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