy must be followed in conjunction with other [Your Business] policies and guidelines governing appropriate workplace conduct, behavior and governing the use of company systems and assets including information. [Your Business] complies with all applicable federal, state and local laws as they concern the employer/employee relationship, and nothing contained herein should be construed to violate the rights or responsibilities contained in law. Employees are reminded that many laws also deal with the use and disclosure of company information, and company held data such as personally identifiable information, credit card data and the like, which is protected by law and the company will pursue vigorous prosecution under the law for misuse of company, customer or other information entrusted to the company.

[Your Business] has established the following guidelines for employee use of the company's technology and communications networks, including the Internet and e-mail and information, in an appropriate, ethical, compliant and professional manner. Though not included here, additional policies and procedures concerning the use of technology and information may be posted, distributed and/or amended by the company from time to time and employees are expected to be aware of and comply with such policies and procedures at all times.

All technology provided by [Your Business], including computer systems, communications networks, company-related work records and other information stored electronically, is the property of the company and not the employee. In general, use of the company's technology systems and electronic communications should be job-related and not for personal convenience.

Employees may not use [Your Business]'s Internet, e-mail or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.

Disparaging, abusive, profane or offensive language; materials that might adversely or negatively reflect on [Your Business] or be contrary to its business interests; and any illegal activities—including piracy, cracking, hacking, extortion, blackmail, copyright infringement and unauthorized access to any computers or data are expressly forbidden.

Copyrighted materials belonging to entities other than [Your Business] may not be transmitted by employees on the company's network without permission of the copyright holder. Employees must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy for reference only. Saving copyright-protected information to a network drive without permission is prohibited. Sharing the URL of an Internet site with other interested persons for business reasons is permitted.

Employees may not use the systems or technologies in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and "spamming" (sending e-mail to thousands of users.)

To prevent contamination of [Your Business] technology and communications equipment or systems by harmful computer viruses, malware, ransomware or other digital threats, downloaded files must be downloaded or used consistent will all IT policies and procedures; and, given that many browser add-on packages or "plug-ins" or other software, drivers and executable code may not be compatible with other company programs, may cause problems for company systems or place the company or its information assets at risk of misuse or disclosure, downloading or installing such items is prohibited without prior permission from IT.

Every employee of [Your Business] is responsible for the content of all text, audio, image or data files that he or she places or sends over the company's Internet and e-mail systems. No e-mail or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else. [Your Business]'s corporate identity is attached to all outgoing e-mail communications, which must reflect corporate values and appropriate workplace language and conduct at all times. It should also be noted that the company may pursue additional actions against employees who violate the technology and information policies of the company including sanctions beyond dismissal such as prosecution under applicable local, state or federal statutes, and, that the company will cooperate fully with law enforcement or other agencies investigating or prosecuting relevant to technology or information.

Employees do not have any expectation of privacy for any e-mail and other electronic communications transmitted by, on or using Company equipment, systems and networks and all such communications are the property of the company subject only to regulation and limitation in law as may be applied to communications concerning employee's personal data. Therefore, [Your Business] reserves the right to examine, monitor, record and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite without notice of any kind to employees.

Internal and external e-mail, voice mail, and text messages are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the company.

Company's Right to Monitor and Consequences for Misuse: All company-supplied technology, including computer systems, equipment and company-related data, information and work records, belong to the company and not to the employee user. Employees understand the company routinely monitors usage, use patterns, content and activity, and employees should observe appropriate workplace discretion in their use and maintenance of such company property.

Because all the computer systems and software, as well as e-mail and Internet connections, are the property of [Your Business], all company policies apply to their use and are in effect at all times. Any employee who abuses the company-provided access to e-mail, the Internet, or other electronic communications or networks, including social media, may be denied future access, and, if appropriate, be subject to disciplinary action up to and including termination, and/or prosecution, within the limitations of applicable federal, state or local laws.

The use of company systems, such as email, on a non-company or privately owned device, such as a cell phone, tablet or personal computer are also subject to all applicable company policies and procedures, and employees do not have an expectation of privacy in such circumstances. By an employee's use of any company system with a non-company device, the employee grants authority to the company to inspect, search, monitor

or record any company related activity on such device consistent with policies of the company.

Questions regarding the use of company technology should be directed to your manager, supervisor, HR or the IT department.

One effective way to avoid the personal device used on company system confusion and challenge is to create separate Internet 'Guest' account/access. Such an account, usable by visitors to the company and employees needed or wanting to check personal email and such can use the visitor account without compromising their expectation of privacy on a personal device. Further, such a strategy provides an excellent mechanism to further isolate sensitive company networks from casual usage and 'open pathways'.

Privacy Policy

Privacy policies are a little bit different than technology policies and speak more to how data and information are handled in and around your business. Often these policies are issued by a department or group within the company. Human Resources will have privacy policies driven in large part by law and regulation while Engineering or Sales will have policies driven largely by confidentiality or export regulation. Finance or Sales will have policies driven by the use of credit cards along with confidentiality.

The items that follow are not legal advice. They are suggestions to help you define policies that are functional but should be tailored to your company, business situation and regulations applicable to your business and business locations.

Your policies, and as noted earlier, training, training, training, should focus on How Employees Handle Data, Use Mobile Data – Where It Is, How It Moves, and How Data Are Treated at PCs or Workstations

Your business needs to protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid negatively impacting customers. The protection of data is a critical business requirement, while keeping in mind that flexibility to access data and work effectively is needed.

Employees and contractors (everyone from contract programmers to accountants) with access to the company's data need to be aware of what company data are, what restrictions may apply and, when in doubt, ASK for guidance. Data may be financial, developmental, customer, supply chain, marketing or planning.

Use a security awareness training program (several are commercially available and many local colleges or universities have materials available) to help your employees understand the issues and needs. Well educated employees are a great asset in protecting data.

Set a clear visitor policy as appropriate for your business. Be sure to cover simple direct policies about escorting visitors, identifying them and responding if something unusual occurs. Often, your insurance or safety providers will have policies that can provide a good template to use.

Several direct and simple policy statements can go a long way to protecting your data and the data of your customers. Assure that employees know, and appreciate, the significance of, and restrictions to, any data they are handling. Never permit the use of non-company email systems for any company data. Be sure desks, printers and copiers are kept clean and that no company data are left exposed. Use secure passwords and access controls (more on password policies a bit later). Use access controls and access logs so you'll know who has been accessing sensitive data. Terminated or departing employees must immediately return all data and devices, so be certain that your IT department/staff coordinate with HR to promptly prevent access by any

departing employees. Be certain to inventory ALL mobile devices and the data contained on them, and have an easily accomplished notification system for any suspected breach, loss of a device or data, or unusual activity. Lastly, be sure that any data being moved is subject to a specific company policy – from the simple emailed monthly QuickBooks file to the accountant to the transfer of new engineering data to a customer.

If your business permits off-site or remote work by employees it is essential to have a policy regulating this and to build in appropriate controls like VPN (virtual private network), encryption and periodic reviews of hardware and software systems.

And, not to be too redundant, but have a good support system in place to encourage employee compliance with data awareness and reporting of any known or suspected breach. Be sure employees know the importance and sensitivity of data, who to call, when to call and how to help deal with a potential data breach or loss.

While it is true that no policy can deal with all potential threats, attacks and plain old mistakes, particularly in a small business, awareness and quick response are excellent tools to mitigate loss and damage. Simple steps like a live or telephone confirmation of an unusual request can often be the difference between an attack thwarted and a successful one.

MAKING TECHNOLOGY CHOICES

It is important, particularly in small businesses, to choose technology carefully and purposefully. Yes, many small businesses can't readily afford to always be on the forefront of data processing technology. However, it is important to have a technology plan that meets both internal and external needs. Plans that integrate policy, training and procedure to ensure good value for invested capital also ensures good operating returns and fits within your cyber and data security plans.

Often, applying a set of critical questions to a technology acquisition will provide many small businesses with a great start to a good decision. Begin with an appraisal of the current state of your technology and systems – how old is your current hardware, hold old is the software, have updates been routinely applied, does it continue to meet your operational needs, and if not, determine why. Are your operating systems up to date? Are 'compatibilities' becoming an issue with new software or hardware, with customers, with suppliers, with production systems, with design and research or engineering efforts, with your industry or market sector as a whole?

Costs, naturally, are an ever-present concern in small businesses. Do the same sort of cost analysis for technology that you would do for any other capital expenditure in your business. What will this investment enable, what savings or productivity increases will it generate, what sales or marketing efforts will it support, is it a required purchase or update in response to a customer requirement, etc.

Technology can often advance a small business and should be looked at in that context as well. Can a new technology provide a market edge over the competition? Will it set you apart from others in a positive way? For example, would the addition of 3D printing help you to better sell a customer for whom your business manufactures parts or components by making your business a more integral part of your customer's development process? Would enhanced graphics capability better support merchandising efforts by your customers?

The essence of your technology choice is direct: what will it do to advance the business and what is my payback? And, how will I incorporate it into my cybersecurity plans?

SOME BASIC RULES AND GUIDELINES FOR SMALL BUSINESS CYBERSECURITY

Insurance

We insure our businesses to protect against specific risks. Loss or corruption of data is a risk, so you should seriously consider insurance. And, like many insurance purchases, data breach or loss insurance often will be accompanied by a suite of tools and services the insurance company wants you to use to better control their exposure. So, two birds with one stone, protection and a set of experts, tools and programs to enhance protection - certainly worth considering.

Firewalls

Like the name suggests, a firewall is a barrier to getting into your data systems. It's your first line of defense against external access to your systems and data. Be certain to apply firewalls to all points of access. While they may be programmed somewhat differently depending on what you're protecting, never leave any of your access points unprotected. From stock operating system firewalls in Windows and Apple iOS, to full-on hardware/software systems like Barracuda, you can select a firewall that makes operating and economic sense for your business or as required to meet a specific requirement. If you provide wireless for customers or visitors, use a separate Internet connection apart from your company connection. For a few dollars monthly it's cost effective protection, and it can have some side benefits. If you permit employees to use sites like Facebook or Twitter while at work, be sure they use the 'visitor' wireless and keep the traffic – and risk – off your business systems.

Configuring Wireless Access

Many small businesses make extensive use of wireless systems. They're cheaper and easier to install and so much hardware and software is built for wireless access. Wireless security can vary greatly and it doesn't really take much effort to do it better. All too many small businesses are still using WEP (Wired Equivalent Privacy) which is a security protocol, specified by IEEE standard, 802.11b, designed to provide a wireless local area network with a level of security and privacy comparable to what could expected of a wired network (wired local area networks have the added protection of physical security mechanisms like controlled access to the building, and are effective for a physical environment but are ineffective for wireless because radio waves are not limited by the walls.

WPA2, the acronym for Wi-Fi Protected Access 2 - Pre-Shared Key, is a method of securing a network using an optional Pre-Shared Key (PSK) authentication. Though originally designed for home users without an enterprise authentication server, WPA2 provides much greater protection than WEP and is often as simple to apply as reading the sticker on the side of your wireless modem or router.

To encrypt a network with WPA2-PSK you provide your router not with an encryption key (which can be a complex procedure), but rather with a plain-English passphrase of 8 to 63 characters. Using a technology called TKIP (Temporal Key Integrity Protocol), the passphrase and the network SSID (Service Set Identifier, a 32 character unique ID attached to the header of packets sent over your wireless local-area network that is like a password) combine to generate unique encryption keys for each wireless client and then constantly change the keys (unlike WEP which is limited to static keys). If your Internet provider, whether via cable or phone company, doesn't have this info on your modem/router, call and get your system upgraded.

Anti-Virus, Malware, Spyware Software

There are many providers in this arena, again ranging from simple off the shelf software systems to highly advanced hardware/software systems and third party monitoring. For many small businesses a good software system is likely adequate. However – and that's a big however - having a system and not updating it regularly is like not having a system at all. Don't be penny wise and pound foolish with cyber protections. Most systems are quite cost effective, i.e., less than $100 annually. For context, computer viruses, like their human counterparts are bits of code that can infect, causing a host of serious issues. The digital equivalent for an antibiotic is anti-viral software which can diagnose, quarantine and/or eliminate virus code.

Malware refers to software that infects and attacks your system a bit differently than a virus. It can freeze your system, preventing you from using your own computer. It can hijack your data (ransomware), which will demand payment to let you once again access your data. Spyware is in some ways the most insidious. It looks to copy and transmit data, sometimes including keystrokes, to somewhere else. Why? Well your system just logged into anybank.com, the next thing you type is your username, then your password. That can be quite interesting information for someone other than you. Get an appropriate system, put it in place, keep it updated and be sure no employees are working to circumvent it. One easy way to control circumvention is to restrict the 'Administrator' of each computer to the IT department or person. This prevents the local or assigned user from installing software without IT approval. It's not perfect but a very helpful step.

Ransomware

"Ransomware is now one of the fastest growing classes of malicious software," says Fedor Sinitsyn, a senior malware analyst at the security firm Kaspersky Lab. "In the last few years it has evolved from simple screen blockers demanding payments to something far more dangerous."

Ransomware attacks generally fall into two categories: scareware and lockers. Scareware is a social-engineering attack that displays an official-looking notice of a fine, often for the PC having allegedly been used to view pornographic or other illegal material. Much more insidious, however, are locking or "encryptor" attacks, which encrypt files, operating system kernels or a master boot record, then throw away the encryption key unless users or businesses quickly pay a ransom.

Though frightening, there are effective strategies business of every size can employ to minimize and offset ransomware attacks often reducing a potential impact of substantial economic damage to a mere nuisance with minimal restore and recovery costs.

Employ Anti-Malware Tools

Ransomware, as the name implies, is a form of malware, and often can be blocked by anti-virus or anti-malware engines that correctly signature-match malicious code. But many related attacks - often launched via phishing e-mails, fake downloads, and malicious URLs - originate more often with "crimeware" toolkits, which can exploit any of a number of vulnerabilities to install malware. Furthermore, by the time any ransomware is detected, an infected PC may already have played host to malware designed to steal financial or other data, launch distributed denial-of-service attacks or relay spam.

For example, ransomware known as "Critroni CTB-Locker" as well as "Onion," recently discovered by malware researcher Kafeine, is distributed by the Andromeda bot. This first infects PCs with an e-mail worm designed to send spam e-mails and download further attack code notably Critroni ransomware.

Similarly, Cryptolocker was being pushed to PCs that were first infected by Gameover Zeus which attackers used to steal financial information then encrypted infected hard drives, holding data hostage to increase profits.

In our increasingly mobile world ransomware attackers are now targeting Android devices. To defend against these, be sure employees with Android devices use anti-malware software and procedures. Many of these tools include cloud-based backup, enabling infected devices to be wiped and restored, which many security experts say is the only reliable way of eliminating ransomware infections.

A growing number of ransomware attacks are now targeting servers with Windows server ransomware being the most prevalent, leaving small and medium-sized firms particularly at risk.

Backup Everything, Regularly, Routinely, Repeatedly

As digital memory has continued to become less and less expensive, our ability to back-up more data has become increasingly simple and cheaper. Having a complete, clean, backup data set is a great offset to ransomware. Your ability to replace your data on infected systems can be a nuisance, might have a small cost and is likely a bit disruptive for a short period of time but it's a far cry from losing all of your data.

So, one of the best ways to battle ransomware that locks down servers or other systems is to maintain offsite backups. "Encrypting data is the equivalent of destroying it; the protection against the destruction of data is to make copies," says security consultant William Hugh Murray.

Murray acknowledges that most enterprises already back up corporate data to an offsite location. But he warns that too often, these backups can be directly accessed from the system where the data originated. Many cloud-based services, like Dropbox, allow access to storage directly from a user's file system. Instead, Murray says offsite or cloud-based backups must not only be stored offline, but also made to be not directly accessible from the originating system. "If the file system can access the offsite or cloud-based backup, so too can the ransomware." Murray says.

On the one hand, ransomware is very scary – the encrypted files are damaged beyond repair. But if you have properly prepared your system, it is really nothing more than a nuisance. Here are a few strategies to help keep ransomware from ruining your small business.

The single biggest thing that will defeat ransomware is having a regularly updated backup. If you are attacked with ransomware you may lose that document you started earlier this morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from backup, you can rest easy. Remember, ransomware like Cryptolocker encrypts files on drives that are mapped - including any external drives such as a USB, as well as any network or cloud file stores to which you've assigned a drive letter. So, what you need is a regular backup regimen, to an external drive or backup service, one that is not assigned a drive letter and is disconnected when it is not doing a specific backup. And, have multiple backups to help ensure that you haven't backed up the malware and have more than one choice of data sets from which to restore.

Always show hidden file-extensions since many malware or ransomware files frequently arrive with the extension PDF.EXE, counting on Window's default settings of hiding known file-extensions. If you re-enable the ability to see the full file-extension, it can be easier for employees and users to spot suspicious files - not perfect but a good step in a good direction.

If your gateway mail server has the ability to filter files by extension, you should deny mails sent with ".EXE" files, or to deny mails sent with files that have two file extensions, the last one being executable ("*.*.EXE" files, in filter-speak). If you do legitimately need to exchange executable files in your particular business and want to deny emails with ".EXE" files, you can use an internal standard like zipping or encrypting files during the exchange.

You can create rules in Windows or with certain protection software to disallow a particular behavior used by Cryptolocker, which is to run its executable from the App Data or Local App Data folders. Again, if your business needs to run software from this area you likely have the skills to create the exception rules.

It is common for ransomware and malware like Cryptolocker/Filecoder to access target machines using Remote Desktop Protocol (RDP), which is a Windows utility permitting others to access your desktop remotely (sometimes used in support and repair applications). If you do not require the use of RDP, you can disable it to further protect your systems from these and other RDP exploits.

To disable Windows Remote Desktop

1. Click System in Control Panel.

2. On the Remote tab, clear the Allow users to connect remotely to your computer check box, and then click OK.

Note: You must be logged on as an administrator or a member of the Administrators group to disable the Remote Desktop feature.

Ransomware authors often rely on the fact that many businesses run outdated software with known vulnerabilities, which can be exploited to access your system. You can significantly decrease the potential for ransomware pain and impact if you routinely update your software. Some vendors release security updates on a regular basis (Microsoft and Adobe both use the second Tuesday of every month), but there are often unscheduled updates in case of a sudden known threat or critical update. Enable automatic updates if you can, or go directly to your software vendor's website, as malware authors sometimes disguise their works as software update notifications.

It's always a good idea to have both anti-malware software and a substantial firewall to help identify threats and suspicious behavior. Malware is frequently sent by new variants to avoid detection, which is why it is important to have layers of protection.

If however, you have run a program you suspect to be ransomware, there's a couple of things to try immediately. Disconnect from WiFi or unplug from the network immediately. Breaking the physical connection can be important to minimizing or reducing the impact.

If you have System Restore enabled on your Windows machine, you might be able to take your system back to a known-clean state. But, again, you have to out-smart the malware. Newer versions of ransomware like Cryptolocker can have the ability to delete these shadow files from System Restore so they won't be there when you try to replace the damaged versions reinforcing the need for an effective backup strategy.

Passwords

Where to begin? Simply put, the longer and more complex the password the safer your systems will be. Poor password procedure is like leaving the keys in the car, while it is running, and parked on a busy street,

with the windows open, and a 'Steal Me' sign in the window. The role that passwords play in securing small business networks and data is often underestimated and overlooked. Passwords are a key line of defense against unauthorized access to your system and data.

Weak passwords provide attackers with easy access to your computers and network, while strong passwords are considerably harder to crack, even with password-cracking software available today. Password-cracking tools continue to improve, and the computers that are used to crack passwords are faster and more powerful than ever. Password-cracking software uses one of three approaches: intelligent guessing, dictionary attacks, and brute-force automated attacks that try every possible combination of characters. Given enough time, the automated method can crack any password. However, strong passwords are much harder to crack than weak passwords. And, control systems that lock accounts after several failed attempts or that add increasing intervals to the password retry are a great protection against brute-force attacks. All computers in your small business should take advantage of 'user account' features that are part of virtually all operating systems. Each user of a computer should have his/her own account. Setting up user accounts is quite easy and it means that when you use the computer it knows it's you, accesses your data, your security profile and limits, etc., and can be quite helpful in a small business where shared hardware can be an issue.

A weak password is essentially no password at all. Passwords like 'guest' or 'password' are especially weak. Passwords with user or personal or company names are not good. Think about how your bank or credit card company requires you to set a password. Yes, there is a reason for the complexity – it makes for a much better password.

A strong password is at least seven characters, does not contain identifiable data like 'tomsdeskpc' and contains characters from the four character groups: upper case letters, lower case letters, numbers and symbols.

Consider the use of 'pass phrases' much like a password, but a lot longer and tougher to guess or brute-force past.

It is also essential to have strong policies around passwords. Apart from the obvious (like they cannot be written on a note on the desk), they can't be shared, they must be changed regularly and must be changed immediately if there is even a suspicion of a password having been compromised. And – quite importantly – you must require that different passwords be used for different functions. With the convergence of external systems using emails as a system login, many people use the same password across many functions – not a good idea. Require a different password for each different application. Not only will this make each application inherently more secure, it can dramatically slow the access of a compromised account across the enterprise.

Your password polices should take the nature and sensitivity of your data into account. An isolated visitor Internet access point with Guest as a password is likely OK but you probably want to change bank and similar access passwords frequently, perhaps quarterly, to be practical. If you have a system administrator you can also run password software that will check against previously used passwords, or overly simple or just not meeting the rules that you've set, i.e., must include one uppercase, one lowercase, one number, one symbol, must be at least 12 letters, etc.

You can create passwords that contain characters from the extended ASCII character set. Using extended ASCII characters increases the number of characters that you can choose, which would take more time for password-cracking software to crack. Before using extended ASCII characters in your password though, test them to make sure that extended ASCII characters are compatible with the software and operating systems your business uses. Be especially cautious about using extended ASCII characters in passwords if your organization uses several different operating systems. (Side note: Windows passwords can be up to 127

characters long. That's a bit extreme, especially if any computers on your network are running Windows 95 or 98 which only allows 14 characters.)

Physical Cybersecurity

Don't forget the simple steps like locking file cabinets, desks and offices where computers and data are kept. It's tough to access a computer that isn't on a network and is in a locked room or quite simply is turned off. While it's said that locks are for honest people, they can take away crimes of opportunity. Use paper shredders and place them near areas of sensitive data. If it's necessary to print sensitive data during use, be sure you can get rid of it when you're done. Remember, it's not illegal to rummage garbage that is left outside a structure. Many of us will never be the object of such an attack, but some recent media about a new product or contract could raise interest among competitors or landlords or opportunists. Have normalized procedures in place as effective adjuncts to your cybersecurity policies and that plug the physical holes often found in cyber security efforts.

We discussed mobile data a bit earlier but to reinforce – always protect laptops, tablets and smartphones. Know where they are and what data are on them at all times. Be sure data are encrypted. Set policies regulating usage and let all staff know the policies are serious and will be enforced.

Outsourcing

Many small businesses outsource many functions from accounting to software development to supply chain interaction to marketing to cloud storage. Cybersecurity is a concern every step of the way. Like any chain, it's only as strong as the weakest link. Don't be fooled into thinking that just because you outsource critical applications or store information offsite, at a supposedly secure datacenter or cloud provider or ISP, that you are not responsible for that data. If you are outsourcing any of your operations or data management to a service provider you must constantly be asking that provider how they address your cybersecurity. It's important to note that you're still 100% liable for a breach – even if it didn't happen on your hardware. So before you outsource any business functions, such as payroll, Web hosting or customer service, investigate each company's cybersecurity and data privacy systems and practices, and make sure they are adequate for your needs.

BACKUP YOUR DATA

An integral part of your cybersecurity plan is data backup – and control of those backups since they are another copy of the data.

An integral part of your cybersecurity plan is data backup – and control of those backups since they are another copy of the data. No that's not a typo – we can't really say it often enough: backup, backup, backup. The cost of memory has entered the realm of almost trivial, and the speed of communications is moving beyond our ability to complain about how long something is taking. There's no reason to not be frequently backing up your data with on-site, off-site and disconnected copies. Inventory and control the copies. After all, they are copies of your data and are valued the same as all of your other data. Don't backup to a USB and then toss it to a family member to record the latest video share – return it to specific physical control for ongoing inventory.

The key strategy of data backup is to maintain the ability to quickly re-build or restore your data from a known point. The known point is key. If your business has been hit with malware or ransomware, having a good series of backups gives your security team the tools needed to get your business back up and running.

Depending on the nature and volume of your business, backups can be done on short or long intervals. If your transactional volume is low and has readily available paper backup (like invoices or sales orders), a weekly backup can be appropriate as it might only be a few hours of data entry to 'catch-up'. Conversely, if you have a high transaction volume like we might see in banking, a daily backup likely makes more sense. You need to evaluate the time and cost of rebuilding the interval that wasn't backed up to make a good decision. And don't forget to decide which data are backed up on which cycle. Don't forget that daily operating data are also important. All of those letters, quotations and customer correspondence on your desk top PC are as difficult to replace as financial data, so be sure to include those data elements in your plan.

Next, decide how and where to execute the backups. A few principles are important to keep in mind. Backups need to be clean data copies, should be on-site and off-site (in the event of fire or local destructive event like a storm, or flooding, or your PC fails). How will you apply controls like a data inventory? How will you address seemingly simple things like naming your backup files (to be sure you know which ones to use)? What will your backup destruction policy be (i.e., how many copies will you keep and for how long)? Will you use a manual or automated system?

Many modern operating systems, like Windows or Apple iOS, have a range of features already built-in to help with backing up. Be sure though to start at the beginning as you make your plan. By that we mean use all of the tools available to you, from directory and file structures to file naming conventions. If you store all of your data on a computer in some obscure directory that is not included in the backup, well, it just won't be there when you need to rebuild.

In the Windows Operating System:

Open Backup and Restore by clicking the Start button Picture of the Start button, clicking Control Panel, clicking System and Maintenance, and then clicking Backup and Restore.

Do one of the following:

If you've never used Windows Backup before, click Set up backup, and then follow the steps in the wizard. Administrator permission required If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

If you've created a backup before, you can wait for your regularly scheduled backup to occur, or you can manually create a new backup by clicking Backup Now.

Always store media used for backups (external hard disks, DVDs or CDs) in a secure place to prevent unauthorized people from having access to your files. We recommend a fireproof location separate from your computer. You should also encrypt the data on your backup.

To create a new, full backup:

After you create your first backup, Windows Backup will add new or changed information to your subsequent backups. If you're saving your backups on a hard drive or network location, Windows Backup will create a new, full backup for you automatically when needed. If you're saving your backups on CDs or DVDs or USBs and can't find an existing backup disc, or if you want to create a new backup of all of the files on your computer, you can create a full backup.

Here's how to create a full backup:

1. Open Backup and Restore by clicking the Start button Picture of the Start button, clicking Control Panel, clicking System and Maintenance, and then clicking Backup and Restore.

2. In the left pane, click Create new, full backup.

In an Apple system:

Back up with Time Machine: With Time Machine, you can back up your entire Mac, including system files, apps, music, photos, emails and documents. When Time Machine is turned on, it automatically backs up your Mac and performs hourly, daily, and weekly backups of your files.

When you use Time Machine on a portable computer, Time Machine not only keeps a copy of everything on your backup disk, it also saves “local snapshots” of files that have changed on your internal disk, so you can recover previous versions. These local snapshots are made hourly unless you turn Time Machine off, and they’re stored on your portable computer’s internal disk. If you accidentally delete or change a file, you can use Time Machine to recover it.

Time Machine's Starfield

Even though Time Machine creates local snapshots on your portable computer, you should also back up your files to a location other than your internal disk, such as an external hard disk, a disk on your network, or a Time Capsule. That way, if anything ever happens to your internal disk or to your Mac, you can restore your entire system to another Mac and get all your information back where it belongs in no time.

Attach an external hard disk to your Mac and turn it on. You're asked if you want to use the disk to backup your Mac. Click Use As Backup Disk, then follow the instructions in Time Machine preferences.

To open Time Machine preferences, choose Apple menu > System Preferences, then click Time Machine. From there you can choose a backup disk and set encryption options; start, pause, and resume a Time Machine backup; and restore items backed up with Time Machine.

Be sure to keep your Time Machine backup disk secure.

As you can see, backups really can be pretty easy.

If your data backup and security needs are more extensive than locally programmed, performed and stored backups; or if you're working on multiple platforms and operating systems; or have remote workers and locations; or also utilize portable devices, you should consider cloud or automated off-site storage or using a backup service. A February 24, 2016 PC magazine article compares several remote, cloud-based backup services. Large services like Iron Mountain, Barracuda and many others have scalable solutions. A Google search for data center backup will provide a plethora of choices.

APPS AND APPLICATION OR SOFTWARE DEVELOPMENT

Lately, it's not uncommon for many small businesses to be in a position either to develop internally or with external resources new software applications or apps for mobile devices. From customer loyalty programs to inventory inquiry and sales support programs, small businesses are often creating new uses for technology.

It is essential in the development process to consider cybersecurity – on multiple levels. Start with who is developing the application or program design, the English language description of what the software or code will do, who will be actually writing the code, who will test and integrate the new code or application into your current systems and procedures, and how will you monitor the entire process from an operations and cybersecurity perspective. Ask questions throughout the process. Is it necessary to access all the data being requested? Can data tables be parsed to better isolate critical elements? Can you limit the visible or transmitted data to better protect it? Can you parse the functions of the software, performing some operations in-house on well-controlled systems and then 'push' results to the app? Remember, a critical eye in the development process can save greatly downstream.

Additionally, what are the cybersecurity protocols of your web host? Are their security certificates and registrations correct and current? Do they subscribe to a set of procedures with which you (and maybe your insurance carrier) are comfortable? What are the protections available to your business should one of their employees or contractors create or cause a breach or similar security error?

Security is not the sole responsibility of the developer. It's everyone's. Foster a healthy environment of mutual responsibility and accountability from all involved. What is your development lifecycle, what are the priorities, what are the specific objectives?

Often the lifecycle steps to software development are Planning, General Design, Testing, Implementation or Operation, Updating, and ultimately, Decommissioning.

In Planning, be sure to consider cybersecurity requirements and potential regulatory issues (are you asking for personal information, will people under 18 be using it, etc.), what is your 'risk tolerance' to misuse of the software.

General Design often addresses the 'look and feel' of the software, how it works, what the screens look like, etc. Again, assess at this step how much data and processing needs to occur at the device vs. in a more controlled environment. This is a good step to begin including threat modeling, who might be interested in opportunities presented by the software, why, how might it be attacked, etc. Consider your overall security architecture, credentialing and authentication, access control, data transfer protocols, encryption, data clearing at the device, buffer controls, etc.

Testing is pretty self-explanatory. Try it out. Does it do what it was designed to do? Try all possible command configurations, emulate all software actions and interactions. Financial or other high value or high sensitivity applications might merit the services of 'white hat hackers,' security companies that will try to break your code or hack your software – on your behalf – and try to identify vulnerabilities to be addressed.

Implementation or Operation is the actual distribution and use of the application or software. Have a plan to roll out in stages to ensure constant control. Monitor usage patterns and comments to be sure your testing was effective. Threat vectors evolve in much the same way as software. Be sure to stay on top of evolving threats that may be indirect (i.e., via operating systems or browsers in addition to direct threats).

Updating is the process by which you continuously update and improve the software or application in response to evolving need, changing business logic or customer demand. How will you 'push' updates to users? What is your compatibility process and requirement? How long will version 1 work after version 2 is issued? Compatibility can also raise cybersecurity concerns. If an update addresses security issues present in previous versions, how will you be sure your update is making the needed fix moving forward?

Decommissioning is the process by which you terminate the software or application. Will you have a hard or soft termination, what happens to any and all data files associated with the effort, how will you undo any authentication or credentialing procedures that were operating, how will you ensure that all access paths from the software to your systems or data are closed off?

Remember, good cybersecurity awareness throughout the process is the most efficient and effective way to prevent or fix vulnerabilities across the software lifecycle at the same time code is being written.

A DATA BREACH OR 'HACK' HAS HAPPENED, NOW WHAT?

First, how will you know you've been breached? Do you have appropriate access control logs? Do you have network controls and access logs, file restrictions, download traps, download notification? Do you have staff with the necessary skills to identify a breach, control the damage and preserve forensic data? Even if you have logs and controls, does anyone routinely look at them? Does anyone evaluate them?

Then do your best to contain the breach. Isolate the hack or virus and define the scope of the incident. Once you have identified that there has been a breach, it's critical that you isolate and contain it. If it's IT-related, that may mean shutting down a server (or multiple servers) or disconnecting from the Internet for a while, until the threat has been eliminated. If you have been hacked, make sure you have eradicated all malware (e.g., viruses, worms, spyware) from your systems and take steps to recover any lost information, such as restoring data from backups.

Next (or simultaneously), contact your lawyer and/or a security expert. Forty-six states, as well as the District of Columbia, have security breach notification laws (you can visit Privacy Rights Clearinghouse for a list), but these laws differ from state to state. If a crime has been committed, contact your local police department or, if you feel they are unequipped to deal with cybercrime or information theft, contact your local FBI office. For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Also, in some cases, you may need to notify your customers if their personal information has been compromised. But before you do this, consult with your attorney and law enforcement contact as to when and how. Similarly, you should designate a person within your organization -- or hire a public relations or crisis management consultant or firm -- to be the point of contact for information about the breach, your response and how affected individuals can get help (if necessary).

When a data breach occurs, quick action is important to help get your business back up and running, and to restore vendor, supply chain and public confidence. Cyber liability insurance and data breach insurance can help a business to address costs like notification, identity protection solutions, public relations, legal, liability and more.

To mitigate the risk of civil litigation and other penalties when a data loss or theft occurs, a cyber liability or data breach insurance policy generally also provides access to professional assistance to help small business comply with best practices, and applicable laws and regulations.

A small business must have a quick response when a data breach occurs to minimize the impact of a data security incident on customers, employees and the long-term health of the business. Business reputation is at risk. There are laws and regulatory requirements that must be addressed immediately or a small business may face steep penalties and lawsuits. Many small business data breach or cybersecurity insurance includes access to experienced breach response partners to assist in meeting mandated obligations and communicating to those who may be affected by a cyber threat, breach or theft of personally identifiable information entrusted to the small business.

Often, cyber insurance can greatly help prepare businesses to avoid or defend against a data breach. Many small business data breach or cyber coverage policies include access to services addressing security measures needed to prevent or minimize an incident. For example, these services can help businesses with network security, employee training, developing appropriate privacy and network policies and procedures, identifying and managing company assets, and incident response planning. Data security is challenging and requires a holistic, multi-faceted approach, and often a significant investment. Maximize your return on investment by accessing the resources that come with an insurance company.

Does Your Business Need Cyber Liability or Data Breach Insurance?

The long and short answer is maybe. Not to be confusing, but think of it this way. What am I protecting? What's the value of what I'm protecting? What's the cost of protection? What will the protection do for me?

While many business owners understand that the personally identifiable customer information they have on their computers (names, dates of birth, social security numbers, etc.) is a target and an online presence leaves them open to liability claims, many may not appreciate the potential costs of a breach from internal or external sources. This is a key to determining if insurance is for you.

The bottom line: It's much more expensive to fix a breach than to prevent one. And most of the time, you can prevent data security breaches by practicing safe tech, as outlined in the steps above.

ADDITIONAL RESOURCES

There are many sites and sources for additional help in the cybersecurity arena. We caution users to rely only on information that they believe to be accurate, genuine, applicable to your situation and from a source you feel is trustworthy.

Internet Service Provider – often your communications provider can assist with tools, planning and services for cybersecurity

The U.S. Small Business Administration – SBA.gov has a variety of resources and referrals to local service providers

Federal Trade Commission – in addition to their Protecting Personal Information guide, the FTC has several compliance and assistance resources, and tools helpful to small business

Federal Communications Commission – as the primary regulator of most communications services the FCC can assist in several ways

Business.gov – integrates many government resources into a readily navigated website to connect you to available services

ASBDC.US.org – the ASBDC is the national association of Small Business Development Centers, the nation-wide network of local, providers of one-to-one small business assistance

OnGuardOnline.gov – is a resource of U.S. Homeland Security with resources for individuals, children and small business

NIST.gov – the National Institute of Standards and Technology presents a range of information on topics from the national cybersecurity framework to applicable standards

Private and non-profit resources – from the ISSA (Information Systems Security Association) to the NTCA (National Rural Broadband Association) many trade, educational and local/regional business groups exist to provide resources, referrals and information

GENERAL BUSINESS CONCEPTS

YOUR BUSINESS PLAN

Every business requires a plan. Why should you go to the effort of creating a written business plan? There are three major reasons:

- The process of putting together a business plan, including the thought you put in beforehand, forces you to take an objective, critical, and unemotional look at your business project in its entirety.
- The finished product—your business plan—is an operating tool which, when used properly, will help you better manage your business and work toward its success.
- The completed business plan is a way to communicate your ideas to others and provides the basis for your financing proposal.

The importance of planning cannot be overemphasized. By taking an objective look at your business, you can identify areas of weakness and strength, pinpoint needs you might otherwise overlook, spot problems as they arise, and begin planning how you can best achieve your business goals. It may even help you to avoid some problems altogether**.**

This guide has been designed with these considerations in mind. It is important that you complete as much of the work as possible. A professionally prepared business plan won't do you any good if you're not familiar with every aspect of the plan. This deep understanding comes from being involved with your plan's development from the very start.

No business plan, no matter how carefully constructed, will be of any value unless you use it. Going into business is a very serious matter in terms of your future and your family's future—over half of all new businesses fail within the first two years of operation. A major reason for failure is lack of planning.

Use your plan. Don't put it in a bottom drawer of your desk and forget about it.

A business plan can help you avoid going into a venture that is doomed to failure. It can help you see if your proposed venture is marginal.

Finally, your business plan provides the information others need to evaluate your venture, especially if you need to seek outside financing. A thorough business plan automatically becomes a complete financing proposal which will meet requirements of most lenders**.**

Suggested Business Plan Outline

Cover Sheet

- Name of business
- Names of owners
- Address and phone numbers of business

Statement of Purpose

The Business
- Description of business
- Market
- Competition
- Location
- Advertising
- Management
- Personnel
- Application and Expected Impact of Loan (if needed)
- Summary

Financial Data

Supporting Documents
- Personal resumes
- Personal financial requirements and statements
- Cost-of-living budget
- Credit reports
- Letters of reference
- Job descriptions
- Letters of intent
- Copies of leases, contracts, legal documents, and anything else relevant to the plan

Cover Sheet

The cover sheet should:

- Identify the name of the business and the date of the plan
- Identify the location and telephone numbers of the business or where the owners can be reached
- Identify the person who wrote the business plan.

The cover sheet should not be elaborate, but should be neat and attractive. If you have a logo, use it. If the plan is to be submitted as a financing proposal, use a separate cover sheet for each bank or capital source you want to submit it to.

Statement of Purpose

The first page should state the plan or proposal objectives as simply as possible. If for your sole use, the statement should be a brief description of how you intend to use the plan.

If the plan is also to be used as a financing proposal, the statement of purpose becomes more complex. It should include responses to the following questions:

- Who is asking for the money?
- What is the business structure (sole proprietorship, partnership, corporation, etc.)?
- How much money is needed?
- How will the money be used?
- How will the funds benefit the business?

- Why does the loan or investment make sense?
- How will the funds be repaid?

The deal you are proposing — the loan or investment, its use and expected effects on the business, and how you will repay it — should be supported by the rest of the plan.

If you are not seeking a loan, the plan should still support and justify the use of your own money (or the money of partners, friends, family).

Keep the statement short and businesslike. It will usually be no longer than half a page, but may be longer if necessary. Use your judgment.

Contents Page

The Contents Page should follow your Statement of Purpose. The remainder of the plan should be devoted to elaborating on and supporting the Statement of Purpose. A business plan, even for a modest project, generally runs to 20 pages or more.

There are three main sections of your plan:

- The Business
- Financial Data
- Supporting Documents

Description of Your Business

This is the most important, most complex part of your business plan. It should make a clear statement of:

- What the business is (or will be)
- What market you intend to service, the size of the market, and your expected share
- Why you can service that market better than your competition
- Why you have chosen this particular location
- What management and other personnel are available and required for the operation
- Why (if appropriate) borrowed money or an equity investment will make your business more profitable

These six considerations are crucial. They are the written policy of your business—rules you should not deviate from without compelling reasons. Since policy gives stability and direction to your business, it requires a great deal of thought and planning.

Your business will reflect your personality and abilities—not someone else's. In describing your business idea, aim at clarity and simplicity. A rule of thumb: If you can't describe your idea clearly and simply, you haven't thought it through.

Deciding what your business is—and where you want it to be in five years—is the most important decision you will have to make. If a small business is involved in more than one activity, your judgment of what the central activity or central activities are is crucial. Your entire planning effort is based on your perception of what business you are in. Be sure to take the time to think this decision through.

The description of the business includes:

- Type of business: Is your business primarily merchandising, manufacturing, or service?
- The status of the business: Is your business a start-up, an expansion of a going concern, or a takeover of an existing business?
- The business form: sole proprietorship, limited liability company (LLC), partnership, or corporation?
- A statement of why your business will be profitable
- The date you plan to start the business
- The hours your business will be open (if your business is a seasonal business, describe how the hours will be adjusted seasonally).

Knowing exactly what your business does and how it operates enables you to plan for profits effectively. Before you begin to consider profit-making, you must be able to clearly state the aims and goals of your business. As the business progresses, the question of how to make profits must be continually asked.

For a New Business

Your description of the business should contain responses to the following questions:

- Why will you be successful in this business?
- What is your experience in the business?
- Have you spoken with other people in this kind of business? What were their responses?
- What will be special about your business?

Many businesses fail to take advantage of the insights and experience of actual and potential competitors. Your best single source of information, they will often give you much valuable advice for nothing more than a chance to share their expertise. Talking with competitors (and observing their business practices) will also help you define what the special advantages of your own business could be.

Two more questions to consider:

- Have you spoken with prospective trade suppliers to find out what managerial and/or technical help they will provide?
- Have you asked about trade credit?

Trade credit is a source of funds. “Net due in 30 days” allows you to use the supplier’s money for the 30 days—like a non-interest-bearing loan. This means, however, that you may forgo any frequently available cash discount if you pay the bill within 10 days. Taking the discount your supplier offers can represent a substantial savings. If you can borrow the funds somewhere else at a lower rate of interest, you should do so. However, such credit is often not available until a business has been in operation long enough to establish a reputation for paying on time.

Many suppliers also offer free services as an inducement to buy their products. For instance, store fixture manufacturers give free layout advice, and utility companies give hints on how effective use of light can create more sales. Two additional considerations:

- If you will be doing contract work, what are the specific terms of the contract? (Reference any firm contract or letter of intent, and include it as a supporting document.)
- How will you offset any slow payment by the customer?

Especially important for anyone contemplating contract work is to find out how and when you will be paid. Get a feel from other contractors about their experiences. Remember that a slow-paying customer can put you out of business if you aren't prepared. If you find that slow payment is a fact of life, plan ahead to compensate for the shorfall.

For a Takeover

Your description should contain a brief history of the business you plan to take over and should respond to the following questions:

- When and by whom was the business founded?
- Why is the owner selling it?
- How did you arrive at a purchase price for the business?

Businesses that are strong and growing are infrequently offered for sale, and most sellers may give—not necessarily deliberately—misleading reasons for selling their business. Protect yourself. Ask your banker to check out the business. This is a routine activity for the bank, which has the means to find out such information. You can also ask your lawyer or accountant who are often experienced in this area.

Pricing a business requires professional expertise and ethics. Paying for a professional appraisal may turn out to be an excellent investment, as it not only establishes a fair price for the business but also provides justification for the price if outside financing is needed. Include a copy of the appraisal as a supporting document. The price should reflect business assets, the rate of expected income on your investment, and perhaps a "goodwill factor," such as patents which can be capitalized, a reputation for excellent service, or an advantageous lease.

Since you will be repaying the purchase price out of profits, make sure that you get what you are paying for. Consider the following:

- What is the trend of sales?
- If the business is going downhill, why? How can you turn it around?
- How will your management make the business more profitable?

These last two items should be supported by income statements and tax returns. If a business is sliding downhill, there may be reasons which aren't obvious. Discuss the owner's reasons for selling. Ask the bankers involved with the business. It is difficult to restore a tarnished reputation. It can't be done overnight.

Some additional thoughts as you check out the business: Have you evaluated and aged the inventory? Checked with trade creditors? Aged the receivables? What is the condition and age of operating machinery? Does the business owe money—and if it does, will you inherit the liabilities? Check with state, federal, and local agencies concerning outstanding taxes due.

Determine exactly what you are buying. You are planning to put your money on the line. Don't be afraid to ask for advice before you commit yourself to any deal. A good attorney is essential at this point to help determine what you are buying and to make sure that the terms of the sale are in your favor.

For Purchasing a Franchise

Many small business owners have been helped in getting a start by investing in a franchise. You may want to consider such an investment.

Most franchises require some or all of the following:

- Initial franchise or license fee
- Training costs
- On-site start-up and promotional costs
- Periodic royalties
- Charges for the building, equipment, inventory, supplies
- Bookkeeping charges (occasionally)

Along with the franchise costs, you should have on hand working capital for at least three months of operation, and preferably more. You can determine working capital needs by a simple formula: multiply living expenses by three and add total franchise costs.

Keep in mind that a parent company is involved in franchising for two basic reasons: to expand, and to raise capital. So if you have a reasonably good credit record and pass all financial requirements, most franchisers will bend over backwards to get you on their team. The help that franchisers provide usually includes assistance with business plans, loan application help, introduction to lending sources, and, in many cases, they serve as guarantor of the loan.

Remember that the price of the franchise does not always reflect the actual cost of the business. Additional costs can include down payments on the land, building, and equipment, fixtures, signs, and many other items.

Be sure you understand the requirements of your cash investment. Do a thorough search of the company in which you will be investing your money. Federal franchise laws require that all franchisers give the franchisee a full and complete disclosure, including a description of the business, training programs, services provided, number of franchises, financial statements, and audits. They must fully describe all that will be required of the franchisee.

It is imperative that you, as the potential franchisee, retain legal counsel to review all contracts, agreements, and other documentation that may be required before signing them.

THE MARKET

To generate an ongoing sales flow, you must become knowledgeable about your market — the people who will be buying your service, product, or merchandise.

Basic market considerations are:

- Who is your market?
- What is the current size of the market?
- What percent of the market will your business expect to capture?
- What is the market's growth potential?
- As the market grows, does your share increase or decrease?
- How will you satisfy your market?
- How will you price your service, product, or merchandise to make a fair profit and also be competitive?

Define Your Market

In marketing terminology, define your target market—the target of all your efforts. You do this by considering:

- Who needs your product or service?
- Who buys the kind of merchandise you stock?

It may be necessary to alter your service, product, or merchandise mix to meet the needs of the market you have targeted.

However, you must first know exactly who your market is. Perhaps it is defined by geographic location, socioeconomic or ethnic factors, age, gender, or other conditions.

Whatever your market elements, make sure you identify them. One way to do this is to simply list all important characteristics, and then, by using Census data or other available information, find out to what extent these characteristics are present in different areas.

You must then measure your target market. As simple as this may sound, remember, having too few customers puts you out of business. Although your business will receive cash from four sources—sales, loan proceeds, sale of fixed assets, and proceeds of new investment—it will ultimately rely on sales as the main source of money. (If there are no sales, there is no business.)

You can obtain information about the size of your market from your Chamber of Commerce, the SBDC, trade publications, marketing consultants, other business persons, libraries, schools and colleges. Census data, which you can find at your nearest library or online, is an excellent source of information.

Get help in assessing the market from such sources rather than trying to guess by watching passing traffic and hoping for the best. Good marketing strategy must be planned, and it must be based on good information.

When you have a feel for your market, answer the following questions:

- How will you attract and keep this market?
- How can you expand your market?

These two critical questions lead to other ideas to consider, such as how and where to advertise, the suitability of your location, and how attractive your office or store is to the clientele you hope to draw.

The second aspect of your marketing strategy concerns price:

- What price do you anticipate getting for your product?
- Is the price competitive?
- Why will someone pay your price?
- How did you arrive at the price? Is it profitable?
- What special advantages do you offer that may justify a higher price?

To make a profit, your business must make more on sales than it spends (both directly, as in cost of goods sold, and indirectly, as in overhead and selling costs). Many businesses flounder because they lose sight of this simple truth.

A Brief Note on Credit

Will you offer credit to your customers? If you do, you are, in effect, making a loan to them. Can you afford to do this? Do you have to extend credit? Can you evaluate credit risk? Can you collect? Can you afford to write off bad debts?

Customer credit can represent an unexpected cash drain on the business. If you must offer credit, make sure that you plan how to absorb its effects. Offering credit to your customers costs you money, especially if you then have to borrow funds to cover these accounts. It may strangle your business by tying up funds you could possibly use for other purposes.

Pricing

Keep in mind that pricing reflects a total package of product and service and expenses.

There is no point in pricing yourself out of the market, nor is there anything to be gained from a price which puts your business in the red.

Competition

If you have decided on your target market, and it is large enough to be profitable, and it contains reasonable expansion possibilities, the next step is to identify and assess your competition. Consider these questions:

- Who are your five nearest competitors?
- How will your operation be better than theirs?
- How is their business: Steady? Increasing? Decreasing? Why?
- How are their operations similar and dissimilar to yours?
- What are their strengths and weaknesses?
- What have you learned from watching their operations?

This section should enable you to make your business more profitable by picking up good competitive practices and avoiding your competitors' errors. Opening a business in a market that is already more than adequately serviced is a common error. Carefully evaluating the competition will sometimes lead you to alter your basic business strategy or modify operations to compete more effectively. This should be an ongoing practice, since market shift and success attract competition.

Learn from competitors' mistakes, and go after the market segment currently being inadequately served. A good practice is to identify an unserved or underserved target market, identify the needs of that market, and go after it**.** An advantage for a small business is its ability to operate profitably in a market too small for big businesses to consider. Checking out the competition is a valuable extension of your marketing efforts.

Location

Proper site location can help your business make money. If you are going into business, first try to identify the ideal site, then figure how close you can come to it, remembering that rent is computed as the combination of space and advertising.

Information about specific geographic areas is available from Chambers of Commerce, trade sources (such as magazines and associations, planning commissions, bankers, and lawyers), and industrial development commissions. They may also have information about tax breaks and financing incentives for businesses that will employ substantial numbers of people in towns under their commission.

Do not go into business in a given spot simply because the price is low. Rent and purchase prices are usually fixed by market forces, and a low price can reflect low desirability. Although for some operations, this consideration is beside the point, for others-–merchandising operations in particular—it is a very important factor.

Each business has its own location needs. If your enterprise is manufacturing or wholesale, low rent and easy access to transportation routes are very important. For most retail operations, however, exposure to people and accessibility are most important. Traffic studies may be available for the area you are considering. Sources of this information may include the state or local highway agencies, the local library, or Chambers of Commerce. Your local banker may well be one of your most useful information sources. Some locations seem to be "jinxed," and most likely he or she will know why and will tell you.

In this section of your business plan, you should answer the following:

- What is your business address?
- What are the physical features of your building?
- Is your building leased or owned? State the terms.
- If renovations are needed, what are they?
- What is the expected cost? Get quotes in writing from more than one contractor. Include quotes as supporting documents.
- What is the neighborhood like? Does zoning permit your kind of business?
- What kind of businesses are already in the area?
- Have you considered other areas? Why is this one desirable for your business?
- Why is this the right building and location for your business?
- How does this location affect your operating costs?

The key to correct site selection: keep in mind that a bad site can put you out of business, while a good site can increase your profits. Once you get started, or if you are already located, keep a constant eye on changes in your location—new roads may be built, populations may shift, zoning ordinances may change. Such changes could mean you need to alter your business plan.

Advertising

Effective advertising can help owner-managers of small companies achieve benefits such as increased sales, sustained sales volume, and reduced selling costs. The secret to such results is not so much in the amount of money budgeted for advertising, but in how it is spent.

Advertising can be one of small businesses' most effective weapons in an intensely competitive business climate. It can offer a creative and effective way for retailers to bid for their fair share of the market in the face of stiff competition and rising costs.

Advertising is not an end in itself, but rather, a means of providing customers with convincing reasons why they should patronize a particular business.

Businesses should always build their advertising messages around the particular advantages they are prepared to offer their customers. Usually, these advantages relate to price and quality of products, convenience and accessibility of store location, or quality of service.

Planning for Timely Advertising

While frequently considered a temporary expedient, advertising should be based on long- range planning, which includes more immediate plans and goals. Moreover, it should be consistent throughout the year as a cumulative sales effort. Although this planning should be the controlling factor, advertising plans should be flexible.

Because small businesses have limited funds, they must plan carefully to obtain maximum effectiveness from their advertising expenditures. Advertising should be planned in relation to the overall merchandising program. It should also be coordinated with such specific management activities as buying, inventory balancing, and acquisition of new customers. In other words, the effectiveness of a limited advertising budget can be greatly strengthened if advertising goals are planned in relation to the total merchandising and selling program.

Timing is possibly the most important single consideration in the planning of effective small business advertising. Timing involves adjusting the advertising plans not only to seasonal sales patterns but also to the business's special days and to the community's or shopping district's special events. Coordination of the advertising program with the buying schedule is also necessary. A promotional advertisement which is not backed up by adequate merchandise can do more harm than good.

Media, Copy, and the Internet

It is becoming a truism that you will not be taken seriously as a business without an Internet presence. Businesses should explore fully the opportunities of presenting themselves to customers via the Internet. An Internet presence can be inexpensive and effective.

The newspaper is a medium used by many small businesses. Other effective media for business are direct mail, radio, television, handbills, billboards, and increasingly, the Internet—through a company website. Also don't discount the effectiveness of a well-designed sign for your location.

The key to success in direct-mail advertising is a carefully selected and maintained mailing list. Small businesses should not overlook the use of radio and television where local rates are low enough to fit the budget of a small shop. These media can be used occasionally with great effectiveness to advertise outstanding promotional events.

Each business must determine the type of advertising copy most appropriate to the identity or image they are seeking to establish in the public mind. All advertising copy benefits from observing the basic rules of eye appeal, simplicity, brevity, straightforwardness, and credibility. An advertising message that is obscure, confusing, or misleading may be successful in the short run, but generally is bound to fail.

To be effective, an ad must:

- Attract attention of the reader or audience
- Offer visual persuasion showing how the product will benefit the customer
- Show why the product is necessary and why it should be purchased at this time
- Encourage purchase, giving reasons for buying, particularly from the business doing the advertising.

Sources of Advertising Help

Businesses can find many outside sources of assistance, such as the following:

- The advertising departments of newspapers offer assistance in preparing copy, art work, and layout. They are often willing to advise the business on general merchandising and sales promotions planning.
- The firms that supply the retailer with merchandise often provide advertising materials free of charge, grant advertising discounts, and participate cooperatively in the business's advertising by sharing a portion of the cost.
- Direct-mail agencies compile specialized mailing lists which the business can use to contact selected customer groups. These agencies also assist in the preparation of mailing literature.
- Trade newspapers and magazines often provide useful information to the business manager about advertising practices. Trade associations, Chambers of Commerce, and Better Business Bureaus also provide information on advertising and advertising ethics.
- Some advertising agencies specialize in servicing small businesses, and typically will take full responsibility for all aspects of advertising.

In addition, businesses should keep well informed about their competitors' advertising. The larger ones usually have effective advertising, and a study of the methods they use, the merchandise they feature, the style of their copy, and the size and layout of their advertisements can provide helpful ideas.

Budgeting

Advertising has three basic goals:

- Sell goods and services
- Create a positive business image
- Allow the advertiser to compete successfully

Budgeting for advertising is necessary for maximum returns. The amount to spend depends on many factors, such as specific promotional objectives, store location, competition, age of store, and past success in attracting customers. Often, businesses discover that what they need to spend on advertising and what they can afford to spend are not the same. They must study their own situation carefully and, within the limits of their financial capabilities, allocate funds on a planned basis over an extended period, usually six months.

MANAGEMENT

Roughly 98 percent of small businesses fail because of managerial weakness; fewer than two percent of the failures are due to factors beyond the control of the people involved.

Your business plan must take this into account. If you are preparing a financing proposal, you should make sure that your prospective financial source is aware of the steps you have taken or are taking to correct any weaknesses in your managerial staff. If you are to use your business plan to the fullest, you should highlight both management strengths and weaknesses.

There is no known cure for incompetence, but there are direct cures for inexperience: Acquire the necessary experience yourself, or find a partner or employee who does**.**

In preparing the Management section, you should cover five areas:

- Personal History of Owners and Key Managers
- Related Work Experience
- Duties and Responsibilities
- Salaries
- Resources Available to the Business

Properly treated, these five will help make a proposal convincing.and a business plan useful. The aim is to spot areas of potential weakness before problems arise and threaten to put you out of business**.**

Personal History of Owners

In this segment, include responses to these questions:

- What is your business background?
- What management experience have you had?
- What education (including both formal and informal learning experiences) have you had which has a bearing on your managerial abilities?
- Personal data: age, where you live and have lived, special abilities and interests, reasons for going into business. Keep in mind that your family will be affected by your decision to go into business. Try to assess the potential impact. While they may be supportive now, will they continue to be supportive a year from now?
- A personal financial statement must be included as a supporting document in your business plan if it is a proposal for financing.

Bankers and other lending sources want to see as much collateral as possible to secure their loan. Be forewarned: Under most circumstances, the personal credit worthiness of the principals will be a major concern for the banker. Also, you wll undoubtedly be expected to sign personally for the loan. This means that your personal assets could be taken if the business fails — even if it’s set up as a corporation.

Related Work Experience

This segment is an expansion of the experience factors mentioned earlier. It requires, but is not limited to, information on the following:

- Direct operational experience in this type of business

- Managerial experience in this type of business
- Managerial experience acquired elsewhere—whether in totally different kinds of businesses, or as an offshoot of club or team membership, civic activities, church work, or some other activities.

While some managerial skills are transferrable, others are not. Managerial experience and expertise that is not carefully balanced can cause serious problems. The talents required of a financial specialist are quite different from those of a used-car salesman. A combination of both sets of talents in one individual is rare.

Duties and Responsibilities

Once you have filled in the experience and skills—and have a feel for the weaknesses—of the proposed management, this segment is relatively simple.

Make sure that you spell out in advance:

- Who does what
- Who reports to whom
- Where the final decisions are made

Allocating duties and responsibilities is critical. If the chain of command is unclear to your employees, you will have personnel problems. This is a major responsibility of management and must not be evaded under the guise of "we can work it out later when we see where the problems are."

Salaries

When completing this section, include salaries of management and all employees. Don't forget to include employee benefits as well as salaries (e.g., medical, pension, Social Security, insurance coverage). Be realistic when computing upper-level salaries.

Knowing what you need, as distinguished from thinking you know what you need, takes effort. One sure way to damage a small business is to take the money out for family necessities. If your business can't afford to pay you a living wage, and you have no other income or savings, you had better reconsider your deal.

Resources Available to the Business

All businesses, no matter how small, need the services of:

- Accountant
- Lawyer
- Insurance broker

If you don't have any of these services, make sure you get them immediately**!**

Other sources of assistance include:

- Small Business Development Centers
- Business, trade, civic organizations, which often have a pool of talent available to their members
- Small Business Administration technical assistance and SCORE programs

Avail yourself of all of these. And don't forget: Your banker can be among the most helpful partners you have. If you borrow money, the bank has a vested interest in the success of your business.

You won't necessarily have to use all of these secondary resources, but it is a good idea to know what help is available if you need it.

Summary

This section should make you aware of the necessity of developing your management skills, and, for the skills you do not possess, of accessing all outside resources (legal, financial, etc.) available to you. Keep in mind the necessity of managing your business rather than letting the business manage you. Constantly review and re-evaluate the status of your business. In this way, you will drastically diminish the odds of failure. Keep this section short, direct, and honest.

Personnel

Businesses stand or fall on the strength of their personnel. Good employees can make a marginal deal succeed; poor employees can destroy the best business. Studies have consistently shown that out of 100 customers who stop patronizing the average store, more than 70 do so because they didn't get prompt, courteous attention.

Here are some questions to think about in determining your hiring needs:

- What are your personnel needs now? In the near future? In five years?
- What skills must your staff have?
- Are the people you need available?
- Do you need full or part-time staff?
- Will you pay them salaries or hourly wages?
- Will you offer fringe benefits?
- Will you pay for overtime?
- Will you have to train people? If so, at what cost to the business?

Application and Expected Impact of Loan

This section is important, whether you are seeking a loan or planning to finance your deal yourself. In determining how much money you will need and for what purposes, do not rely on guesses when exact prices are available. Specify how you arrived at your figures. It may be helpful to make a list.

Fill out your reasonable choice. It may be important to you to have a luxury item or two, but weigh the cost. A tabular worksheet is particularly useful for a start-up business and can be used whenever a purchase of additional equipment is contemplated.

Make sure that this section contains responses to the following:

- How is the loan or investment to be spent? This can be fairly general (working capital and new equipment, inventory, supplies).
- What is the item to be bought?

- Who is the supplier?
- What is the price?
- What is the specific model name and number of your purchase?
- How much did (or will) you pay in sales tax, installation charges, and freight fees?

Your banker may be interested in using whatever it is that you are buying as collateral for the loan. By having a list, your loan can be processed faster.

Consider the possible advantages of leasing some of the capital equipment you need, and definitely look into the advantages of renting rather than owning your business building. If you have the money to buy, owning may (or may not—ask your accountant) be less expensive than leasing. If you are short of cash, a lease arrangement may enable you to ease cash problems by lowering your investment in fixed assets (perhaps a sale/lease-back deal). Leases also have greater flexibility. As your business grows, you can often make changes more readily. It is also possible to save money on taxes by deducting lease payments as business expenses.

Most important, ask yourself how the loan will make your business more profitable.

Interest is an expense which reduces profits. If you propose borrowing money or investing your own, you must know how the money is going to work for you.

Make sure it earns more than it costs! A well-thought-out business plan can be an asset to any small business. If you have followed the steps outlined in this guide, you should be able to develop a good, workable plan.

Financial Plan

To effectively manage your finances, plan a sound, realistic budget by determining the actual amount of money needed to open your business (start-up costs). The first step to building a sound financial plan is to devise a start-up budget. Your start-up budget will usually include such one-time only costs as major equipment, utility deposits, down payments, security deposits, etc.

A start-up budget should allow for these expenses:

- Personnel (costs prior to opening)
- Occupancy (lease, rent or mortgage)
- Legal/Professional Fees
- Equipment
- Supplies
- Salary/Wages
- Income
- Utilities
- Payroll Expenses
- Internet
- Licenses/Permits
- Insurance
- Advertising/Promotions

The operating budget is prepared when you're actually ready to open for business. The operating budget will reflect your priorities in terms of how money will be spent, the expenses you will incur and how you will

meet those expenses. Your operating budget should also include money to cover the first three to six months of operation. It should cover the following expenses:

- Personnel
- Lease/Rent/Mortgage
- Loan Payments
- Legal Fees
- Accounting
- Supplies
- Salaries/Wages
- Dues/Subscriptions/Fees
- Repairs/Maintenance
- Insurance
- Advertising/Promotions
- Depreciation
- Payroll Expenses/Payroll Taxes
- Internet
- Travel/Entertainment
- Miscellaneous

The financial plan should also describe the type of financing you're seeking, the amount of money you're looking for, how you plan to use these funds and the preferred terms for repayment.

The financial plan will be the tool prospective investors, bankers, and even you will use in order to determine the feasibility of the business you are presenting. If the business already exists, it should illustrate the current financial status of your business and represent your best estimate of its future operation. If the business is new, a projection will suffice. The results presented should be both realistic and attainable. The financial forecasts should come in the form of three-year cash flow and balance sheet statements.

CASH FLOW PROJECTION

Year One

	Month	1	2	3	4	5	6	7	8	9	10	11	12	Total
Cash In-Flows														
	Sales													
	Other Income													
Total In-Flows														
Cash Out-Flows														
	Cost of Goods Sold													
	Rent/Mortgage													
	Owner's Salary													
	Other Salaries													
	Payroll Taxes													
	Advertising & Promotion													
	Utilities													
	Loan Payments (current)													
	Loan Payments (previous)													
	Telephone													
	Office Expense													
	Dues & Subscriptions													
	Accounting													
	Insurance													
	Professional fees													
	Internet													
	Repairs & Maintenance													
	Licenses & Permits													
	Travel & Entertainment													
	Legal fees													
	Bank charges													
	Miscellaneous													
Total Out-Flows														
Net Cash Flow														
Beginning Cash Balance														
Ending Cash Balance														

CASH FLOW PROJECTION

		Year 2				
	Quarter	1	2	3	4	Total
Cash In-Flows	Sales					
	Other Income					
Total In-Flows						
Cash Out-Flows	Cost of Goods Sold					
	Rent/Mortgage					
	Owner's Salary					
	Other Salaries					
	Payroll Taxes					
	Advertising & Promotion					
	Utilities					
	Loan Payments (current)					
	Loan Payments (previous)					
	Telephone					
	Office Expense					
	Dues & Subscriptions					
	Accounting					
	Insurance					
	Professional fees					
	Internet					
	Repairs & Maintenance					
	Licenses & Permits					
	Travel & Entertainment					
	Legal fees					
	Bank charges					
	Miscellaneous					
Total Out-Flows						
Net Cash Flow						
Beginning Cash Balance						
Ending Cash Balance						

Pro-Forma Balance Sheet
(Opening Day of Business)

ASSETS	
Cash	
Accounts Receivable	
Inventories	
Prepaid Expense	
Other Current Assets	
TOTAL CURRENT ASSETS	
FIXED ASSETS	
Land	
Leasehold Improvements	
Equipment	
Vehicles	
Other Fixed Assets	
Subtotal Fixed Assets	
Less: Accumulated Depreciation	
TOTAL FIXED ASSETS	
TOTAL ASSETS	
CURRENT LIABILITIES	
Accounts Payable	
Current Portion of Long-Term Debt	
Accrued Expenses	
Other Current Liabilities	
TOTAL CURRENT LIABILITIES	
LONG-TERM DEBT, net of current portion	
OWNER'S EQUITY	
Paid-In Capital	
Retained Earnings	
TOTAL OWNER'S EQUITY	
TOTAL LIABILITIES & OWNER'S EQUITY	

Pro-Forma Income Statement

	Year	1	2	3
	Sales			
	Other Income			
Gross Profit				
Operating Expenses				
	Cost of Goods Sold			
	Rent/Mortgage			
	Owner's Salary			
	Other Salaries			
	Payroll Taxes			
	Advertising & Promotion			
	Utilities			
	Telephone			
	Office Expense			
	Dues and Subscriptions			
	Accounting			
	Insurance			
	Professional fees			
	Internet			
	Repairs & Maintenance			
	Licenses & Permits			
	Travel & Enertainment			
	Legal fees			
	Bank Charges			
	Miscellaneous			
	Depreciation			
	Interest			
Operating Expenses				
Net Income				

GENERAL OPERATIONS

Advertising as Part of Your Marketing Plan

Marketing and advertising are often mistaken for one another. Advertising is actually part of the marketing process. Advertising includes all activities in the paid promotion process, whereas marketing includes planning what, where, how, and to whom you will sell your product or service.

Putting together an advertising campaign for your business should entail a clear idea of:

- How much to spend
- What type of media to use
- What market area to reach
- How often to run any ads

If you make decisions haphazardly or use a "seat-of-the-pants" approach, the results will probably show it.

To help organize a cohesive plan, it is wise to commit your ideas and decisions in the form of a written advertising plan. This helps you identify areas that need to be looked at in developing an advertising campaign. And it gives you a written reference that you can and should periodically review during the course of the year.

Marketing Plan Format

Although there is no one marketing plan format for all businesses, a plan can be developed using the following topic list as a guide:

- Advertising Objectives. What are you trying to achieve? Establishing a particular identity for your project, such as "the most dependable" or "lowest price" (often called positioning), or simply trying to increase sales?

- Advertising Strategy. This should contain the overall methodology to meet advertising objectives. For example, if the primary objective is to convey the message that your product is "the most depenable,"the strategy should explain how this is to be carried out.

- Creative Strategy. This contains guidelines or specifics to assist in the creative aspects of advertising. Creative aspects include slogans, themes, use of graphics and colors, logos, copy guidelines, and mechanical specifications (e.g., typestyles and sizes, use of photography, and details of reproductions).

- Media Plan. This should identify the media mix (combination of print, broadcast, and other). A media schedule details the types of media that should be used for advertising throughout the year. This may be generic and contain only types of media that will be used, such as the Internet, radio and newspapers, or specific and contain types of media and corresponding identities, such as WXYZ Radio and the *Daily News*. The media budget includes costs associated with each ad placement (cost of airtime, newspaper space, magazine placement). The media budget is then used as part of your advertising budget.

- Advertising Budget. This has two components: the media budget and the production budget. The production budget contains all costs associated with production of advertisements. Typical items include: time and materials from in-house staff (normally not included if your company does not cross-charge departments), photography, purchased services such as typesetting or use of consultants,

or the entire creative and production charge if you use an advertising agency. Transfer the total to your master budget, where you can represent it as either a total advertising line item or break it down into media and production components.

Overall Promotional Strategy

The primary goal of advertising is to position your company and product in the mind of the potential customer. Advertising is one of three major promotion methods. The others are personal selling and public relations.

Personal Selling

Personal selling is the dominant form of promotion, done through sales clerks, telemarketing, and/or field salespeople. Personal selling is flexible and enables greater control over the sale, since questions can be answered, the sales pitch can be customized, and the sale can be closed. Many customers build strong bonds with salespeople, counting on them for in-depth information on a product, on industry trends, and on special treatment in pricing and order lead times. For these reasons, it is necessary to maintain adequately trained salespeople and keep them well informed about your current products, and your competitors' products as well.

Salespeople must know how much flexibility they are allotted for adjusting prices, modifying standard product offerings, extending credit, and promising delivery dates. The ability to respond to customer inquiries helps build confidence. Many companies assign titles such as marketing representative, marketing specialist, or sales engineer to indicate this type of authority.

Salespeople are often responsible for customer support in addition to getting orders. This allows valuable input to the company that could affect other sales. Good sales techniques can forge strong customer-company relationships and can result in repeat business and secondary promotion through word of mouth. Friendly, knowledgeable salespeople can be one of your best promotion assets.

Sales promotion includes activities supporting personal selling. These include brochures, fliers and catalogs, novelties, displays, and trade shows.

Public Relations

Public relations includes any type of publicity that is generally not paid for, and that seeks to create interest or favorable recognition for the company and its products or services. Public relations provides an economical way to enhance your company's image. The disadvantage: You have little or no control over how much of your message gets through.

Many activities present excellent public relations opportunities; these include new product announcements, giving or receiving awards or significant contracts or grants, hiring new key personnel, as well as stunts, shows, exhibits, grand openings, guest appearances by celebrities or dignitaries, sponsorships, and fundraisers.

For most public relations activities, the company must take the initiative to generate media interest. In most cases, this involves preparing and distributing a press release describing the activities, and including photographs, when available.

The Four "Ps" of the Marketing Mix

Promotion is only one component of marketing, more specifically, the marketing mix, which consists of **Four Ps: Promotion, Product, Place and Price**. Marketing involves managing decisions about the mix, that is, type and amount of promotion, product, place, and price.

Promotion

Promotion consists of your overall strategy for putting your product or service in front of the appropriate buying public and creating an environment in which sales result. In considering all of the elements of promotion (marketing, advertising, public relations, etc.), do not overlook the Internet, potentially and actually the most powerful business promotion tool to arrive in decades. Increasingly, almost every business, if it is to be taken seriously, will have an Internet presence in the form of a website. Your SBDC business adviser can explore with you the opportunities and options the Internet offers your business.

Product

Product refers to the goods and services that your company provides. You need to define your product in terms of the target market.

Typical key product decisions include:

- Product features
- Accessories
- Packaging
- Warranty
- Service
- Installation
- Instructions and/or training

Pay close attention to trends, and minimize the possibility of making product decisions based on fads. Product decisions are not only initially important, but must be updated to reflect changing consumer wants and needs.

Place

Place refers to the where your product or service is distributed, or where your customer comes in contact with you.

For retail establishments, location is the primary factor. Obviously, a retail store should be accessible to the target market and have adequate parking, if necessary. Other location pluses include frontage exposure and proximity to other major, non-competing retail stores.

Other types of businesses must decide whether to sell through dealerships, distributors, mail order, jobbers, the Internet, or a combination of methods.

Price

Prices should conform to the overall company pricing strategy. Ask yourself: Does your company have a low price strategy, an at-market strategy, or upscale market strategy?

How does your pricing compare to that of your competitors? If your pricing is consistently higher, does your product offer recognizable differences that will justify the additional price? If so, maybe this is something you should bring out in your advertising.

External Factors Affecting the Market Mix

We have just described the four internal factors that you can control as a business manager. This marketing mix is central to your marketing strategy. But there are also external factors—technological, economic, societal, political, legal, and natural—that you cannot control.

Technological Factors

Introduction of new technologies, and obsolescence of old technologies, has a direct impact on the marketing mix by making a continuous stream of new products available which are priced for, promoted in, and sold to new markets.

An example of a major new resource created through advancements in technology is the Internet, made possible through developments in integrated circuit technology, the spread of personal computers, and the conversion of an advanced defense-oriented system to civilian purposes.

Technological advances in areas such as biotechnology, medicine, chemistry, automation, metals, and advanced materials provide the knowhow for similar development for countless new products.

The Internet is another example of a technology producing profound change in the ways in which we do business and conduct our lives.

Economic Factors

The state of the economy influences demand for particular products, and determines how they are sold and promoted and at what price they are offered.

A sluggish economy decreases consumer demand for most products. Increased advertising may be required to stimulate sales.

Carefully monitor economic indicators, such as the Consumer Price Index, interest rates, and unemployment rates, and make adjustments to the marketing mix as needed.

Societal Factors

Cultural and social customs, values, and lifestyles require special attention. You may need to take into account issues of multiculturalism, religion, economic status, health, diet and nutrition, crime, and public opinion.

Responding to societal wants and needs with the right product at the right time gives your company a competitive edge.

Political and Legal Factors

Government policies, regulations, and legal actions at federal, state, and local levels can have a dramatic effect on all aspects of the marketing mix.

Two examples of government regulations that impact the marketing mix are those related to product labeling and to the environment. Alcohol and tobacco products must bear special warnings on their labels; where and to what age group they can be sold are heavily regulated. Environmental regulations have placed mandates on industry to develop products that are not harmful to our environment.

Natural Factors

Factors such as geographic location, weather and climate, and availability of natural resources all can influence your marketing mix.

The agriculture industry, for example, requires not only a good geographic location for the type of product being produced, but good weather during growing seasons. These conditions will influence the type of products and growing season yield and price. The occurrence of natural disasters such as floods and hurricanes not only can create hardship for the agricultural producer, but can also result in unexpected delays or depletion of expected agricultural products for companies selling or processing them.

Infrastructure Factors

Finally, the cost and availability of transportation, communication, and energy dictate how markets will be accessed, and how much it will cost to produce and transport products.

High-quality, reliable roads, railways, air transportation, and utilities must exist to enable large-scale economic activity. Improvements must constantly be made to accommodate increasing demand.

Developing a Marketing Plan

To develop a marketing plan, your company should formulate a marketing strategy which identifies target market, marketing objectives, and marketing mix. A marketing strategy defines the game plan for your business. It provides information about your markets and how you intend to penetrate them. It defines the character of your business—for example, as an innovator, challenger, or follower.

While the marketing strategy outlines constraints under which your business will operate, the marketing plan details how the strategy will be carried out. For example, a clothing retailershould provide information on promoting the latest trends in men's sportswear in the marketing plan.

Format

As with the advertising plan, no one marketing plan format is ideal for every business. The following topic list, however, provides a useful guide for constructing a marketing plan:

- Mission Statement. Describe your business purpose, its goals and objectives, and specific strategies to reach them.
- Product/Service. Identify each of your products and/or services, their cost to you, specific characteristics (including competitive advantages and disadvantages), and expected annual sales volume.
- Market. Provide a complete demographic analysis of the customers in each market, including market size. Identify current or projected market or industry trends, as well as information from supporting market studies or test markets.

- Distribution. Identify how products will reach the customer, including labeling, packaging, and shelving information. If you will use distributors, include a list of distributors and satisfaction level from previous experience (if applicable). If you plan to offer cooperative advertising programs with them, include guidelines. Identify details on incentives and sales quotas, and on the handling and returning of goods.
- Competition. Identify competitors by divisions, product lines, and markets. Include competitive strengths and weaknesses. Identify and compare marketing techniques.
- Pricing. Develop price schedules, including discounts, where applicable. Include comparative price lists of competing products, and explanations of price variations.
- Marketing. Provide guidelines for developing your advertising plan. For example, will you do advertising in-house or hire an agency? Do you have preferences in advertising media? Be sure to identify any planned marketing events, such as seasonal sales, new product announcements, and promotions. Provide guidelines for advertising expenditures.
- Sales Forecast. Include a detailed sales forecast for the year. Identify sales commission plans and expected sales quotas.
- Action Plan. Identify major marketing activities, their priorities, completion schedule, and the people or organizations responsible for carrying them out.
- Production. Include product production information, if applicable, to ascertain availability of products in the face of projected demand. Identify contingency plans to increase product availability, if required.

The marketing plan should be a pivotal document for developing your advertising plan. Re-evaluate and update your marketing plan regularly so it is always up to the moment and can be used reliably.

Putting It All Together

Managing an effective advertising program for a business requires a great amount of research and planning. While larger companies devote an entire staff to advertising responsibilities, smaller companies should delegate advertising responsibilities to at least one individual. This advertising specialist should be (or become) knowledgeable in advertising media—in particular, rates and coverage areas.

Advertising should not be a one-time event at the time an ad is placed, but rather a continuous process. Databases of media information should be maintained and updated frequently so that when this information is needed, it is complete and up to date. You can use media directories such as Standard Rates and Data, available in the reference section of many libraries, or call or write or visit the website of the sales department of any newspaper, magazine, radio station, television station, cable company, or other medium.

Past advertising effectiveness should be evaluated to determine which strategies have worked in the past, enabling you to adjust the marketing mix. Don’t forget to adjust your advertising messages to conform to changes in the external environment, as well as competitive advertisements.

Develop an advertising budget from the bottom up, by determining true costs of planned advertising activities, rather than by simply allocating an arbitrary dollar amount for your total advertising effort. This gives the most accurate cost projection, and enables you to better identify true costs for future advertising budgets.

Above all, use good business sense. Although advertising requires a substantial share of a company's financial resources, it also projects a lasting image of your company, its products, and services for years to come.

ACCOUNTING AND RECORD KEEPING

"If you don't understand the need for good records, you don't have enough experience to start a business."
— Anonymous

This quotation emphasizes the importance of accounting and record keeping. Many businesses have fail because the owners did not maintain the records necessary to allow for sound management of the business.

Why Keep Good Bookkeeping Records?

The Internal Revenue Service requires that everyone in business keep records. "The law does not require any special kind of records. You may choose any system that is suited to your business and that will clearly show your income," says the IRS.

Good record-keeping also helps you monitor the business for planning, controlling, and budgeting purposes. As an owner, you must plan for the future of the business, based on financial knowledge rather than guesswork. Good business decisions are made from timely and accurate information about the company.

Up-to-date bookkeeping records should provide useful data for you to make intelligent decisions to operate your business successfully. Your records should yield information such as:

- sales information and operating results
- fixed and variable costs
- profit and loss
- inventory levels
- data comparisons - current & prior
- financial statements
- tax returns and reports to regulatory agencies

What System Should You Use?

Small business owners should use a simple and practical bookkeeping system. Because owners are usually busy with daily operations, it is imperative that the bookkeeping not be cumbersome.

A good system should be:
- simple to use
- easy to understand
- reliable
- accurate
- consistent
- timely

Cash and Accrual Methods of Accounting

Before we consider the fundamental elements of bookkeeping systems, let's talk about cash andaccrual methods of accounting.

Using the **cash method** of accounting means you record your sales at the time you actually receive the cash. You also record your expenses when you pay out the cash. This method follows the cash flow in and out of your business and is used by most small businesses because of its simplicity.

Under the **accrual method** of accounting, you would record all sales and all expenses when the service is performed or the goods are delivered, regardless of when payment is received or made. Using this method requires the use of an account for "receivables" and another for "payables" in your records to allow you to keep track of what is owed to you and how much cash you owe.

You may use what is known as the **hybrid method**, which incorporates both methods: Using the cash method during the year and the accrual method at year-end allows you to accurately state your income because you can record unbilled sales and expenses in the year they have actually occurred. An "account receivable" and "account payable" would again be necessary. This method is preferred by businesses with 30-day credit accounts because it allows a more accurate accounting of profit and loss without the bother of keeping these two extra accounts throughout the year.

Any of these methods is acceptable. It is up to you to decide which one best suits your situation.

Elements of Bookkeeping

Currently, there are many bookkeeping systems to choose from on the market—all fulfill the six requirements of a good system. Choose a system with rules and methods for collecting, processing, and summarizing financial and economic data that is useful in your decision making.

Any bookkeeping system should include at least the following:

- business checkbook
- chart of accounts
- daily summary of cash receipts
- disbursements journal
- monthly summary of cash receipts and disbursements

Storage Medium

Although there is no requirement to keep your records in bound books, you should use either pre-packaged forms or columnar paper designed for bookkeeping purposes. Your records are your tool for the present and future management of the business.

Business Checking Account

The first step in setting up your system is to open a separate checking account. Shop around to learn which financial institution charges the price you want to pay and offers the services you need for your operation. Banks are competitive, and prices for services can vary.

Take into consideration the location, reputation, hours of operation, and friendliness of the bank you select. You may be interested in "one-stop shopping." If your business grows and at some later date you are looking for funding, cultivating a good banking relationship will be a priority.

Visa/MasterCard Privileges

If you plan to offer credit to your customers through Visa/MasterCard, you will want to ask the bank if they provide this service and what the bankcard discount would be. Offering Visa/MasterCard allows your customers to buy without having to pay cash. There is no risk to you of customer no-payment. This security does not come without a cost. The bank charges a percentage of the ticket price, which is called the bankcard

discount, which is usually determined by the annual dollar amount of credit sales generated through your firm. For the initial year, a percentage is assigned and is adjusted each year thereafter accordingly.

Business Checkbook

Once you have opened the checking account, you will want to use it for all "cash in and cash out." All money you receive, whether from sales, loans, personal equity advances, or other sources, should be deposited into the checking account. All payments, including deductible expenses and personal withdrawals, should be made by check. This gives you internal control over your most precious asset — cash.

Each deposit made and check written must also be recorded in your business checkbook. Be sure to keep deposit slips and sales invoices or statements on file. These will provide documentation of your business transactions and supply an "audit trail," should the Internal Revenue Service ever decide to audit your company.

Reconciling Your Bank Statement

A basic principle of good recordkeeping is reconciling your bank statement with your checkbook each month. Normally, because of timing differences, your checkbook balance and the bank statement will not agree if your business has been active. You may have made deposits after the date of the bank statement or written checks that have not yet been cashed. It is also possible that the bank made special debits and credits to your account and included them on the bank statement but that these have not yet been entered into your records. Reconciling your bank statement to your checkbook is the only way to prove your cash account. The balance in your checkbook and the balance on the statement must be adjusted to the true cash balance, with the items causing the difference indicated. Below is an illustration of how to reconcile your bank statement:

Sample Bank Reconciliation as of January 31, 2006

Balance on bank statement 1,609.83
Add deposits not credited:
1/27 . . . . . 701.33
1/30 . . . . . 380.65
Subtotal 1,081.98
TOTAL 2,675.53
Subtract outstanding checks:
Check # 88 . . . . . 66.70
Check # 89 . . . . . 9.80
Check # 92 . . . . . 212.47
Check # 93 . . . . . 150.00
Subtotal 438.97
Adjusted balance per bank statement 2,236.56

Balance shown in checkbook 2,240.56
Add deposit of 600.40 for 1/8 entered as 594.40 (difference) 6.00
Subtotal 2,246.56
Subtract bank service charge . . . . . (10.00)
Adjusted checkbook balance 2,236.56

Chart of Accounts

To achieve an efficient bookkeeping system, you must set up a separate account for each item that you plan to record. Every account is titled and numbered and classified as asset, liability, owner's equity, revenue, or expenses. This procedure is known as selecting a chart of accounts for your business. Following is a model:

XYZ COMPANY Chart of Accounts

ASSETS (100-199)
- 100 Cash
- 110 Inventory
- 120 Equipment

LIABILITIES (200-299)
- 200 Loan(s) Payable
- 210 Sales Tax Payable

OWNER'S EQUITY (300-399)
- 300 Jane Doe, Capital
- 310 Jane Doe, Drawing

REVENUE (400-499)
- 400 Merchandise Sales
- 410 Service Sales

EXPENSES (500-599)
- 500 Purchases
- 510 Rent Expense
- 520 Utilities Expense
- 530 Salaries Expense
- 540 Interest Expense
- 550 Supplies Expense
- 560 Advertising Expense
- 570 Miscellaneous Expense

When a business transaction occurs, it must be entered into your records; the amount is entered as an increase or decrease in these accounts. For example, $150 of merchandise sold is entered into the Merchandise Sales account, increasing the Revenue. Recording the deposit of the $150 into the checking account increases the Assets - Cash account.

The accounts keep a tally of the monetary activities of your business.

There are no standardized account titles. You will want to select titles that clearly and precisely indicate the nature of the account. The accounts are numbered using at least a three-digit system to allow space for 100 account titles within each classification. However, you should have only as many accounts as necessary to keep tabs on your business operation.

Daily Summary of Cash Receipts

Not all cash received is income. Cash can come into a business from many sources, including sales income, bank loans, personal advances, interest earned, sale of equipment, and other. Every transaction involving the receipt of cash must be recorded in your bookkeeping system.

To accomplish this, use a Cash Receipts Journal. The form can vary according to the needs of your company. Typically, column headings are used to provide flexibility in identifying affected accounts. Remember that any sales on credit are not entered into a Cash Receipts Journal. This journal is used only to record cash actually received**.** Following is a model:

Cash Receipts Journal

Date	**Explanation**		
6/1	Merchandise		
Sales	Sales Tax	Other	Total Received
152.55	10.68	0.00	163.23

Date	**Explanation**		
6/5	Service		
Sales	Sales Tax	Other	Total Received
80.84	5.66	0.00	86.50

Date	**Explanation**		
6/12	Merchandise		
Sales	Sales Tax	Other	Total Received
179.84	12.59	0.00	192.43

Date	**Explanation**		
6/26	Service		
Sales	Sales Tax	Other	Total Received
115.00	8.05	0.00	123.05

Date	**Explanation**		
6/30	Bank Loan		
Sales	Sales Tax	Other	Total Received
		1,000.00	1,000.00

Date	**Explanation**		
6/30	Total Cash		
Sales	Sales Tax	Other	Total Received
662.00	46.34	1,000.00	1,708.34

Disbursements Journal

You must enter daily all expenditures made in cash or checks. These payments from company funds may be made for deductible and nondeductible disbursements. For a particular expense to be deductible when computing your taxable net profit, it must be an "ordinary and necessary" expense incurred in your trade or business for an item that is not a capital asset. A capital asset has a life of more than one year and is subject to special IRS rules in expensing and/or depreciating when you compute profit and loss on your tax return.

Since this journal accounts for all cash out of the business money, it is critical that each disbursement be carefully recorded and supported with objective evidence, usually in the form of a business document such as a supplier's invoice. Following is a model:

Disbursements Journal

Date	**Paid To**		
6/1	ABC Advertising		
Check	Acct #	Account Title	Amount
224	560	Adv. Exp.	85.00
Date	**Paid To**		
6/7	Mark Baker		
Check	Acct #	Account Title	Amount
225	510	Rent Exp.	400.00
Date	**Paid To**		
6/9	National Grid		
Check	Acct #	Account Title	Amount
226	520	Util. Exp.	125.80
Date	**Paid To**		
6/17	General Supply		
Check	Acct #	Account Title	Amount
227	500	Purchases	437.95
Date	**Paid To**		
6/20	Jane Doe		
Check	Acct #	Account Title	Amount
228	310	Drawing	250.00
Date	**Paid To**		
6/24	NYS Sales Tax		
Check	Acct #	Account Title	Amount
254	210	S.T.Payable	230.07

6/30 Total Payments: $1,534.61

Note: Two non-deductible disbursements were made—one to New York State to turn over the sales tax collected, and one to Jane Doe for a personal withdrawal.

Monthly Summary of Cash Receipts and Disbursements

It is important to have information available in summary form with year-to-date balances for each account. These balances provide the data to create financial statements, prepare government reports, and make decisions for operating and controlling the business. Following is a model:

510 Rent Expense Ledger

Date	Increase	Decrease	Cumulative Balance
20XX			
Jan	400.00		400.00
Feb	400.00		800.00
Mar	400.00		1,200.00
Apr	400.00		1,600.00
May	400.00		2,000.00
Jun	400.00		2,400.00

Keeping Records

The IRS says you must keep your records for as long as they may be needed to administer any IRS provision. Keep records that support an item of income or deduction on a return until the statute of limitations runs out — usually three years after the return is due or filed, or two years from the date the tax was paid, whichever occurs later.

You may wish to keep your records for a longer period. For instance, journals and ledgers should be kept indefinitely. Supporting documents can be discarded whenever you stop using them, provided it is past the three-year statute of limitations.

Business Versus Personal Records

Your business records must be kept separate from personal records. Do not commingle funds or information. If you have more than one business, you must keep a set of records for each business. For example, if you own a consulting firm and a car wash, you would need to keep three sets of records: one for each of the businesses and one for your personal records.

Getting Started

Ideally, getting your bookkeeping system up and running would occur at the time the first sales or expense has been incurred. The sooner you have your system in place and ready to accept the information from your business operations, the smoother the job of planning, controlling, and budgeting will be. Be accurate when recording dollar amounts of cash in and cash out, and keep supporting documents in your files. As you get more experienced, this process will become easier to handle. Above all, stay on top of your bookkeeping.

The **IRS website** contains a special section for small business and the self-employed. It offers a broad range of resources across federal and state agencies, as well as industry/profession specific information for self-employed entrepreneurs, employers and businesses.

Here are the IRS site addresses that might be of specific interest:

Home page for small businesses and self-employed individuals - *http://www.irs.gov/businesses/small/index.html*

Small business forms and publications - *http://www.irs.gov/formspubs/index.html*

IRS forms in espanol - *http://www.irs.gov/espanol/article/0,,id=132230,00.html*

Frequently Asked Questions - *http://www.irs.gov/faqs/index.html*

APPENDIX A

10 CYBER SECURITY TIPS FOR SMALL BUSINESS

Broadband and information technology are powerful factors in small businesses reaching new markets and increasing productivity and efficiency. However, businesses need a cybersecurity strategy to protect their own business, their customers, and their data from growing cybersecurity threats.

1. Train employees in security principles

Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2. Protect information, computers and networks from cyber attacks

Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. Provide firewall security for your Internet connection

A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system's firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. Create a mobile device action plan

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost/stolen equipment.

5. Make backup copies of important business data and information

Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable and payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

6. Control physical access to your computers and create user accounts for each employee

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7. Secure your Wi-Fi networks

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. Employ best practices on payment cards

Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don't use the same computer to process payments and surf the Internet.

9. Limit employee access to data and information, limit authority to install software

Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Source: Federal Communications Commission (www.fcc.gov/general/cybersecurity-small-business)

APPENDIX B

LEGISLATION PERTINENT TO A DATA BREACH

Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have legislation requiring private, governmental or educational entities to notify individuals of security breaches involving personally identifiable information that could affect them.Typically, these laws define who must comply (e.g., businesses, data brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with social security number, driver license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition, viewing or copying of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Alaska	*Alaska Stat. § 45.48.010 et seq.*
Arizona	*Ariz. Rev. Stat. § 44-7501*
Arkansas	*Ark. Code § 4-110-101 et seq.*
California	*Cal. Civ. Code §§ 1798.29, 1798.80 et seq.*
Colorado	*Colo. Rev. Stat. § 6-1-716*
Connecticut	*Conn. Gen Stat. § 36a-701b, 2015 S.B. 949, Public Act 15-142*
Delaware	*Del. Code tit. 6, § 12B-101 et seq.*
Florida	*Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)*
Georgia	*Ga. Code §§ 10-1-910, -911, -912; § 46-5-214*
Hawaii	*Haw. Rev. Stat. § 487N-1 et seq.*
Idaho	*Idaho Stat. §§ 28-51-104 to -107*
Illinois	*815 ILCS §§ 530/1 to 530/25*
Indiana	*Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq.*
Iowa	*Iowa Code §§ 715C.1, 715C.2*
Kansas	*Kan. Stat. § 50-7a01 et seq.*
Kentucky	*KRS § 365.732, KRS §§ 61.931 to 61.934*
Louisiana	*La. Rev. Stat. §§ 51:3071 et seq., 40:1300.111 to .116*
Maine	*Me. Rev. Stat. tit. 10 § 1347 et seq.*
Maryland	*Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 - 1308*
Massachusetts	*Mass. Gen. Laws § 93H-1 et seq.*
Michigan	*Mich. Comp. Laws §§ 445.63, 445.72*
Minnesota	*Minn. Stat. §§ 325E.61, 325E.64*
Mississippi	*Miss. Code § 75-24-29*

Missouri	*Mo. Rev. Stat. § 407.1500*
Montana	*Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 et seq., 33-19-321*
Nebraska	*Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807*
Nevada	*Nev. Rev. Stat. §§ 603A.010 et seq., 242.183*
New Hampshire	*N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21; 189:66*
New Jersey	*N.J. Stat. § 56:8-161, -163*
New York	*N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208*
North Carolina	*N.C. Gen. Stat §§ 75-61, 75-65*
North Dakota	*N.D. Cent. Code §§ 51-30-01 et seq., 51-59-34(4)(d)*
Ohio	*Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192*
Oklahoma	*Okla. Stat. §§ 74-3113.1, 24-161 to -166*
Oregon	*Oregon Rev. Stat. § 646A.600 to .628, 2015 S.B. 601, Chap. 357*
Pennsylvania	*73 Pa. Stat. § 2301 et seq.*
Rhode Island	*R.I. Gen. Laws § 11-49.2-1 et seq., 2015 S.B. 134, Public Law 2015-138, 2015 H.B. 5220, Public Law 2015-148*
South Carolina	*S.C. Code § 39-1-90, 2013 H.B. 3248*
Tennessee	*Tenn. Code § 47-18-2107; § 8-4-119 (2015 S.B. 416, Chap. 42)*
Texas	*Tex. Bus. & Com. Code §§ 521.002, 521.053; Tex. Ed. Code § 37.007(b)(5); Tex. Pen. Code § 33.02*
Utah	*Utah Code §§ 13-44-101 et seq.; § 53A-13-301(6)*
Vermont	*Vt. Stat. tit. 9 § 2430, 2435*
Virginia	*Va. Code § 18.2-186.6, § 32.1-127.1:05, § 22.1-20.2*
Washington	*Wash. Rev. Code § 19.255.010, 42.56.590, 2015 H.B. 1078, Chapter 65*
West Virginia	*W.V. Code §§ 46A-2A-101 et seq.*
Wisconsin	*Wis. Stat. § 134.98*
Wyoming	*Wyo. Stat. § 40-12-501 et seq.*
Dist. of Columbia	*D.C. Code § 28- 3851 et seq.*
Guam	*9 GCA § 48-10 et seq.*
Puerto Rico	*10 Laws of Puerto Rico § 4051 et seq.*
Virgin Islands	*V.I. Code tit. 14, § 2208*

** States with no security breach law: Alabama, New Mexico, and South Dakota*

APPENDIX C

LAWS REGULATING DATA PRIVACY IN THE U.S.

The following list contains a number of United States federal and state laws that have provisions for data privacy, control or regulation:

- Americans with Disabilities Act (ADA)
- Cable Communications Policy Act of 1984 (Cable Act)
- California Senate Bill 1386 (SB 1386)
- Children's Internet Protection Act of 2001 (CIPA)
- Children's Online Privacy Protection Act of 1998 (COPPA)
- Communications Assistance for Law Enforcement Act of 1994 (CALEA)
- Computer Fraud and Abuse Act of 1986 (CFAA)
- Computer Security Act of 1987 – (Superseded by the Federal Information Security Management Act (FISMA)
- Consumer Credit Reporting Reform Act of 1996 (CCRRA) – Modifies the Fair Credit Reporting Act (FCRA).
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003
- Electronic Funds Transfer Act (EFTA)
- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Fair Credit Reporting Act (Full Text).
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission Act (FTCA)
- Driver's Privacy Protection Act of 1994
- Electronic Communications Privacy Act of 1986 (ECPA)
- Electronic Freedom of Information Act of 1996 (E-FOIA)
- Fair Credit Reporting Act of 1999 (FCRA)
- Family Education Rights and Privacy Act of 1974 (FERPA; also called the Buckley Amendment)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
- Privacy Act of 1974 – including U.S. Department of Justice Overview
- Privacy Protection Act of 1980 (PPA)
- Right to Financial Privacy Act of 1978 (RFPA)
- Telecommunications Act of 1996
- Telephone Consumer Protection Act of 1991 (TCPA)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- Video Privacy Protection Act of 1988 discussion and overview

APPENDIX D

LAWS REGULATING DATA PRIVACY OUTSIDE THE U.S.

The following list contains a number of international privacy related laws by country and region:

- Argentina: Personal Data Protection Act of 2000 (aka Habeas Data)
- Austria: Data Protection Act 2000, Austrian Federal Law Gazette part I No. 165/1999 (Datenschutzgesetz 2000 or DSG 2000)
- Australia: Privacy Act of 1988
- Belgium: Belgium Data Protection Law and Belgian Data Privacy Commission Privacy Blog
- Brazil: Privacy currently governed by Article 5 of the 1988 Constitution.
- Bulgaria: The Bulgarian Personal Data Protection Act, was adopted on December 21, 2001 and entered into force on January 1, 2002. More information at the Bugarian Data Protection Authority
- Canada: The Privacy Act – July 1983
  Personal Information Protection and Electronic Data Act (PIPEDA) of 2000 (Bill C-6)
- Chile: Act on the Protection of Personal Data, August 1998
- Colombia: Two laws affecting data privacy – Law 1266 of 2008: (in Spanish) and Law 1273 of 2009 (in Spanish) Also provides any person the right to update their personal information
- Czech Republic: Act on Protection of Personal Data (April 2000) No. 101
- Denmark: Act on Processing of Personal Data, Act No. 429, May 2000
- Estonia: Personal Data Protection Act of 2003. June 1996, Consolidated July 2002
- European Union: European Union Data Protection Directive of 1998
- EU Internet Privacy Law of 2002 (DIRECTIVE 2002/58/EC)
- Finland: Act on the Amendment of the Personal Data Act (986) 2000
- France: Data Protection Act of 1978 (revised in 2004)
- Germany: Federal Data Protection Act of 2001
- Greece: Law No.2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.
- Guernsey: Data Protection (Bailiwick of Guernsey) Law of 2001
- Hong Kong: Personal Data Ordinance (The “Ordinance”)
- Hungary: Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interests (excerpts in English)
- Iceland: Act of Protection of Individual; Processing Personal Data (Jan 2000)
- Ireland: Data Protection (Amendment) Act, Number 6 of 2003
- India: Information Technology Act of 2000
- Italy: Data Protection Code of 2003
- Italy: Processing of Personal Data Act, January 1997
- Japan: Personal Information Protection Law (Act) (Official English Translation)
  Law Summary from Jonesday Publishing

- Japan: Law for the Protection of Computer Processed Data Held by Administrative Organs, December 1988.
- Korea – Act on Personal Information Protection of Public Agencies Act on Information and Communication Network Usage
- Latvia: Personal Data Protection Law, March 23, 2000
- Lithuania: Law on Legal Protection of Personal Data (June 1996)
- Luxembourg: Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data.
- Malaysia – Common Law principle of confidentiality Personal data Protection Bill (Not finalized) Banking and Financial Institutions Act of 1989 privacy provisions.
- Malta: Data Protection Act (Act XXVI of 2001), Amended March 22, 2002, November 15, 2002 and July 15, 2003
- Mexico: Federal Law for the Protection of Personal Data Possessed by Private Persons (Spanish)
- Morocco: Data Protection Act
- Netherlands: Dutch Personal Data Protection Act 2000 as amended by Acts dated 5 April 2001, Bulletin of Acts, Orders and Decrees 180, 6 December 2001
- New Zealand: Privacy Act, May 1993; Privacy Amendment Act, 1993 & 1994
- Norway: Personal Data Act (April 2000) – Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act)
- Philippines: DATA PRIVACY ACT OF 2011 There is also a recognized right of privacy in civil law and a model data protection code.
- Romania: Law No. 677/2001 for the Protection of Persons concerning the Processing of Persona Data and the Free Circulation of Such Data
- Poland: Act of the Protection of Personal Data (August 1997)
- Portugal: Act on the Protection of Personal Data (Law 67/98 of 26 October)
- Singapore – The E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce
- Slovak Republic: Act No. 428 of 3 July 2002 on Personal Data Protection
- Slovenia: Personal Data Protection Act , RS No. 55/99
- South Africa: Electronic Communications and Transactions Act, 2002
- South Korea: The Act on Promotion of Information and Communications Network Utilization and Data Protection of 2000 http://www.internet.org.za/ect_act.html
- Spain: ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data
- Switzerland: The Federal Law on Data Protection of 1992
- Sweden: Personal Data Protection Act (1998:204), October 24, 1998
- Taiwan: Computer Processed Personal data Protection Law – applies only to public institutions
- Thailand: Official Information Act, B.E. 2540 (1997) for state agencies (Personal data Protection bill under consideration)

- United Kingdom: UK Data Protection Act 1998 Privacy and Electronic Communications (EC Directive) Regulations 2003 official text, and a consumer oriented site at the Information Commissioner's Office
- Vietnam: The Law on Electronic Transactions 2008

APPENDIX E

ACRONYMS

The cybersecurity area is essentially dominated by computers, the government and law enforcement so its sure to have lots of acronyms. Here's a partial list of some of the more 'common' acronyms you might come across when dealing with cybersecurity in small business.For additional terms, acronyms and definitions, visit ***NIST.gov***:

3DES	Triple Data Encryption Standard
A&A	Assessment and Authorization
ACL	Access Control List
AD	Active Directory
AD-IDS	Anomaly Detection Intrusion Detection System
ADP	Automated Data Processing
AES	Advanced Encryption Standard
AFC4A	Air Force C4 Agency
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFOSI	Air Force Office of Special Investigation
AFPD	Air Force Policy Directive
AFS	Apple File Sharing
AH	Authentication Header
AIMS	Automated Infrastructure Management System
AIS	Automated Information Systems
ALE	Annual Loss Expectancy
AMIDS	Audit Monitoring and Intrusion Detection System
ANSI	American National Standards Institute
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
APIs	Application Program Interfaces
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASD	Assistant Secretary of Defense for Command, Control, Communication and Intelligence
ASIMS	Automated Security Incident Measuring System
ASR	Automated System Recovery
ASSIST	Automated System Security Incident Support Team
ATC	Authorization to Connect
ATD	AuthorizationTermination Date
ATM	Asynchronous Transfer Mode
ATO	Authorization to Operate
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input And Output System
BMA	Business Mission Area
C&A	Certification and Accreditation
C&A WG	Certification and Accreditation Working Group
C2	Command and Control
C3	Command, Control and Communication
C2W	Command and Control Warfare
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance

CA	Certificate Authority
CAAP	Critical Asset Assurance Program
CAC	Common Access Card
CAL	Category Assurance List
CAP	Connection Approval Program
CAST	Carlisle Adams Stafford Tavares
CBF	Critical Business Functions
CC	Common Criteria
CC	Common Criteria
CCA	Clinger-Cohen Act
CCB	Configuration Control Board
CCI	Control Correlation Identifier
CD	Cross Domain
CD-R	Compact Disk Recordable
CDS	Cross-Domain Solution
CEI	Computer Ethics Institute
CERT	Computer Emergency Response Team
CERT/CC	CERT/Coordination Center
CESA	Cyberspace Electronic Security Act
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CI	Counterintelligence
CIAC	Computer Incident Advisory Capability
CIAO	Critical Infrastructure Assurance office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPWG	Critical Infrastructure Protection Working Group
CIRT	Computer Incident Response Team
CISA	C4I Integration Support Activity
CITAC	Computer Investigation and Infrastructure Threat Assessment Center
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman, Joints Chiefs of Staff Instruction
CMDS	Computer Misuse Detection System
CMP	Certificate Management Protocols
CMS	COMSEC Management System
CN	Canonical Name
CNA	Computer Network Attack
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CO	Central Office
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CPS	Certificate Practice Statement
CPSR	Computer Professionals of Social Responsibility
CRL	Certificate Revocation List
CSA	Computer Security Act

CSIRT	Computer Security Incident Response Team
CSS	Central Security Service
CSSO	Computer Systems Security Officers
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority (DAA)
DAC	Discretionary Access Control
DARPA	Defense Advanced Research Projects Agency
DASD	Deputy Assistant Secretary of Defense
DASD(DT&E)	Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
DATO	Denial Of Authorization To Operate
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCMO	Deputy Chief Management Office
DCPDS	Defense Civilian Personnel Data System
DDoS	Distributed Denial of Service
DES	Digital Encryption Standard
DES	Data Encryption Standard
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIACCS	Defense IA Command and Control System
DIAMOND	Defense Intrusion Analysis & Monitoring Desk
DIAP	Defense Information Assurance Program
DIB	Defense Industrial Base
DIDS	Distributed Intrusions Detection System
DII	Defense Information Infrastructure
DIMA	DoD portion of the intelligence mission area
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITPR	DoD Information Technology Portfolio Repository
DITSCAP	DoD IT Security Certification and Accreditation Process
DITSWG	Defense Information Technology Security Working Group
DMARC	Domain Based Message Authentication
DMARC	Telephone or Communications Connection Demarcation Point (PSTN)
DMC	Defense MegaCenter
DMS	Defense Message System
DMZ	Demilitarized Zone
DN	Distinguished Name
DNI	Director of National Intelligence
DNS	Domain Name Service
DoD	Department of Defense
DoD CIO	DoD Chief Information Officer
DoD ISRMC	DoD Information Security Risk Management Committee
DoDD	Department of Defense Directive
DoDI	DoD Instruction
DoDIIS	DoD Intelligence Information System
DODIN	Department of Defense information networks
DoDM	DoD manual
DoE	Department of Energy

DoN	Department of the Navy
DoS	Denial of Service
DOT&E	Director, Operational Test and Evaluation
DREN	Defense Research and Engineering Network
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSAWG	Defense IA Security Accreditation Working Group
DSL	Digital Subscriber Line
DSS	Defense Security Service
DSSS	Direct Sequence Spread Spectrum
DT&E	Developmental Test and Evaluation
DTM	Directive-Type Memorandum
E/APL	Evaluated Approved Product
EAL	Evaluation Assurance Level
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EFOIA	Electronic Freedom of Information Act
EIEMA	Enterprise Information Environment Mission Area
EIGRP	Enhanced Interior Gateway Routing Protocol
EITDR	Enterprise Information Technology Database Repository
EM	Emergency Management
eMASS	Enterprise Mission Assurance Support Service
EMI	Electromagnetic Interference
EOP	Executive Office of the President
ESP	Encapsulating Security Payload
ETA	Education, Training and Awareness
ETAPWG	Education, Training, Awareness and Professionalization Working Group
EULA	End User License Agreement
FAT	File Allocation Table
FERPA	Family Educational Rights and Privacy Act
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FIPSPUB	Federal Information Processing Standard Publication
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FIWC	Fleet information Warfare Center
FN	Foreign National
FOIA	Freedom of information Act
FSO	Field Security Office
FTP	File Transfer Protocol
FTS	Federal Telecommunications Service
GAO	General Accounting Office
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GFS	Grandfather Father Son
GIG	Global Information Grid
GMITS	Guidelines for the Management of IT Security
GOSC	Global Operations and Security Center
GOTS	Government Off-the-Shelf
GSA	General Services Administration
GSII	Government Services Information Infrastructure
GSM	Global System for Mobile Communications

GUI	Graphical User Interface
GUID	Globally Unique Identifier
HBSS	Host Based Security System
H-IDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
I&A	Identification and Authentication
I&W	Indications and Warning
IA	Information Assurance
IAD	Information Assurance Document
IAG	Information Assurance Group
IAM	Information Assurance Manager
IANA	Internet Assigned Numbers Authority
IAO	Information Assurance Officer
IAPWG	Information Assurance Policy Working Group
IASE	Information Assurance Support Environment
IATAC	Information Assurance Technology Analysis Center
IATC	Interim Authority to Connect
IATO	Interim Authority to Operate
IATT	Interim Authority to Test
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
ICMP	Internet Control Message Protocol
ID	Intrusion Detection
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IEEE	Institute for Electrical and Electronics Engineers
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IIS	Internet Information Server
IM	Instant Messaging
IMAP	Internet Message Access Protocol
INFOCONs	Information Operations Conditions
INFOSEC	Information Systems Security
INFOSYS	Information Systems
IO	Information Operations
IP	Internet Protocol
IPR	Internet Protocol Router
IPSec	Internet Protocol Security
IPTF	Infrastructure Protection Task Force
IPX/SPX	Internetwork Packet Exchange / Sequenced Packet Exchange
IR	Infrared
IRC	INFOSEC Research Council
IRM	Information Resource Management
IRP	Incident Response Plan
IRS	Incident Reporting Structure
IRT	Incident Response Team
IS	Information Systems

ISDN	Integrated Systems Digital Network
ISN	Initial Sequence Number
ISO	International Organization for Standardization
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISRMC	Information Security Risk Management Committee
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITMRA	Information Technology Management Reform Act
ITU	International Telecommunications Union
IW	Information Warfare
IWD	Information Warfare Defensive
JCCC	Joint Communications Control Center
JCIDS	Joint Capabilities Integration and Development System
JDIICS	Joint DII Control Systems
JFS	Journaled File System
JID	oint Intrusion Detection
JIE	Joint Information Environment
JIEO	Joint Interoperability Engineering Organization
JIWG	Joint IA Operations Working Group
JPO STC	Joint Program Office for Special Technical Countermeasures
JTF-CNO	Joint Task Force Computer Network Operations
JWICS	Joint Worldwide Intelligence Communications System
JWID	Joint Warrior Interoperability Demonstration
KDC	Key Distribution Center
KEA	Key Exchange Algorithm
KMI	Key Management Infrastructure
KS	Knowledge Service
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LCP	Link Control Protocol
LDAP	Lightweight Data Access Protocol
LE	Law Enforcement
LE/CI	Law Enforcement and Counterintelligence
LEA	Law Enforcement Agency
LRA	Local Registration Authority
MA	Mission Area
MAC	Mandatory Access Control
MAC	Media Access Control (or Code)
MCDES	Malicious Code Detection and Eradication System
MDA	Message Digest Algorithm
MD-IDS	Misuse Detection Intrusion Detection System
MIME	Multipurpose Internet Mail Extensions
MLS WG	Multilevel Security Working Group
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MSSP	Managed Security Service Provider
MTBF	Mean Time Before Failure
MTTR	Mean Time To Repair
NA	Not Applicable

NACIC	National Counterintelligence Center
NAT	Network Address Translation
NC	Non-compliant
NCIS	Naval Criminal Investigative Service
NCP	Network Control Protocol
NCSC	National Computer Security Center
NDA	Nondisclosure Agreement
NDS	Netware/Novell Directory Services
NDU	National Defense University
NetBEUI	Network Basic Input Output System Extended User Interface
NetBIOS	Network Basic Input Output System
NFS	Network File System
NIAC	National Infrastructure Assurance Council
NIC	Network Interface Card
NID	Network Intrusion Detector
N-IDS	Network-based Intrusion Detection System
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIPRNet	Non-Classified Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NITB	National INFOSEC Technical baseline
NLM	Netware Loadable Modules
NNTP	Network News Transfer Protocol
NOC	Network Operations Center
NOS	Network Operating System
NOSC	Network Operation Security Center
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSD	National Security Directive
NSIRC	National Security Incident Response Center
NSOC	National Security Operations Center
NSS	National Security System
NSS	Netware Storage Service
NSTAC	National Security Telecommunication Advisory Committee
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSU	Non-Standard Usage
NTFS	New Technology File System
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications & Intelligence
OCSP	Online Certificate Status Protocol
OES	Open Enterprise Server
OFDM	Orthogonal Frequency Division Multiplexing
OIG DoD	Office of the Inspector General of the Department of Defense
OMB	Office of Management and Budget
OPSEC	Operations Security
ORNL	Oak Ridge National Laboratory
OS	Operating System
OSD	Office of the Secretary of Defense
OSD/JS	Office of the Secretary of Defense/Joint Staff
OSPF	Open Shortest Path First
OT&E	Operational Test and Evaluation

OU	Organizational Unit
OUSD(P)	Office of the Under Secretary of Defense (Policy)
PAO	Principal Authorizing Official
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PCCIP	President's Commission on Critical Infrastructure Protection
PCI	Payment Card Industry
PDA	Personnel Digital Assistant
PGP	Pretty Good Privacy
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIT	Platform Information Technology
PKC	Public Key Cryptography
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PM	Program Manager
PM/SM	Program Manager/System Manager
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Program Protection Plan
PPP	Point to Point Protocol
PPS	Internet protocol suite and associated ports
PPSM	ports, protocols, and services management
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent/Inexpensive Disks
RAS	Remote Access Services
RBAC	Role-Based Access Control
RC	Ron’s Code or Rivest’s Cipher
RCERTs	Regional Computer Emergency Response Teams
RDN	Relative Distinguished Name
RDT&E	Research, Development, Test and Evaluation
RF	Radio Frequency
RFC	Request for Comments
RFP	Request for Proposal
RFQ	Request for Quote
RFI	Radio Frequency Interference
RIP	Routing Information Protocol
RMF	Risk Management Framework
ROSC	Regional Operations and Security Center
RPC	Remote Procedure Call
RRAS	Routing and Remote Access Services
RSH	Remote Shell
RT&E	Research, Test, and Evaluation
S/MIME	Secure Multipurpose Internet Mail Extensions
SABI WG	Secret and Below Interoperability Working Group

SAINT	Security Administrator's Integrated Network Tool
SAP	Special Access Program
SAPCO	SAP Central Office
SAR	Security Assessment Report
SATAN	Systems Administrators' Tool for Assessing Networks
SBU	Sensitive-But-Unclassified
SCA	Security Control Assessor
SCAO	SIPRNET Connection Approval Office
SCAP	Security Content Automation Protocol
SCCVI	Secure Configuration Compliance Validation Initiative
SCG	Security Configuration Guide
SCI	Sensitive Compartment Information
SCRI	Secure Compliance Remediation Initiative
SECDEF	Secretary of Defense
SEI	Software Engineering Institute
SET	Secure Encrypted Transaction
SHA	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transport Protocol
SIM	Subscriber Identification Model
SIO	Special Information Operations
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officer
SITR	Secret Internet Protocol Router Network Information Technology Registry
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SLIP	Serial Line Internet Protocol
SM	System Manager
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNAP	Systems/Networks Approval Process
SNMP	Simple Network Management Protocol
SP	Special Publication
SPB	Security Policy Board
SPX	Sequenced Packet Exchange
SQL	Structured Query Language
SRG	security requirements guide
SSAA	Systems Security Authorization Agreement
SSE	System Security Engineering
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSO	Single Sign On
STIGs	Security Technical Implementation Guides
STP	Shielded Twisted Pair
T&E	Test and Evaluation
TACACS	Terminal Access Controller Access Controller System
TAG	Technical Advisory Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer Systems Evaluation Criteria
TFTP	Trivial File Transfer Protocol
THREATCON	Threat Condition
TLS	Transport Layer Security

TPM	Trusted Platform Module
TRANSEC	Transmission Security
TRMC	Test Resource Management Center
TSN	Trusted Systems and Networks
U.S.C.	United States Code
UC	Unified Capabilities
UCAO	Unclassified Connection Approval Office
UCDMO	Unified Cross Domain Management Office
UCMJ	Uniform Code of Military Justice
UDP	User Datagram Protocol
UPN	User Principal Name
UPS	Uninterruptible Power Supply
UR	User Representative
URL	Uniform Resource Locator (Universal Resource Locator)
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required and Obstruct Terrorism
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(P)	Under Secretary of Defense for Policy
USSTRATCOM	United States Strategic Command
UTP	Unshielded Twisted Pair
UV	Ultraviolet
VAAP	Vulnerability and Assessment Program
VAS	Vulnerability Assessment System
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Networks
WAP	Wireless Access Point
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WMA	Warfighting Mission Area
WML	Wireless Markup Language
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web
XKMS	eXtensible Markup Language Key Management Specifications
XML	eXtensible Markup Language

- NOTES -

- NOTES -

- NOTES -

- NOTES -