Network and System Security for Small- and Medium-sized Businesses

(This document includes the full plan, including Parts 1, 2, and 3.)

Should You Be Concerned about Computer Security? If you question whether you need to improve the maturity your cybersecurity posture, just do an online search about the cost of "ransomware" and a "data breach", and then consider the implications if your personal company information was posted online for everyone to see or was encrypted so you lost all your company information!

Realistic Computer Security: Cybersecurity is a Journey, not a Destination. Understand that nothing can be 100% secure; our journey is all about reducing the risk of compromise to an acceptable level and being able to respond quickly to a security incident. You must use people, processes, and technology to take steps in the right direction, make incremental changes, and plan the phases for this work to be carried out. Your security posture must mature over time. Just make a plan and start from where you are - NOW.

Purpose and Overview

This security plan is meant to help small- to medium-sized businesses (SMBs) secure their digital information. It assumes that you have a local area network with a connection to the Internet.

If you are an individual looking for computer security advice, please see the "Essential Security Measures for Home Computers" document (which also has some great advice for SMBs) at www.ComputerSecurityNW.com. If you are an individual or part of a team living overseas, I highly recommend that you take the training and follow the steps listed at www.expatdigital.com

If the steps here sound like "Greek to you", then you should probably hire a computer professional to help you with this process. Don't let "lack of technical skill" be an excuse to not accomplish the tasks listed here.

This Security Journey includes the following major steps, as detailed in the document below. (See the accompanying "Checklist" that lists these items in a succinct manner.)

Part 1: Implement Essential Security Measures (Basic Security Controls & Security Policies)

A. Critical Steps: (No Risk Assessment Needed)

- Network Hardening - Boundary Defense
- Workstation and Server Hardening
- Traveling & Remote Workers
- Mobile Device Security

Consider doing some basic risk assessment work at this point.

B. Very Important Steps:

- Disaster Recovery Plans (with Backups)
- Cloud-based Security
- End-User Security Awareness Training
- Miscellaneous System Security Items

C. Important Steps:

- Create and Comply with Security Policies
- Control Vendor Access and Understand Vendor Risk
- Security Assessments
- Incident Response Planning – Prepare for a Breach

Part 1: Implement Essential Security Measures

Rationale: Every business (and individual) must protect themselves against common cybercriminals looking to illegally profit from their electronic information (e.g. identity theft, banking information, ransomware demands, online impersonation to scam friends, stealing your network bandwidth to attack others, crypto-mining, etc.).

Apply These Critical/Basic Security Controls

1) **Boundary Defense: Network Hardening Process**
   a) Install a "small business router" in addition to your Internet modem. A business-grade router increases your security by providing separate firewall and NAT capabilities, including a more robust router operating system (O.S.). (Do not get a "consumer-grade" version of a router; they are inadequate for maintaining a secure network posture.)
      i) See my "Secure Routers for Home and Small Businesses" document for specific recommendations on which routers to purchase and how to configure them.
      See: www.computersecuritynw.com
      ii) Any medium-sized business, or a business with more security needs, should strongly consider getting a network Firewall, separate from the one included in a small business router. Consider the following high-quality and well-respected firewalls:
         (1) Palo Alto Networks PA-220: www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-220
         (2) Cisco ASA 5506-X with FirePOWER Services: www.cisco.com/c/en/us/support/security/asa-5506-x-firepower-services/model.html (or other similar models, found here: www.cisco.com/c/en/us/products/security/asa-firepower-services/compare-models.html)
         (3) Fortinet entry-level Firewalls: www.fortinet.com/products/next-generation-firewall/entry-level.html
      iii) Larger businesses, besides needing a separate Firewall, will most likely also want to apply a network segmentation strategy, based on security needs of data in their data center.
   b) Change the default passwords on all equipment in the environment, including all network equipment (routers, switches, Wi-Fi access points, etc.) and "smart devices" (anything that has a network connection, including all Internet-of-Things [IoT] devices).
   c) Wireless Access Control: For all wireless networks (Wi-Fi) make sure to implement WPA2 or turn off Wi-Fi if you don't need wireless connectivity.
   d) If you host a web server (or offer other services) accessible from the Internet at your place of business (as opposed to having a third-party hosting environment), make sure to put it in a network Demilitarized Zone (DMZ). (This can be a "logical DMZ", using a port off the router/firewall, or can be a hardware DMZ by purchasing two hardware Firewalls.)
      i) Run vulnerability tests against all software on your web server.

2) **Workstation and Server Hardening Process**
   a) (See the "Essential Security Measures for Home Computers" document for more workstation hardening ideas and for details of many of these processes.)
   b) Make sure to run an updated version of the operating system (O.S.), such as Windows 10 (or Windows Server 2016) or a newer macOS. Do NOT run versions that are no longer supported, such as Windows XP/7 or Windows Server 2003/2008.

i) **Critical Note:** No matter where you are in the world, you must purchase a legitimate copy of the operating system. The operating system must not be a pirated copy; these free, pirated copies are known to be full of viruses and backdoor programs that steal your passwords and data. -- If you are looking for a "free" operating system, then run Linux.

c) Vulnerability Management: Keep your Operating Systems patched by regularly applying security and critical updates (for Microsoft, Apple, Linux, etc.).
   i) This is a critical step!! Most exploits can be stopped by applying patches and updates to your operating system and programs!
   ii) If possible, set the O.S. to update automatically. If not automatically updated, put a plan in place to install updates monthly.

d) Remove all unnecessary software, especially Adobe Flash and Java
   i) If this software is needed, make sure it is updated to the latest version, and set to automatically update.
   ii) Note that Adobe Flash is a dying software; soon to be no longer supported or updated. It is full of security flaws. You should work actively to remove it from your environment.

e) Servers: Reduce the attack surface by turning off all unnecessary services and software on systems. For more details, do an Internet search for best practices for Server Hardening.

f) Web-Browser Hardening: Web-browsers (such as Internet Explorer, Edge, Chrome, Firefox, etc.) are the most insecure and most widely attacked software on your computer.
   i) Run only the latest version of the web-browser you choose to use.
   ii) Minimize the use of any web-browser plug-ins; many only make your browser less secure, and some are used to steal your information or leak your private actions.
   iii) Only run Adobe and Java plug-ins actively in your web browser when you are using them. (In other words, "disable" them when they are not needed for the website you are viewing.)
   iv) Do NOT allows your browser to automatically store your passwords for online logins/accounts! Use a third-party password program that encrypts your passwords. See my "Essential Security Measures for Home Computers" for suggested password programs.
   v) You should not browse the Internet from a Server! If you must do so, only do this very cautiously and only when there is a business need to do so; only go to known good websites for a very specific purpose, such as downloading a program update.

g) Controlled Use of Administrative Privileges: For Windows users, require that all accounts be run in "Standard" (i.e. non-administrative) mode. In other word, the average user should NOT be an "Administrator" of their own computer; at most they should be a "Power User". This helps reduce the damage malware can do on your computer. If admin rights are needed, use a separate username that has privileged rights only when you need them.

h) Malware Defenses: Run reputable Antivirus software and make sure it is updated automatically.
   i) The built-in Microsoft antivirus software is typically not adequate protection.
   ii) Even if you run only Mac computers, you still need to install antivirus software.
   iii) See my "Essential Security Measures for Home Computers" for suggested antivirus suites.

i) Make sure your software firewall is active on all workstations.

3) **Traveling or Remote Workers**:

a) Any machine traveling outside your office should run full disk encryption. This will minimize any breach of confidential information in case the computer is lost or stolen. (You should have a very good business reason for deciding not to do full disk encryption! I can't think of one.)

i) Both Windows and Macs come with very good hard disk encryption capabilities included in their business versions.
ii) Most likely you will want to encrypt hard drives on all computers, to avoid exposure in case machines are stolen or confiscated from your office.

b) Make sure remote workers use VPN software/services on their computers anytime they are in public Wi-Fi locations.

c) If you provide Internet-accessible software or services to your employees, then one of the most important things you can do is to require multi-factor authentication (MFA – also referred to as two-factor authentication [2FA]). If this applies to you, then you MUST make this a priority! This should no longer be considered optional if you are concerned about the confidentiality of any data accessible from the Internet. (See "Resources for Further Research" section below for more info on MFA.) - **NOTE**: People use either the term "Multi-Factor Authentication" (MFA) or "Two-Factor Authentication" (2FA) to refer to the same thing, using at least 2 ways of confirming a person is who they say they are, usually a username/password and a smartphone confirmation (SMS, Google Authenticator app, etc.)
   i) For instance: if people can access their email from a web-browser, then that is an internet-accessible web service that must require MFA/2FA; otherwise, just assume that bad-actors are reading some or all your email! Seriously!
   ii) Any Cloud-provided services (such as file storage [e.g. Dropbox], email, other applications) should include this requirement for MFA.
   iii) Your MFA solution can consist of the free "Google Authenticator" app installed on the user's smartphone, or can pay for a more robust corporate version of MFA software, such as the excellent solution provided by Duo (www.duo.com). (See "Resources for Further Research" section below for more MFA production options.)

4) Mobile Device Security

a) Even without a formal Mobile Device Management (MDM) program or policy, you need to consider the sensitivity of data your users are storing on their mobile devices (smartphones, tablets, etc.).

b) Consider things like: requiring operating system security updates, requiring a PIN/Password on each device, auto-lock after a certain amount of time not used, remote wipe if/when device is lost, required encryption of device, etc.

c) See this page for further advice on Smartphone security: www.computersecuritynw.com/essential-smartphone-security

d) Larger organizations should implement a full MDM solution such as Microsoft's InTune or VMware's Airwatch.

Before continuing the information security journey as outlined below, consider doing a high-level risk assessment as outlined in Part 2 of this Plan.

Continue with Very Important Security Controls

5) Basic Disaster Recovery Plan – Data Recovery Capabilities

a) Backup all important data regularly and automatically!! This may be your only chance of recovering from a ransomware event!
   i) See my "Simple Backup Strategy" document for ideas if you have not already implemented a rigorous backup strategy.
   ii) Data should be encrypted as it is backed up.
   iii) Make sure to store backups offsite to protect against large-scale disasters. (At least periodically and regularly take backups offsite, if not all the time).
   iv) Periodically test your backup to make sure you can recover files when needed, especially the first time you create a backup.
   v) Monitor the backup process (log files) to make sure the backup completed properly.
      (1) Worse than not having a backup is thinking you have one, only to find out that you cannot restore critical data when you need it!

b) Make sure to document an overview of a data recovery plan for various scenarios, such as a ransomware event, deleted files, hard disk crash, theft of networking equipment, etc.

6) Cloud-based Security

a) Make sure to manage confidential information stored in the Cloud (such as Box, Dropbox, Google Drive, MS OneDrive, etc.)
   i) Consider using Cloud storage services that offer strong security offerings, such as, data access segmentation, mature security governance, and data loss prevention features. You should understand the features you require and use Cloud storage appropriately.

b) You should know what information is stored online, understand the risks (e.g. the possibility of data being hacked into and stolen, the possibility of being read and used by the hosting company for marketing purposes, the cloud service being offline and thus having no access to your data, etc.), and make sure to have it protected with strong passwords, and contingency plans.

c) You may want to make sure all data is encrypted before being put into the Cloud.

d) Make sure to manage passwords for these Cloud services; if passwords are compromised, your data will be stolen.

e) If possible, use two-factor authentication (2FA/MFA) for all online/Cloud accounts.

7) Train Your Users – Lack of security-awareness by your users can be the largest security hole in your environment!

a) Most security incidents depend on the cooperation of your users for successful exploitation. Criminal hackers use social engineering tactics to trick users into cooperating with them. This can come via many means, such as through email, phone call, text, a pop-up on a web-browser, etc.

b) Many, if not most, security incidents start with a phishing email and a user clicking on an attachment that either steals their login credentials or installs malware.

c) Be very suspicious of unsolicited phone calls, or a pop-up in a web-browser asking you to install anything or even to click “OK”. (See blog post about Social Engineering at www.computersecuritynw.com/blog for more details and examples.)

d) Strongly consider having all users take an online training course on general security practices, but at least tell them the following items:
   i) (If you are a worker or organization living in a foreign country, I strongly recommend that all your team members take the training at www.expatdigital.com)

ii) Never open unsolicited attachments to emails!! STOP immediately if an emailed attachment asks for your username and password; this is a credential-stealing attack!
iii) Understand Phishing and don't fall for it; e.g. your bank will NEVER ask for your password!
iv) Do not click on website links (URLs) in emails! Unless you have initiated that email being sent to you (by asking for a password reset, etc.), and even then, be suspicious. You are better off going to a trusted website and logging in via your normal method.
v) Don't believe a website pop-up that tells you that you have a virus and urges to you "click here" to scan/clean. Use your already-installed, trusted antivirus program.
vi) Do not respond to emails of business requests for money transfers (or from friends caught overseas with no money) without independently verifying the sender and the request. (E.g. validate the request with a phone call or text message, not via email.)

8) Miscellaneous System Security Items

a) Ensure email is encrypted in transit. This is the standard for any high-quality email provider, so hardly needs to be said. Just confirm your servers and clients are configured to only accept encrypted email.
b) To reduce the possibility of users being fooled by phishing emails, consider implementing a spam filter (centrally or on each computer individually).
c) Use an encrypted password vault program to store all administrative passwords.
d) If you have Service Accounts, make sure they have very complex passwords. You should use a very long password here (maybe 20+ characters) since these accounts are used to run software services and should not be used to login to the computer console.
e) Regularly update the firmware of all equipment in your environment.
f) **Higher Risk Situation (or larger networks):** A centralized log management system (or a SIEM) should be deployed and monitored to help detect and respond to security incidents and breaches.
g) To protect from electrical glitches and equipment being corrupted by shutting down unexpectedly, you should use Uninterruptible Power Supplies (UPS) on all your computers and equipment.

Continue with these Important Security Measures

9) **Security Policies -** Create basic security policies and expectations for all your employees/workers, and make sure they understand and follow them. Here is a basic overview of some of the policies you should create. See examples on the Internet for details.

a) Password Standards, including items such as:
i) Use long and strong passwords for all online accounts (especially financial ones and any Cloud storage) (See Resources at the end of this document for password suggestions.)
ii) DON'T use the same password for all your accounts. Use unique passwords for any important account.
iii) To remember important and unique passwords, use a program that encrypts your passwords, such as Dashlane, LastPass, KeePass, or 1Password.
iv) See the Resources section below for help on specific password policy items. However, consider this suggestion: *IF* you make your passwords strong enough, *AND* make sure your systems "lock out" a user after 5 or 6 incorrect password attempts, then you should not need to change your password every 60 or 90 days; changing the password once a year is adequate. – However, this will not be true if passwords are stolen, which is very common; so strongly consider implementing **multi-factor authentication** [MFA/2FA].

b) Protect any sensitive data written to flash drives or in backups, by encrypting it. Flash drives are easily lost or stolen.
c) Identify your strategy for data stored in the Cloud. Make sure to include details such as, which Cloud storage providers are acceptable to use, what kind of data should or should not be stored in the Cloud, password policies for Cloud providers, what kind of devices should or should not be used for Cloud access, requirement for multi-factor authentication [MFA/2FA], etc.
d) Create a Mobile Device usage policy, outlining requirements and expectations.
e) If employees travel with computers/laptops: do full disk encryption (BitLocker, VeraCrypt, FileVault, etc.)
f) Recycle your computers (and printers) securely by deleting all personal information first; or reformat and re-install the operating system.

10) Control Vendor Access and Vendor Risk

a) If you allow vendors to access your systems, you need to understand and manage the risk this poses. You don't know how vendors manage their security. If their systems or passwords are compromised, then your systems can be compromised. (This is a very common occurrence and the attack method for many "secure" companies.)
b) Control how you allow vendors to access your systems, especially if accessing via a remote location; you should either require multi-factor authentication [MFA/2FA] or require they coordinate with you and use a Webex-type session to login to your systems.
c) Furthermore, if you send data to vendors, then it is out of your control. If the vendor's systems are breached, your data may be compromised. Only send minimal/required data to vendors and insist that they have robust security practices/program as well as strong contractual arrangements for data breach contingencies.

11) Internal and External Security Assessments

a) You should be doing regular risk assessments of data and systems in your environment, as described in Part 2 of this document.
    i) Comprehensive risk assessments should be done regularly, such as annually.
    ii) On-going risk assessments should be done for any new systems or software introduced into your environment.
    iii) Set priorities for projects and to increase your security controls based on the level of risk discovered.
b) In order to give you a real-world view of how secure your environment is from criminal hackers, you should consider hiring a reputable firm to perform an external security assessment of your information systems. These security assessments can include various kinds of External Penetration Tests, Vulnerability Assessments, a Wireless Assessment, Social Engineering tests, Phishing attacks, etc.
c) The outcome of these kinds of assessments will give you a sense of your security posture as presented to potential attackers, as well as give you a concrete list of security items that you should address to make your organization more secure.

12) Incident Response Planning – Prepare for a Breach

a) In this Internet connected world, it is inevitable that you will have a "security incident". This may be anything ranging from a malware outbreak or ransomware attack, to a full-blown breach in which your most confidential data is accessed illegally. Your ability to detect this incident and

respond quickly is in direct relation to how much damage will be done, and cost incurred. The longer someone is in your network without you responding, the worse the damage will be.

b) You need to have a plan for how you will investigate and respond to a real or potential security incident, whether that be a phishing incident (where someone enters their credentials into an attackers website), a malware attack (that gives attackers a foothold into your network), a ransomware attack, or a Business Email Compromise attack (where you lose money based on a scam). Create a plan. Practice the plan. Involve all levels of your organization in creating and testing your plan. Following these steps to create your incident response plan:

c) **Write out a Plan**: Note the following 6 items for a written incident response plan: (from: digitalguardian.com/blog/incident-response-plan - See the link for more details.)
   i) **Assemble an Internal Team**
   ii) **Identify External Data Security Resources** – "Breach developments can get out of hand before the company can identify, interview and hire the experts needed to help the company meet breach-related obligations and minimize liability. A good Response Plan will identify each outside resource, provide full contact information ..."
   iii) **Differentiate Breaches** – "The Response Plan should have sufficient flexibility to establish an appropriate and effective process for different types of breaches."
   iv) **Create an Action Item Checklist** – "Well-crafted Response Plans for larger companies should include a checklist of prioritized action items to be completed immediately after the company learns of a potential significant data breach."
   v) **Track Key Breach-Related Rights, Obligations, and Deadlines**
   vi) **Review and Update the Response Plan Regularly**

d) As with the "risk assessment" below (Part 2), this can be a daunting topic. Don't get bogged down in details. Just start a plan. Write a paragraph about what constitutes an "incident." Identify internal and external people who should be contacted in case of an incident. (Include their phone numbers in the plan.) Write down the basic steps of responding to a few different malware or breach scenarios. Refine as you go. - See some resources for Incident Response listed in the Resources below.

Special Situation to Note - Ransomware:
Protect against and be prepared for ransomware attacks. (For an introduction to this topic and a list of further resources, see my blog post on Ransomware here: www.computersecuritynw.com/blog)

If there is someone in your organization who can concentrate on maturing the information security posture of your organization, a good follow-up to this document is the "CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs)." The steps listed in this Network & Systems Security Plan and in that document complement each other. See www.cisecurity.org/resources/white-papers/?o=controls

---

Part 2: Assess Any Special Risks and Requirements

Rationale: After implementing fundamental security controls (as addressed in Part 1 above), each business must further assess their situation to understand any special risks to their information. This "risk assessment" will make sure they account for potential negative impacts arising from the compromise of any particularly sensitive information. It will also account for any elevated threats (or threat actors) they may need to protect against.

Frequency: Comprehensive risk assessments of all information should be done regularly (probably annually), but at least any time major changes take place in your infrastructure, equipment, or operating systems. Furthermore, you should be doing regular risk assessments of all new hardware or software as it is introduced into your environment.

Start Here: As you read the steps here, just start with what you know. You may immediately recognize some of the most critical data you have, know where it is stored, and know who might want to access it. With that knowledge you can easily identify an area of greatest concern (or threat scenario). Write it down. Choose what security controls would help minimize the risk of that happening. The things you are most concerned about may indeed be the greatest risks to your organization. Start there and then reiterate through the process!

Outline of Major Steps (as detailed below):
1. Consider if you have any special adversaries
2. Identify all critical data assets
3. Identify where this critical information is stored and how it is transmitted
4. List out various Threat Scenarios for critical data assets
5. Calculate Risk to Prioritize Cybersecurity Efforts
6. Implement strong security controls for sensitive data based on risk (How to identify risk, How to prioritize risk, Select security controls to mitigate risks)

NOTE: If you or your people are working in a foreign country I strongly suggest you take the training found at www.expatdigital.com in order to live and operate securely and effectively. This site focuses on helping you understanding your risk situation and applying appropriate security controls.

Step 1: Consider if you have any special adversaries

Think about any adversaries you might have (beyond opportunistic criminal hackers) who would be actively seeking your information (or in whose hands your information would be especially damaging), such as antagonistic individuals/neighbors, militant groups, or hostile governments.

1) If you identify special adversaries, you need to further consider both the motivation and capabilities of these adversaries. If they have sophisticated hacking capabilities, and if they have strong motivation to obtain your information, then the likelihood of them accessing your data is greatly increased and you will need to apply more stringent security controls.
2) If you identify special adversaries, then you will need to implement further security controls and precautions (beyond those in Part 1 above).

Step 2: Identify all critical data assets

Take time to identify and list all the important information that you keep in your environment. Consider: personal contact information, email, company plans, financial information, emails, photos, etc.

1) The value of this information should be considered in terms of the following:
   a) Confidentiality - what damage would you suffer if the information was made known to unauthorized individuals (like special adversaries, or just posted on the Internet)?
   b) Availability - what if the data were lost (by hardware failure, encrypted by ransomware, accidentally deleted, etc.) and was not able to be restored/recovered? Even if the data could be recovered, would there be serious problems during the time it took to restore?
      i) Consider the impact if you lost connection to the Internet, due to a hardware outage or a Denial of Service attack? What data would inaccessible? How would that impact to your business?
   c) Integrity - what if someone erroneously changed the data, intentionally or unintentionally?
2) If applicable, interview all relevant individuals in your organization, to understand *what* information you have and *where* it is stored.
3) **NOTE:** Make sure to strongly protect this list of data assets as it can be a map to your most critical information if the list itself were to fall into the wrong hands. Consider if your situation is too risky to even keep a list of your valuable information written or listed anywhere. It should at least be encrypted and possibly only be a mental list.
4) **NOTE:** If you have information stored on your computer systems that may endanger others (like getting people killed or imprisoned), most likely it should NOT even be stored electronically!
   a) If you must store highly sensitive information, make sure it is strongly encrypted.
      i) Even if strongly encrypted, it is usually operational mistakes (people and process) that leak data, not the weakness of the encryption technology.
   b) AND Consider storing it in a way that would need two documents for it to be useful for an adversary or criminal hacker, such as listing pseudonyms in one file, but people's real names in another file, without an obvious connection between the two. These real names would be kept *very* secure (such as by using steganography along with encryption, and/or kept in different locations, or only kept on paper and hidden, etc.).

NOTE: If you don't have any special adversaries or any especially sensitive information, then the rest of this risk assessment may be considered optional for very small businesses (but still helpful for disaster recovery purposes).

Step 3: Identify where this critical information is stored and how it is transmitted

You need to identify where your information is stored and where/how it is transmitted. These storage locations or transmission channels represent points of vulnerability and must have extra security controls applied to ensure the security of the data.

Consider if information is stored and transmitted in the following technical "containers":

1) Stored on local file servers or file sharing areas (such as networked attached storage devices)?
2) Stored on local computers or laptops?
3) Where is this data backed up to? (The primary data may be secure, but then stolen from the backup location.)
4) Is it stored online or with a Cloud provider?
   a) Make sure to take note of all information stored in the Cloud, as this will have special security implications.
   b) Consider encrypting all files before they are put in the Cloud, or at least use a Cloud Service Provider that has very strong security controls, practices, and policies.
5) Is this data transmitted via email?
6) Is the information transferred to other locations via any other means?

7) Is the information stored on removable media, such as a USB flash drive or removable disk?

Step 4: List out various Threat Scenarios for critical data assets

Based on the information you have gathered so far, you should now be able to identify threat scenarios where certain threat actors could try to compromise your data where it is stored or transmitted. You should first just consider security situations that you are aware of and concerned about. These areas of concern are most likely some of the highest risk situations that should be addressed. Once you have listed these areas of concern as the first threat scenarios, you should go through a more rigorous or methodical process to identify other threat scenarios that give rise to cybersecurity risk.

Step 5: Calculate Risk to Prioritize Cybersecurity Efforts

Risk is measured by understanding the impact of a negative security incident (e.g. breach) combined with the likelihood of the event. i.e. RISK = IMPACT * LIKELIHOOD (Or in other terms, Risk = "consequences" * "probability".) The greatest risk exists for events that would cause the greatest negative impact (based on the value of the information) and have the greatest probability of happening (based on the motivation and capabilities of attackers). Understanding your greatest risks helps to prioritize your cybersecurity efforts, since the greatest risks should be addressed first.

A) How to Identify Risk:

Once you have:

- identified what information you have that is sensitive to you and your people,
- considered what would be the negative impact if this information was exposed to unauthorized individuals or if the data were lost or inadvertently changed,
- understand where this data is stored and how it is transferred,
- have an understanding of the capabilities and motivation of your adversaries,
- Then you can combine these elements to create a detailed list of threat scenarios

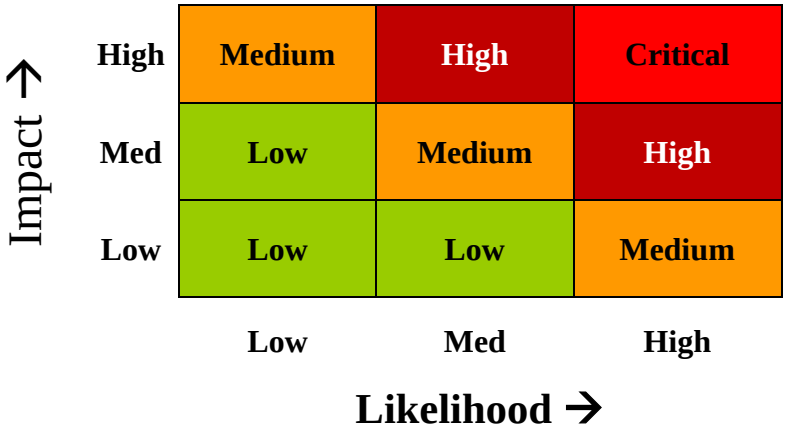
THEN you can better understand the risk to your organization and can decide to apply appropriately robust security controls to minimize the risk of this information being lost or compromised.

B) How to Prioritize Risk:

By mapping out which negative events (threat scenarios) are most likely to occur (based on adversary capabilities and motivation, vulnerability of systems, etc.) and which information is the most valuable (and thus would create a greater impact if compromised), then you can set priorities based on highest risks. As likelihood and potential impact both increase, the risk is greatest. In general, greatest risks should be addressed first.

Although there are sophisticated methods to accurately calculate and quantify risk, the best place for most people to start is by using a qualitative method to calculate risk. This can be done by assigning the values “High”, “Medium”, or “Low” to both Impact and Likelihood of each threat scenario you have identified, starting with your highlighted Areas of Concern. If the likelihood that a certain event could occur, and the negative impact of that event would be considered “high”, then the overall risk would be considered Critical. You should prioritize your cybersecurity efforts based on the highest risks identified.

See this **Risk Matrix** as a visual way to map out the highest risks to your organization:



For example, consider this threat scenario. You may have a list of contacts, which represents some critical and important part of your operations. You know that this information could greatly impact your business if this list got into the hands of your competitors. Thus the **Impact** of this data being breached is High. Furthermore, if you know that your competitors are highly motivated to obtain this list, and you believe they may have considerable computer skills (including time and money), then the **Likelihood** of this data being accessed is also High. Thus, this would be considered a **Critical** risk and should be addressed first. To protect this data and reduce this risk, you must consider where this information is stored and how it might be transmitted. These technical containers would be the place to implement strong security controls to protect this information.

Step 6: Implement strong security controls for sensitive data based on risk

One way you can decrease your risk is by applying further security controls to decrease the likelihood of a security incident/breach, and/or increase your ability to quickly detect a possible breach/incident. In general, the quicker you respond to a breach, the less the damage.

First, list any existing security controls in place for each threat scenario (or overall, per container, etc.) These security controls help to decrease the risk of a negative security incident. Then consider which areas (or data) still have unacceptable risk, where the likelihood and resulting impact of a negative security event still pose more risk than you as an organization are willing to accept. You then should consider what further security controls need to be applied to reduce the risk (by making it harder to exploit a vulnerability).

Please note that you can deal with risk in a number of ways. The most common way is to reduce risk by applying mitigating security controls. You can also avoid a risk by choosing to not keep certain kinds of data or not run certain kinds of systems. (For instance, there is no reason whatsoever to store full credit card numbers. Further, there may be sensitive data about your employees that should not be kept in electronic format based on the risk of harm.) Some risk can be transferred to others by purchasing insurance or by allowing a more capable organization store and secure your data.

Part 3 of this paper will give ideas for security controls to address these risks. (Don't hesitate to engage with third-party cybersecurity experts to help reduce these risks and move forward in your security journey.)

Part 3: Further Risk Reduction & Mature Security Posture

Rationale: As you follow a plan to mature your cybersecurity capabilities, (such as outlined above, and in the CIS Top Twenty Security Controls or the NIST Cybersecurity Framework), you will start to reduce your overall risk and close the inroads of compromise for your most critical data assets. You should choose one of these frameworks and start walking this journey of cybersecurity maturity.

However, the risks you have identified through the risk assessment process outlined above will help you prioritize your cybersecurity efforts based on your greatest outstanding risks. Don't wait for your security posture to mature before addressing these most critical items.

In step 3 of the risk assessment process above (in Part 2), you were asked to identify where your critical data was stored, processed, and transferred. These technical "containers" are points at which your data can be compromised. These containers often contain vulnerabilities that can be exploited by threat actors. The process of reducing risk will include removing vulnerabilities (such as by applying security patches, reducing attack surface, limiting connectivity, etc.) and by applying further security controls (such as encryption, multi-factor/two-factor authentication [MFA/2FA], network segmentation, etc.).

Further Important Steps for Information Security

Make sure that you have thoroughly implemented all the 12 security controls listed in Part 1. You should go back and review them to make sure they are applied to any area of unacceptable risk.
After you have implemented all security controls listed in Part 1, and done at least an overview of Risk Assessment listed in Part 2, then you should do the following:

Step 1: If you have not yet had an outside vendor help you perform a **full penetration test** on your network, then you need to do that now. Also consider other types of assessments an external vendor may offer to perform, such as a security controls assessment, vulnerability assessment, etc. This will provide you will a more realistic view as to the effectiveness of your security controls, and will give you a list of prioritized items that you need to address to further secure your network. Your eyes will be opened as to how secure you really are!

Step 2: As detailed in Part 1, security incidents happen! If you have not yet done so, then now is the time to create your security **Incident Response Plan**!

Step 3: Build **breach detection capabilities**. A mature organization should monitor their network and computers to be able to detect potential data breaches. The average cost of a data breach in the U.S. is almost 4 million dollars. The longer it takes to detect the breach, the more damage can be done and the expensive it is to contain and recover from the breach. Yet, the average time it takes to detect that a breach has occurred is over 200 days! (See www.ibm.com/security/data-breach)

Start looking at system logs or use a system that will alert you based on certain log events. Consider implementing Central Log Management. When you are ready to move on from there, consider implementing a SIEM, either in-house or in conjunction with a management partner.

Some excellent tools that can be used to automate your breach detection capabilities are: CrowdStrike, Exabeam, or Palo Alto Networks' Cortex XDR. However, these tools are not cheap.

Step 4: Related to your ability to respond to security incidents, every business should build robust **Disaster Recovery** and **Business Continuity** plans, based on your business needs. Major incidents of any

kind (such as a fire, a major ransomware event, loss of electrical power, flooding, etc.) can affect a business' ability to operate due to loss of data or the ability for IT systems to function. Be prepared to recover data if your whole data center burns down. Be prepared to continue critical operations if a storm knocks out your power for a week.

A disaster recovery plan will at minimum include a well planned out and tested backup system, to recover all important data your business needs to operate.

Other items to Consider on your Journey to Information Security Maturity

After completing the items above, consider the following lists of security controls and programs to help further reduce risk. If you are unsure about these items, please contact a cybersecurity expert.

Do the "Simple" Things Well:
Backups
System Hardening
Vulnerability Management
Internal Network Segmentation
Central Log Management
Application Whitelisting
Identity and Access Management
DNS Filtering/Monitoring

Dealing with Passwords:
Create password policies: make sure everyone understands their importance and follows them
Multi-Factor Authentication (MFA/2FA) for all Cloud applications and Internet accessible applications
Password Manager Program used in all reasonable situations
Privileged Account Management solution
Microsoft LAPS (Local Administrative Password Solution)

Vulnerability Management Program
Removing all out-of-support or highly vulnerable software (such as Adobe Flash, Java, etc.)
Upgrading all out-of-support operating systems
Patching operating systems on a regular and timely basis
Patching all application programs
Patching all hardware firmware, especially routers, switches, firewalls, etc.
Scanning your environment for known vulnerabilities
Implementing Intrusion Prevention System (IPS) (network or host-based) to perform "virtual patching" capabilities

Miscellaneous Controls:
Encryption of data at rest or in transit. Encrypt disks, USB drives, backups, databases, etc. Make sure all data in transit is encrypted, such as email, internet traffic (VPN if appropriate), file transfers, etc.
Reduce attack surface by turning off all unnecessary services and software on systems
Deploy a hardware or software Intrusion Detection/Prevention Systems (IDS/IPS)

Limit damage of a breach by segmenting your network, starting in your data center (or with your servers). For instance, servers that provide a certain application most likely have no reason to talk to other servers. Database servers, that may hold some of your most sensitive data, should only be talking SQL to certain other application servers.

Develop the capabilities you already use and own, such as maturing practices and configuration used by your Firewall - talk to your vendors!
Deploy robust Spam and Malware filter for email. E.g. ProofPoint, MimeCast, etc.

Further Information Security Principles
Consider the following security principles, which may take further research and education, but should be incorporated into any mature information security program:
Defense in Depth
Least Privilege
Cover, Conceal, Compartmentalize
Zero-Trust Networking

Resources for Further Research

Overall Cybersecurity Guidelines:

1) CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs): www.cisecurity.org/resources/white-papers/?o=controls
   (Main CIS Security Controls page: www.cisecurity.org/controls/)
2) ACSC Small Business Cyber Security Guide: www.cyber.gov.au/publications/small-business-cyber-security-guide
3) Cyber Safe Guide for Small and Medium Businesses (from Canadian Government): www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/ (Includes Password Policy Recommendations.)
4) NIST Cybersecurity Framework: www.nist.gov/cyberframework

Passwords:

1) Four *Random* Words as a Great Password: www.explainxkcd.com/wiki/index.php/936:_Password_Strength – Notice the strength is based on "random" words, not just your favorite words.
2) Creating Good and Complex Passwords: www.paessler.com/blog/how-to-secure-company-it-with-simple-password-rules See the section on "The 'Secure Password' Method" – but, don't be so predictable as: Amazon password starting with AM-, Twitter with TW-, etc. This can get you into trouble if a criminal hacker analyses your passwords.
3) Some good advice from a talented and respected security expert krebsonsecurity.com/password-dos-and-donts - The only thing I would change/advise is that you should NOT merely just use a passphrase like the opening line to a book or joke; password crackers are getting more sophisticated and know this technique. Sprinkle some numbers or characters in there also.
4) Info on Passphrases: en.wikipedia.org/wiki/Passphrase

Risk Assessments:

1) The information security risk assessment: identifying threats: www.vigilantsoftware.co.uk/blog/the-information-security-risk-assessment-identifying-threats/
2) Software to Help do Risk Assessment: www.vigilantsoftware.co.uk/product/vsrisk-standalone
3) Creating a Threat Profile for Your Organization (Note: But don't get bogged down in details) www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Incident Response Planning:

1) Cybersecurity Incident Response Planning: digitalguardian.com/blog/incident-response-plan
2) Responding to IT Security Incidents: technet.microsoft.com/en-us/library/cc700825.aspx
3) 10 steps for a successful incident response plan: www.csoonline.com/article/3203705/security/10-steps-for-a-successful-incident-response-plan.html

End User Security Awareness Training:

1) SANS Ouch Newsletter: www.sans.org/security-awareness-training/ouch-newsletter
2) Federal Trade Commission training and advice for small businesses: www.ftc.gov/tips-advice/business-center/guidance/scams-your-small-business-guide-business

Miscellaneous Topics:

1) Security advice for individuals and small businesses www.ComputerSecurityNW.com
   a) Secure routers for small businesses (bottom of front page)
   b) Smartphone security: www.computersecuritynw.com/essential-smartphone-security
   c) Security Blog Posts: www.computersecuritynw.com/blog
2) Running Windows in Non-Administrative mode for security: See: www.ghacks.net/2017/02/23/non-admin-accounts-mitigate-94-of-critical-windows-vulnerabilities/
3) Network Demilitarized Zone (DMZ). See: danielmiessler.com/study/dmz/ or www.lifewire.com/demilitarized-zone-computer-networking-816407 or fedtechmagazine.com/article/2012/05/four-tips-securing-network-dmz-fed