Quick Solution Assessment:

Cybersecurity Readiness Report

Prepared For:

USA SAMPLE CORP

Prepared by:

John Q. Sample, CISSP, CISM, CRISC, CCSK, COBIT, GSEC GOLD

Crown Business Solutions: Cybersecurity Specialist
A Division of
The Crown Group of Companies

Security Assessment: Introduction

Prepared for:	Sample
Using data provided by:	
Assessment date:	

We **thank you for taking the time** to discuss your current security situation. We've carefully considered your answers to this questionnaire and compiled the following recommendations to consider.

Our Methodology

We work with the world's largest Technology Solutions Brokerage that specializes in cybersecurity. This report is generated using data gathered from their staff of trained security professionals and engineers as well as other brokers, like us, who have experience working with the top security providers in our industry. Our advice is based on data from these interactions, not marketing funds, pay-to-play advertising budgets, or any other factor that would bias us towards one solution versus another.

Using this proprietary data, we have generated this report to help you
1) protect your **network**,
2) protect your **people**,
3) protect your **data**, and
4) help you formulate winning **cybersecurity policies** and procedures.

The endgame here is to help your company get the **most bang for your security buck**, which is why we've prioritized our recommendations in order of importance to both your security posture as well as most compliance audits, not to mention helping you improve your odds of getting approved for a cybersecurity insurance policy. We recommend you begin at the beginning and work your way to the end, and in-so-doing you will inherently address your most pressing needs first.

We also recognize that cybersecurity is not a one-size-fits all affair, which is why we follow up each of our findings with **two of our very best supplier suggestions** so that you can vet both options as you consider the future direction of your security strategy. If you would like to engage with our recommended providers, we are more than happy to connect you with our contacts, who stand at the ready to assist you. Please reach out to me as your first point of contact so that I may send them over the results of this assessment, so we don't have to begin at ground zero, saving you additional time and effort.

Now, let's begin that journey together.

What's at Stake?

Some sobering statistics.

In today's connected world, EVERYONE is a target. Bad actors leverage software, tools, AI technology, and even social engineering to achieve their goal of extorting financial gains from their victims. The main challenge is that they evolve their techniques and technology so fast that it becomes a full-time effort to defend against their tactics. This velocity of change requires companies like yours to turn to highly focused experts whose only job is to find these threats, create countermeasures, and stay vigilant.

Here are some statistics that speak to how your peers - other companies with more than 100 employees but less than 1,000 from the United States - are faring in this battle:

➔ 2021 saw the highest **average cost of a data breach** in 17 years, with the cost rising from **$3.86 million (USD)** to **$4.24 million (USD)** on an annual basis.*

➔ The COVID-19-powered shift to remote work had a direct impact on the costs of data breaches. The average cost of a data breach was **$1.07 million (USD)** higher, **where remote work was a factor** in causing the breach.*

➔ A total of 82% of organizations have admitted to increasing their cybersecurity budgets over the past year, with these funds accounting for up to 15% of total IT spending,**

➔ There has been a significant increase in the overall costs of remedying a **ransomware attack**. While in 2020 the cost was **$761,106 (USD)**, in 2021, the overall cost of remediating a ransomware attack skyrocketed to **$1.85 million (USD**), an increase of 143%.***

➔ 52% of all successful attacks are a result of **human error** or **process failure**

➔ The average breach goes **undetected** for over **200 days.**

➔ **1.6 million** businesses were breached, and **1,500** impacted by Ransomware attacks in 2021

(IBM Cost of a Data Breach Report 2021)* *(Accenture's State of cybersecurity resilience 2021 report)*
****(ENISA Threat Landscape 2021)*

Simply put, most companies that suffer a breach, especially a ransomware attack, don't recover. And the ones that do find themselves frequently re-targeted because they become known as an entity willing and able to pay the ransom. A solid multi-layer plan revolves

around **people**, **processes**, and **technology** that dramatically impacts a bad actor's ability to access your sensitive data and quickly detects when a breach has occurred. We're here to help you plan, execute, and win this battle.

Here is what we recommend, again, in order of importance.

Security Assessment: Findings & Suggestions

Do you have a SIEM that is monitored 24x7 by a SOC?	Yes

FINDING: Congratulations! You responded that you do have a SIEM that is actively monitored by a SOC. As you know, this is the most important first line of defense. **We commend you** on your choice to implement both SOC and SIEM services. But have you heard about Next-Gen SIEM tools?

Traditional vs. Next-Gen SOC Technology: Advanced SOCs leverage next generation tools, specifically **next-generation SIEMs**, which provide **machine learning** and advanced behavioral analytics, threat hunting capabilities, and built-in automated incident response. Modern security operations center technology allows the SOC team to find and deal with threats quickly and efficiently.

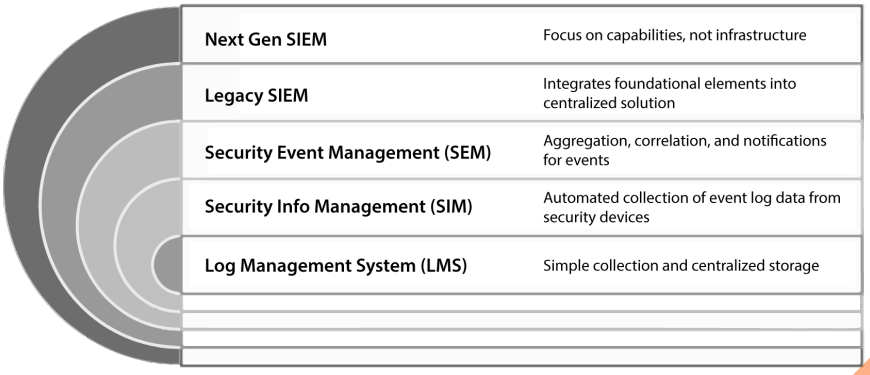
Traditional Tools

- **Security Information and Event Management (SIEM)**
- Governance, risk and compliance (GRC) systems
- Vulnerability scanners and penetration testing tools
- Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and wireless intrusion prevention
- Firewalls, Next-Generation Firewalls (NGFW) which can function as an IPS, and Web Application Firewalls (WAF)
- Log management systems (commonly as part of the SIEM)
- Cyber threat intelligence feeds and databases

Next-Gen Tools

- **Next-generation SIEMs** which are built on big data platform and includes machine learning and advanced behavioral analytics, threat hunting, built-in incident response and SOC automation
- Network Traffic Analysis (NTA) and Application Performance Monitoring (APM) tools
- Endpoint Detection and Response (EDR), which helps detect and mitigate suspicious activities on hosts and user devices
- User and Entity Behavior Analytics (UEBA), which uses machine learning to identify suspicious behavioral patterns

NEXT-GEN SIEM BUILDING BLOCKS



SECURITY OPERATIONS CENTER BEST PRACTICES The following best practices can help you operate your SOC and defend against threats more effectively in a modern threat environment.

Detect threats through all stages of an attack

To cope with the increasing number and complexity of cyber threats, organizations have implemented security solutions that deal with specific vulnerabilities or attack vectors. Attackers in response have created sophisticated responses using multiple techniques. **Point solutions working by themselves cannot identify the relationship between a series of events.** To stop an attacker from penetrating security, security operations must:

- Deploy prevention and detection approaches throughout the entire attack chain, the IT environment, and every attack vector.
- Design the technologies to function together and communicate information.

Investigate all alerts to ensure nothing is overlooked

A copious number of alerts was an early driver for SIEM. SIEM systems created correlation rules to group similar events into alerts; this helped teams deal with the tens of thousands of events isolated daily. Today, organizations state that there are too many alerts to investigate even with correlation, which leaves the organization open to risk.

You need to develop solutions that group alerts and automatically investigate and validate them. They should try to limit the number of events that human analysts must review.

Gather forensic evidence for investigation and remediation

To investigate alerts, security teams require in-depth endpoint and network

activity data. This is made available by forensics solutions. However, forensics tools, specifically on the network, are time-consuming and complex to use.

You should find solutions for forensics that are simple to use and automated. It is important to adopt solutions that proactively combine forensic evidence into investigation procedures. An organization should also convey the results in relation to the alert or lead the data validates.

Leverage security automation

To more effectively analyze larger numbers of security events, identify incidents and mitigate against them, organizations can leverage security automation technologies that complement the work of skilled security analysts.

SOC capabilities depend on technological capabilities — technology can simplify and speed up security processes by collecting and aggregating data, implementing protections against security threats, and automatically responding when breaches occur. When security teams have access to data sources and tools that minimize false positives, analysts can maximize their time **investigating actual incidents**.

Use threat intelligence

When combined with threat intelligence data generated within an organization, external security data provides the SOC team with important insights into vulnerabilities and threats. Intelligence from external sources covers a wide range of data, including vulnerability alerts, incident reports, signature updates, news feeds, and threat briefs. The SOC can leverage security monitoring tools that offer integrated threat intelligence.

Combine data across silos

The SOC team needs to combine data from all security silos to effectively detect and respond to threats. They should receive and consolidate data from:

- **The network** – traffic analysis, URLs, hashes, connection details
- **Endpoints** – information revealed by vulnerability scanners, security intelligence feeds, intrusion prevention (IPS) and detection (IDS) systems, and endpoint protection systems
- **Operating systems** – reviewing logs with security significance and monitoring for anomalous processes
- **Firewalls** – monitoring logs and events on external-facing firewalls
- **Cloud systems** – today the cloud is an inseparable part of the corporate network, and cloud resources must be monitored for security misconfigurations and anomalous activity

OUR RECOMMENDATION: If you are interested in **Next-Gen SIEM tools** to beef up your SOC, are experiencing **Alert Fatigue**, are **less-than-happy** with your current service, or just want to see a **competitive quote** the next time your SOC contract comes up for renewal, we suggest you give the following providers a chance to impress you. After years of performance, each one has earned our recommendation, and you can't go wrong by just having a conversation (we can set this up for you). You can split this up into two distinct projects or tackle it all at once. Here are our recommendations for both the "a la carte" approach and the "all-in-one" approach.

Do you have a CISO or someone committed full-time to your company's security?	**No**

FINDING: You responded that you **do not have anyone** within your company who is *solely* accountable for your company's security. Behind only SIEM + SOC, this is the most important step you can take in building up your security posture. This should be addressed immediately. Most of the companies we deal with find great value in a virtual Chief Information Security Officer (**vCISO**).

TOP 6 BENEFITS OF A vCISO: Hiring a virtual Chief Information Security Officer, or vCISO, offers your organization an **affordable** and scalable **approach** to executive leadership and security expertise while keeping expenses low. Some key benefits of this approach include:

Clear Vision - A virtual chief information security officer offers a clear vision of where your organization's IT security program stands, where it can go, and how to get it there. They **strategize**, **plan** and **execute** a cybersecurity strategy to align with your business strategy.

Addresses Attrition - With the issue of supply and demand, there is a deficit of qualified CISOs because many large, heavily regulated companies are mandated to have a CISO. As a result, Mid-size and SMBs who don't fall under these mandates often struggle to find qualified full-time CISOs. Fortunately, a vCISO offers a creative solution.

Affordable Framework Expert - A virtual CISO costs much less than an in-house, **full-time CISO**. Based on the normal contract rate for virtual CISOs, an organization can save an average of 60% from a typical industry salary. A virtual CISO also provides security and governance on a budget.

Allows Your Internal IT Team to Maintain Focus - vCISOs can focus on the high-level cybersecurity needs of the organization: security policies, guidelines, compliance standards (ex. HIPAA, PCI, GLBA, SOX, FERPA, SOC Reports). This allows the current internal IT team to remain focused on their day-to-day activities and refrain from getting side-tracked and maintain an appropriate workload so they are not 'spread too thin'.

Immediately Up-to-Speed - A qualified CISO will quickly adapt to the hiring organization's environment. This provides immediate value, reduces time waste, and resources. A virtual CISO is typically able to deliver more quickly and efficiently giving the organization more for their money from the start.

Succession Ease - Contracting a virtual CISO allows for critical compliance, governance, and risk management functions to continue if the company were to lose a key staff member. This can reduce stress regulatory and client concerns and allow organizations to focus on finding the right next step instead of scrambling to 'fill the gap'.

OUR RECOMMENDATION: Consider entering into a consulting agreement to obtain a **vCISO (virtual Chief Information Security Officer),** which offers superior value to hiring just one person (see above). A vCISO comes with well-established relationships with other security experts, industry leaders, and vendors which helps with their performance. For less than the cost of one full-time employee, you can have a team of experts that can help you define your strategy, implement best practices, design a comprehensive security plan, and sign off on the necessary legal documents required for certain compliance audits. The best posture starts with a plan and someone (or a team) who can be **held accountable for executing** that plan.

Do you have formal Disaster Recovery, and Business Continuity Plans that are tested annually?	**No**

FINDING: Without a formal DR and Business Continuity Plan in place, your company is sailing in the digital ocean without lifeboats. It's important to have a plan in place in case of a successful ransomware attack, or it could be a situation from which your company can't recover.

ANATOMY OF A GREAT DR AND BUSINESS CONTINUITY PLAN: Insulating the business from the impact of unplanned outages and extreme events is a complex undertaking in today's highly interconnected digital corporate ecosystems. Third parties may deliver business-critical services, which in turn rely on other parties to stay operational. This means the exercise of identifying vulnerabilities that could impact the organization extends well beyond the business's four walls. Here are seven tips for creating a solid DR/BC Plan

Make Business Continuity Strategic Board Business. Business resilience and the ability to absorb the impact of disruption rapidly should be subject to board oversight and evaluation.

Place Technology Front and Center as Both a Risk and Recovery Resource. IT teams should be able to activate backup and disaster recovery protocols remotely. Data center **location** is also an important consideration. If a backup data center is located too close to the primary data center, any localized event such as an extreme storm could impact both sites, preventing failover to the backup site.

Prioritize Mobility and Explore Process Alternatives. Switch to **digital signatures** for authorizing board resolutions and the use of secure board communication channels that operate independently of the corporate network. Finding and documenting alternatives to standard communications channels should be considered part of planning to preserve business continuity.

Monitor Data Risk Across the Digital Environment. Data is the lifeblood of modern commerce and is both an organization's biggest asset and significant risk. For organizations to continue to function, two steps are essential. Firstly, corporate data must continue to flow. Secondly, and even more crucially, this data must be protected and managed in a way that is compliant with data protection regulations.

Create Communications Plans for Key Stakeholders. The board, senior management team, employees, customers, and key third-party vendors may need individual framework communication plans.

Map Out Important Personnel Relationships and Third-Party Contacts. When the organization is under pressure, personal relationships come into their own. People who know one another work improved speed and trust to achieve the necessary ends. All the key relationships and responsibilities for dealing with incidents should be documented and maintained, so current information can be accessed in seconds should it be necessary. Redundancy must also be built-in.

Don't Just Write the Plan, Test the Plan. A business continuity plan must not become shelf-ware, gathering dust during times of stability. It is a living, evolving program that may need to be activated at any point. It must be tested, evaluated, and refined both from a technology perspective and in human terms.

SUGGESTION: Even with these best practices in your toolkit, it may be a good idea to engage with a third-party consultant who specializes in authoring modern and up-to-date Disaster Recovery and Business Continuity plans. These two companies, listed below, are ones that we have found provide the best advice for companies of your size and vertical.

Do you conduct regular security awareness training for your employees?	**Yes**
How frequently do your employees need to complete new training?	**Monthly**

FINDING: Congratulations! You responded that you are currently conducting regular security awareness training for your employees. **We commend you** on taking the important step to keep your team educated so they can understand the evolving threat that will continue to **target them** to gain access to your most sensitive data. With human error being the root cause of over 38% of all breaches, more than network intrusion, you have certainly made a wise decision by engaging a security awareness provider. It is recommended that your employees participate in Security Awareness Training a minimum of once per year.

SUGGESTION:

With a **monthly training cadence**, you're currently **well above the minimum standards** of most industries. The questions you should be asking are "Are the training videos professionally produced and of high quality? Are they interesting? Are they engaging? Are they hitting on the most up-to-date and most relevant threats?" If you'd like to evaluate some high-quality alternatives, we recommend these two firms:

Do you apply security patches to all computing devices within 30 days of release?	**No**

FINDING: One of the best ways to protect your network is to leverage the patches released, for free, by the authors of all applications, operating systems, and firmware (for hardware) that you use. When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation. You need to set up a **process** ASAP to ensure that these patches are applied soon after release to keep your network protected from known vulnerabilities.

SUGGESTION: Patch management is a critical component of vulnerability management, but it's just one piece of the puzzle. To successfully embed **patch management** into your vulnerability management program, the following steps should be implemented:

Establish asset management. An asset management solution helps you gain a full understanding of the assets you have and the vulnerabilities associated with each asset.

Prioritize vulnerabilities. With limited time and resources and an ever-changing threat landscape, it's unrealistic to think that you can fix every vulnerability as soon as it appears.

Remediate vulnerabilities to reduce risk. Identifying and prioritizing vulnerabilities is important, but you're not actually reducing risk unless you're remediating the issues.

Measure the success of your vulnerability management program. To determine if you're achieving a good ROI—and justify the purchase to senior leadership—you'll have to determine how to measure success.

Develop partnerships and support. When something goes wrong, you want to know you have a team of people you can rely on to help troubleshoot.

Here are a few firms that we know do an outstanding job of helping companies like yours set up and execute patch management programs to beef up your vulnerability management approach.

Do you utilize advanced endpoint detection and response (EDR) products on all endpoints and servers?	**Yes**
Which EDR provider(s) are you using?	**SentinelOne (Singularity Platform)**

FINDING: Great news! You have an EDR solution on all endpoints and servers. We congratulate you and commend you for recognizing this need and prioritizing it within your company. The questions you need to be asking yourself now are:

1. Is the solution **still performing** at a high level?
2. Is your team of well-trained security professionals and processes keeping up with **evolving threats**?
3. Is your team experiencing increasing costs and/or **alert fatigue**?
4. Could a new EDR solution **replace your existing investments** in:

- **Antivirus** (See Question 8 for more on EDR as an AV replacement)
- **Data loss prevention** (DLP)
- **File integrity monitoring** (FIM)
- **Host-based IDS/IPS**
- **Network threat/anomaly detection**
- **User Behavior Analytics** (UBA)

SUGGESTION: We suggest you focus on **optimization**, **simplification**, and **cost-savings**. There are so many new EDR solutions on the market, solutions that integrate better into your existing tools, solutions that require less human involvement, and solutions that can replace/displace other investments. We work with two providers who focus exclusively on supporting organizations like yours, who may be struggling to manage the complexities of threat detection and responding to those alarms. These are the two providers we recommend you engage:

Do you perform full and incremental backups of business data regularly?	**Yes**
How long before your backups are overwritten or deleted?	**Not Sure**
Do you test your backups for restorability?	**Not Sure**
Do you ensure your backups are stored physically offsite?	**Yes**
Do you ensure your backups are stored offline?	**No**

FINDING: Great news! You have a backup solution in place. We congratulate you and commend you for recognizing this need and prioritizing it within your company. The questions you need to be asking yourself now are:

1. Are you optimizing your backup **intervals** with the right backup **types**? **(Full vs. Incremental vs. Differential Backup)**
2. Do you know what your **mean-time-to-detection** is of a breach and ensuring you **keep a copy of your backups** at *least* that long?
3. Have you **tested** your current backups to see, in the real world, if you could use them to initiate a full restore?

4. **Where are you storing** your data (offsite vs. on-site)?
5. Do you have a copy of your data that **can't be erased by hackers**?

With so many ways to do this, we've compiled a list of industry-wide best practices to share with you to ensure your data backup strategy is on point.

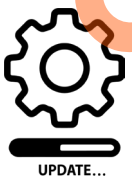
FOOD FOR THOUGHT: The question about backups isn't really, "Which type of backup?" For most companies, it is, "**Which combination of backups (Full vs. Incremental vs. Differential Backup) is right for my needs**?" Many organizations ultimately choose to develop a combined approach to backups, which could resemble one of the following options:

- Full **daily** backup.
- Full **weekly backup** and a **differential daily backup**.
- Full **weekly backup** and an **incremental daily backup**.

While each approach carries its own benefits and risks, your organization needs to consider your need for performance, data protection, total volume of data assets, and the cost of recovery. The following five factors can be used in making a decision about which backup schedule is right for you.

How Active Are Your Read/Write Activities? If you are primarily using your data assets for reference without updating them, known as "read activities," you may not need full backups on a very consistent basis.

What Is Your Tolerance for Recovery Time? With a full backup on a daily basis, all of your assets are in a single set. While a full recovery isn't quite immediate, it can occur very quickly and doesn't require the combination of multiple types of backup files. If your tolerance to any downtime is **zero**, full backups represent the least risk.



How Many of Your Data Assets Are Actively Being Updated? For most organizations, this represents a tiny percentage. A large volume of your data assets may be emails and files from previous years that you are required to retain for regulatory reasons. Unless all of your data assets, applications, and databases are "living," running full backups on a very consistent basis may take more storage space than necessary.

How Much Storage Space Can You Dedicate? Running a full backup on a daily basis requires more than twice the storage space of differential or incremental in many cases. Assuming your business is actively using 25% of your data assets on a daily basis, running a full daily backup each weekday could require five times more storage space than a weekly full

backup and a daily incremental or differential backup. At most organizations, the difference is significant.

How Much Data Do You Have? For some organizations, running a full backup daily is actually the most cost-effective approach. These are typically organizations with minimal data assets, which can be a product of their industry, products, services, or a lack of multimedia data assets. If cost and storage space factors are not prohibitive, a full backup represents the easiest and fastest recovery.

The next question that needs to be addressed is **Data Backup Archiving**, or **how long you keep a copy of it before either deleting it or overwriting it** with a more up-to-date version of your data set. The answer to this question depends on important considerations such as:

The importance of the data (photographs, documents, emails, etc. are more important than application code than can be re-downloaded)

The rules / compliance guidelines under which your company is subject (the length of time you need to archive data may already be made for you)

The capability of your EDR (Endpoint Detection & Response) and SIEM to **detect a breach**. You should always store your data for longer than it takes to for a breach to be discovered, lest your backups become infected as well.

To be more specific, here is a general guide on how long you should keep backups:

- Companies with over 101 and less than 1,000 employees, like yours, are typically best served with a **weekly full backup and daily differential backups**. This balances capability, cost, and time-to-recover.

- A general best practice is to keep backups for at least **three months**. You may need to hold on to them **longer** if 1) your industry requires it and 2) if you are questioning your ability to detect a problem.

- During the past year, the **average** breach took **200** days (**over six months**) to detect, so it's essential to **find out how long** your data is being archived before it's discarded or overwritten.

- Special-purpose backups may have shorter or longer retention plans.

Even with these storage plans in place, many companies lose sight of the overall goal: **recoverability**. We don't want you to repeat the mistakes of others! So while you stated that you don't currently **test your backups**, we strongly suggest you make this a major priority in our ongoing disaster recovery strategy.

An important dimension to data backup involves **WHERE** your backup data is stored. Where you store your data matters because you don't want to have your most precious asset stored in a location without significant physical security in place. Locations like public cloud (which are typically in massive, super-secure data centers like Equinix) and private cloud providers can be considered ideal locations. That's why we recommend you **continue to make offsite storage** of your backups part of your overall survivability planning.

The last consideration to data backup involves storing a copy **OFFLINE**. Keeping a copy of your data offline is a great insurance policy. Usually, when attackers breach your network, their first target is to locate and delete your backups. If you keep a copy of them offline, you will mitigate that major risk. So, while you stated that you don't currently **keep a copy of your backups offline**, we strongly suggest you make this a major priority in our ongoing disaster recovery strategy.

If you have ANY questions about these many recommendations, or to get a quote on Data Backup-as-a-Service, we recommend you consult with these two amazing suppliers that have a track record of excellence:

Do you have an Incident Response (IR) Plan that is reviewed and tested annually?	**No**

FINDING: An IR plan that is reviewed and tested by your Security Leader should be a very high priority for your organization. A good IR plan is a set of **written instructions** that outline your organization's response to data breaches, data leaks, cyber-attacks, and security incidents and contains specific directions for specific attack scenarios, avoiding further damages, reducing recovery time, and mitigating cybersecurity risk.

WHAT SHOULD YOUR IR PLAN LOOK LIKE? Incident response strategies and plans layout what defines a breach, the roles and responsibilities of the security team, tools for managing a breach, steps that will need to be taken to address a security incident, how the

incident will be investigated and communicated, and the notification requirements following a data breach.

Here are some best practices around the different stakeholders that make up a sound Incident Response Plan:

Incident Response Plan: Best Practices

Form a **Computer Security Incident Response Team** (CSIRT) who is responsible for analyzing, categorizing, and responding to security incidents. Incident response teams can include:

- **Incident response manager:** oversees and prioritizes actions during **detection**, **containment,** and **recovery** of an incident. They may also be required to convey high-severity incidents to the rest of the organization, customers, law enforcement, regulations, and the public where applicable.

- **Security analysts:** support and work directly with affected resources, as well as implementing and maintaining technical and operational controls.

- **Threat researchers:** provide threat intelligence and context around security incidents. Organizations will often outsource this function if the expertise does not exist in-house. If this is your organization, look for tools or services that can automatically monitor for leak credentials, data leaks, and third-party and fourth-party vendor security posture.

Senior leadership support is essential to gather resources, funding, staff, and time from different teams. This may be the Chief Information Security Officer (CISO) or Chief Information Officer (CIO) at a large organization or even the CEO or a board member at smaller organizations.

Legal counsel can help your organization understand which data breaches must be reported to regulators and customers, as well as advice around liability for third-party vendor data breaches.

Where an incident is from an insider threat, **Human Resources** can assist with removal of staff and access credentials.

Public relations are essential to ensure an accurate, consistent and truthful message is communicated to the regulators, media, customers, shareholders and other stakeholders.

SUGGESTION: Putting a great Incident Response Plan in place can be challenging, but we've got some **fantastic resources** that you can rely on to help you put this plan in place and more importantly, to test the plan. If your company ever does face a major (or minor) security incident, everyone will know exactly what to do, who to call, and how to handle the situation in a way that minimizes the damage to your firm. If you need help with your Plan, or you'd like to hire a team of people to serve as your IR "SWAT" team (and Threat Research Team), we've vetted some great options for you.

Do you require MFA for remote access to the network?	**Yes**
Do you require MFA to protect Privileged User accounts?	**Yes**
Do you require MFA Authentication for all Cloud resources?	**Yes**
Do you require MFA for all Remote Desktop and Virtual Desktop instances?	**No**

FINDING: Cyber criminals can steal or guess your passwords. Multi-Factor Authentication (MFA) adds a layer of protection to the sign-in process, such as scanning a fingerprint or entering a code received by phone. MFA should be used on all critical infrastructure and to access all sensitive data.

MFA BEST PRACTICES: By verifying an employee's identity before they access your programs, the likelihood of a successful cybersecurity breach is greatly reduced. Implementing MFA for your company is an important step towards continuous data protection, adhering to compliance requirements, and a commitment to improving your cybersecurity infrastructure. Here we have compiled some best-practices for each area of critical infrastructure:

MFA Best Practices

Remote Access to the Network - once inside your physical network, hackers can look for key infrastructure, like data backups, and attack them. Without MFA, the only thing an attacker would need to access your network would be a username and password of just one of your trusted users. We commend and congratulate you on putting MFA in place for all remote access to your network.

Privileged Users with Access to the Network - as we learned from the Solarwinds attack, the most valuable target of hackers is the person (or systems) that have privileged (or Admin) access to the network. Using that access they can lock out other authorized users, permanently delete sensitive data, and cause irreparable harm to your organization. We commend and congratulate you on putting MFA in place for all privileged users of your network.

Access to Cloud Resources - Cloud resources are now just as important to organizations as the local network, if not more so as companies continue to shift their workloads and data storage to the cloud. It's paramount that anyone who is accessing those critical resources be MFA-validated. We commend and congratulate you on putting MFA in place for all users with access to Cloud resources.

Access to Remote Desktops - A remote desktop represents a direct-access path into your network. Once logged in, users can access software, files, data, and anything else that the remote user profile has been authorized to access. It's critical that your employees and contractors (if you have any) be required to present MFA credentials to access their remote desktop instances. We **strongly recommend** instituting an MFA solution for all employees with access to Cloud resources ASAP. You can enable MFA for each of your authorized users **inside the control panel** of your SaaS or PaaS provider.

SUGGESTION: If you would like to open up a dialogue around MFA, talk strategy, vet potential MFA software providers, or are looking for general assistance putting an MFA solution in place, we've partnered with two of the best MFA consultants in the business:

Do you conduct regular phishing campaigns?	**Yes**
How frequently do you conduct phishing campaigns?	**Monthly**

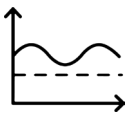
FINDING: You are currently engaged with a vendor to conduct phishing simulations on your employees. It is recommended that phishing campaigns be conducted so that each employee receives at least one test message per quarter. We recommend conducting phishing simulation tests, not more than once a month but at least once every three months (quarterly). In addition to that, we've compiled a list of other best practices so you can see how your current program measures up.

PHISHING CAMPAIGN BEST PRACTICES: Security awareness training should include an ongoing phishing program where you send fake phishing emails to your employees. This helps them develop an awareness of emerging threats, allows employers to see how effective training has been so far, and identifies people who might need more help. The hope is that it will work like a vaccine. Introducing fake phishing emails to trigger a response can train people to recognize and foil future attacks. For this kind of training to be effective, you need a clear plan of attack. Below are five suggested steps you take when building a phishing plan for your company:

Phishing Campaign Best Practices

Prepare to go phishing. Before you start, it's sensible to think about your organization and your **company culture**. Try to establish what level of maturity you want to achieve with your security awareness program. If you have specific goals in mind, it will be easier to work toward success and measure progress.

Plan what happens after phishing. When you run your phishing tests, some people will inevitably fail them. You must decide how you are going to deal with the results. You'll also have to plan how to **deal with people who fail tests**, particularly those who fail tests repeatedly. Failure should trigger some remedial training.



Conduct a baseline test. Establish a baseline by sending a generic phishing email that **simulates what would happen** if a fairly sophisticated phishing attack hit your organization. Send it to everyone

simultaneously so there's no opportunity for people to talk to each other about it.

Launch your ongoing phishing program. You should send out new phishing emails regularly, at least monthly, but biweekly or weekly is better. **You want people questioning new emails**, hovering over links, and being careful. It's also crucial to ramp up the difficulty over time.

Review progress and adapt. Over time you may want to tailor the phishing program to **different departments**, such as finance, HR, or the executive team. Add penalties to your company policies. You'll want to trigger remedial training initially, but if employees repeatedly fail, there must be a penalty if employees repeatedly fail because they're putting the company at risk.

SUGGESTION: How does your current program measure up? How has your phishing vendor performed? Would you like to see if you can upgrade your service for a better price? These are two vendors who would love to compete for your phishing campaign business:

Have you EVER had a Penetration Test performed on your network and connected assets?	**No**

FINDING: Do you know where vulnerabilities are hiding in your environment? Chances are you don't, and a hacker might just find them for you. It's a risk you can't afford to take, but you can prevent it with **penetration testing**.

PENETRATION TEST BEST PRACTICES: By undergoing a penetration test, you uncover cybersecurity weaknesses, study how they can be exploited, and secure them against an attack. Penetration testing is a key part of a security strategy that contributes to protecting from an attack by focusing on vulnerabilities in your environment. As with any security method, penetration testing requires careful planning. Follow these seven best practices for effective results as you implement penetration testing in your environment.

Penetration Test: Best Practices

Define your scope and budget. It might make sense to want to test your entire environment, but the cost might convince you otherwise. Therefore, consider your high priority and low priority areas that need penetration testing. High priority areas are where your greatest vulnerabilities exist.

Include financial and customer data sources. Conduct comprehensive, full-scale penetration testing on your data sources, especially to meet industry and security regulations. But don't stop with just the data sources; also test the software that connects to them and its supporting infrastructure.

Consider penetration testing remotely accessible resources. Whether you have remote employees, remote building automation systems (BAS), or resources that have remote access, factor each remote endpoint into your penetration testing plan. Penetration testers can identify your exposure to external attacks by finding and assessing your publicly accessible assets.

Follow a penetration testing methodology. The results of your penetration test can vary widely based on which methodology you follow. Some of the common testing methodologies and standards include:

- **Penetration Testing Execution Standard** (PTES)
- **Payment Card Industry Data Security Standard** (PCI-DSS)
- **Open-Source Security Testing Methodology Manual** (OSSTMM)
- **OWASP Web Security Testing Guide**
- **National Institute of Standards and Technology** (NIST) Special Publication 800-115
- **Information System Security Assessment Framework** (ISAFF)

Choosing a method is important when conducting your penetration testing. However, as you search for a penetration testing service, consider the methodologies they follow and how they compare to your objectives.

Prepare for the test. Once you decide what you need to test and how you'll conduct it, prepare for the test, for example:

- Know which tests your hosting or **cloud provider** allows and seek proper authorizations to conduct them.
- Identify **team members** who will review the test report and fix issues that were discovered during the test.
- **Schedule patching** to occur after testing is completed and you've reviewed the results unless you need to fix a critical issue that impacts your customers.

Important Note: Any changes you make during penetration testing can affect the testing environment and your results, not to mention waste your pen test investment.

Create a communication plan. Communication is key, even in pen-testing. Establish communication protocols between you, your team, and the penetration testing team to ensure a smooth process. Choose a single point of contact on your team to be available for any critical information and questions during the test.

Choose a qualified pen tester. Your penetration testing service provider should fit these criteria at a minimum:

- Uses automated **and** manual techniques for maximum effectiveness in uncovering vulnerabilities and advanced threats in your environment.
- Examines internal **and** external IT assets by using commercial, open-source, and custom tools to discover rogue or unknown resources that could lead to an attack.
- Explores how high-risk vulnerabilities can be exploited to determine the impact on your operating environment and feasibility of a potential breach.
- Minimizes false positives through further validation and vetting.
- Generates custom reports highlighting the risks of identified and exploited vulnerabilities and offers corresponding strategic mitigation, recommendations, and **actionable**

insights.

The more vulnerabilities your service provider uncovers, the better off your organization is by knowing what to fix before a hacker exploits them.

SUGGESTION: As mentioned above, penetration testing is most effective when performed by an experienced outside service or contractor. Hiring an external resource with little previous knowledge of your systems ensures objectivity in the testing process and exposes vulnerable areas missed by your developers and security team. The service you choose should conduct testing regularly—at least once a year or more frequently, depending on your company's risk exposure and the maturity of your security implemented controls. Here we have also included a less-invasive option for a "Vulnerability Test", in case the timing isn't yet right for penetration testing:

Do you use an advanced email threat protection service?	**Yes**
Do you implement email message authentication, like SPF, DKIM, and DMARC to protect against phishing messages?	**Yes**

FINDING: Let us be the first to congratulate you on using advanced email threat protection services AND for implementing anti-spoofing measures such as SPF, DKIM, and DMARC to authenticate messages and protect against phishing. You realize that email is still one of the most common vectors by which enterprises are attacked. While we recognize that you have taken these great steps already, we'd like to share with you some Microsoft Office 365 (cloud) protection strategies and best practices that are sometimes overlooked.

EMAIL PROTECTION BEST PRACTICES: Specialized standalone email security solutions are available to combat each type of attack. But your IT department needs comprehensive visibility and **control** over the enterprise's overall email security strategy and defense.

Here are four email security best practices to incorporate into your enterprise's overall cyber security strategy if you haven't already.

Email Protection: Best Practices

Improve your endpoint and email security hygiene. Endpoint email security encompasses a variety of tools and processes that protect end-users' devices from being compromised through email-delivered attacks. To combat phishing emails, spam, and malware, enterprises should:

- Install **endpoint email security** software in combination with **anti-virus** protection tools. These can filter and **block malware** or spam emails from suspicious senders and IP addresses and clean up infected systems from sending outbound spam.

- Your endpoint security software needs to confirm whether a **device meets security policies** before granting it access to your network. Remote devices that haven't updated their operating systems, have their firewall turned off, or have other specifically recognized security flaws should be denied access.

- Implementing enterprise-wide policies on **basic password** and corporate email security best practices. For example, you can instruct employees to:

    - **Avoid storing passwords** on paper notes and in public locations,

    - **Avoid duplicating old passwords** or those created on other sites,

    - **Create strong passwords** with characters (@) instead of alphanumeric letters (a),

    - **Use passwords that can't be guessed** by strangers (avoiding names, ages, birthdates, company, social media interests, etc.)

- **Two-factor authentication should also be mandated**, or at least encouraged, for all employees, whether through a mobile phone, an app on a device, or authentication tokens.

- It also helps to **continuously train and test employees** on

email security best practices, including how to spot phishing emails, so they're well prepared to avoid and report them.

Safeguard your email content with encryption. Fully protecting your email content requires that both the content and attachments are encrypted while in transit and at rest in the inbox. Popular email platforms like Microsoft Office 365 (cloud) typically doesn't have the requisite enough enterprise-level email encryption to secure organizations against all cyber threats fully. And to the extent that these platforms support encryption, they only work if both the sender and recipients have certain extensions enabled. **Third-party add-in encryption services can close these corporate email security gaps**.

Implement email server protection. Spam and DDoS attacks on these servers can disrupt regular email transfer and processing. Hackers can also use them as a way to **send spam emails from your server**, harming your reputation and getting you blacklisted. This is why it is important to protect your email servers. Direct your IT team to enforce sound email server protection techniques, starting with:

- Restricting the **mail relay parameter** by specifying a list of domains and IP addresses to which your mails can be safely forwarded
- Limiting the **number of connections** to reduce the chance of spam and DDoS attacks
- Verifying the sender through **reverse DNS lookup** before accepting incoming messages
- Use **content filtering** to fight spammers from accessing your server

Prevent data leakage and breaches. Your enterprise can prevent the leakage of sensitive data in emails by filtering, blocking, or censoring based on keywords, expressions, and rules. For example, your IT team can block all outgoing emails with personal information like social security numbers, credit card information, and files with the keyword "confidential" or "internal use only". A good rule of thumb is to use encryption to protect outbound data while filtering inbound emails to block malware, viruses, and phishing threats. Data loss prevention (DLP) tools can be applied to prohibit sensitive information from spreading outside your enterprise by alerting your IT admin about violations of data access policies.

SUGGESTION: If you are happy with your current email threat protection service, but want to see if there is better pricing available, these are two vendors that we have had a great experience with that you may consider:

Do you have firewalls in place now to protect your local area network?	**Yes**
Are your firewalls being managed and updated to current levels of firmware to your satisfaction?	**No**

FINDING: Nice work! You've got a firewall device to protect your edge, but you're not satisfied with how they are being managed. Not to worry, most companies are in the same situation. We can easily find you a managed firewall provider to secure your local area network. But what about security for the data created in the cloud, sent to the cloud, and downloaded from the cloud? Protecting cloud data, which is **your responsibility,** requires visibility and control. In the steps below, we've outlined a core set of best practices for cloud security that can guide you toward a secure cloud and address cloud security issues.

BEST PRACTICES FOR CLOUD SECURITY: Cloud services are used for multiple purposes in corporate environments, from storing data in services like Dropbox to accessing productivity tools through Microsoft Office 365, and deploying IT infrastructure in Amazon Web Services (AWS). However, security for this data is your responsibility. Here is a two-phased plan that will help you protect your Cloud assets:

Protecting Your Cloud: Security Best Practices

Phase 1: Understand cloud usage and risk - The first phase of cloud computing security is focused on understanding your current state and assessing risk. Using cloud security solutions that allow for **cloud monitoring**, you can accomplish the following steps:

Step 1: Identify sensitive or regulated data. Your **largest area of risk** is loss or theft of data that will result in regulatory penalties or loss of intellectual property. Data classification engines can categorize your data so you can fully assess this risk.

Step 2: Understand how sensitive data is being accessed and shared. Sensitive data can be held securely in the cloud, but you have to monitor **who accesses it and where it goes**. Assess the permissions on files and

folders in your cloud environment and access contexts like user roles, user location, and device type.

Step 3: Discover shadow IT (unknown cloud use). Most people do not ask their IT team before signing up for a cloud storage account. Use your web proxy, firewall, or SIEM logs to discover what cloud services are being used that you don't know about, then run an assessment of their risk profile.

Step 4: Audit configurations for your infrastructure-as-a-service (IaaS) such as AWS or Azure. Your IaaS environments contain dozens of critical settings, many of which can create an exploitable weakness if misconfigured. Start by auditing your configurations for identity and access management, network configuration, and encryption configurations.

Step 5: Uncover malicious user behavior. Both careless employees and third-party attackers can exhibit behavior that indicates malicious use of cloud data. **User behavior analytics** (UBA) can monitor anomalies and mitigate both internal and external data loss.

Phase 2: Protect your cloud

Once you understand your cloud security risk posture, you can strategically **apply protection to your cloud services** according to their level of risk. Several cloud security technologies can help you accomplish the following best practices:

Step 1: Apply data protection policies. With your data now classified as sensitive or regulated, you can **assign policies** that govern what data can be stored in the cloud, quarantine or remove sensitive data found in the cloud, and coach users if they make a mistake and break one of your policies.

Step 2: Encrypt sensitive data with your own keys. Encryption available within a cloud service will protect your data from outside parties, but the cloud service provider will still have access to your encryption keys. Instead, encrypt your data using your **own keys** so you fully control access. Users can still work with the data without interruption.

Step 3: Set limitations on how data is shared. Once data enters the cloud, **enforce your access control policies** across one or multiple services. Start with actions like setting users or groups to viewer or editor and controlling what information can be shared externally through shared links.

Step 4: Stop data from moving to unmanaged devices you don't know about. Cloud services provide access from anywhere with an

internet connection, but access from unmanaged devices like a personal phone creates a blind spot for your security posture. **Block downloads to unmanaged devices** by requiring device security verification before downloading.

Step 5: Apply advanced malware protection to infrastructure-as-a-service (IaaS) such as AWS or Azure. Anti-malware technology can be applied to the OS and virtual network to protect your infrastructure. Deploy **application whitelisting** and **memory exploit prevention** for single-purpose workloads and machine-learning based protection for general-purpose workloads and file stores.

NOTE: Malware can compromise a shared folder that syncs automatically with a cloud storage service, replicating the malware in the cloud without user action. **Scan your files in cloud storage** with anti-malware to avoid ransomware or data theft attacks.

SUGGESTION: If you'd like some help managing your LAN firewall, and/or putting together a **plan** to protect your data and applications in the Cloud, or would like to interview **managed cloud security providers**, we've put together a list of companies we know do a great job:

Do you utilize web filtering to block access to known malicious websites?	**Yes**

FINDING: Congratulations! You are currently using a URL filtering solution to protect your employees from web-based threats and monitor their web activity. Just to make sure you've got all of your bases covered, we've put together a quick list of best practices that you can measure yourself against. Keep up the great work!

WEB FILTERING BEST PRACTICES: These best practices can guide you on how to reduce your exposure to web-based threats without limiting your users' access to web content that they need.

Web Filtering Best Practices

Identify the applications you want to allow. Allowed applications include not only the applications you provision and administer for business and infrastructure purposes and the applications your users need to get their jobs done, and applications you might want to allow for personal use. After you've identified these sanctioned applications, you can use URL filtering to control and secure all the web activity that is not on the allow list.

Plan a smooth web filtering rollout to your organization. Get visibility into your users' web activity to plan the most effective URL Filtering policy for your organization and roll it out smoothly. This includes:

- Use "Test a Site" to see how the Firewall URL filtering cloud database categorizes a specific URL, and to learn about all possible URL categories.
- Starting with a (mostly) passive URL Filtering profile that alerts on URL categories. This gives you visibility into the sites your users are accessing, so you can decide what you want to allow, limit, and block.
- Monitor web activity to assess the sites your users are accessing and see how they **align with your business needs**.
- Block URL categories that classify **malicious** and **exploitive** web content. While we know that these categories are dangerous, always keep in mind that the URL categories that you decide to block might depend on your business needs.
- Use URL categories to phase in decryption and **exclude sensitive or personal information** (like financial services

and health and medicine) from decryption.

- Plan to **decrypt the riskiest traffic first** (URL Categories most likely to harbor malicious traffic, such as gaming or high-risk) and then decrypt more as you gain experience. Alternatively, decrypt the URL Categories that **don't affect your business first** (if something goes wrong, it won't affect business), for example, news feeds.

Listen to user feedback. Make sure to listen to user feedback, run reports to ensure that decryption is working as expected, and then **gradually** decrypt a few more URL Categories, and so on. Plan to make decryption exclusions to exclude sites from decryption if you can't decrypt them for technical reasons or because you choose not to decrypt them.

Decide how users interact with high-risk and medium-risk content. The web content you sanction and the malicious URL categories you block outright are just one portion of your overall web traffic. The rest of the content your users are accessing is a combination of benign (low-risk) and risky content (high-risk and medium-risk). High-risk and medium-risk content is not confirmed malicious but is closely associated with malicious sites. For example, a high-risk URL might be on the same domain as a malicious site, or maybe it hosted malicious content in the past.

Enable Safe Search. Schools and other **educational institutions** should use safe search enforcement to ensure that search engines filter out adult images and videos from search results. You can even transparently enable safe search for users.

Enable the firewall to hold an initial web request as it looks up a website's URL category with the firewall whitelist database. When a user visits a website, a firewall with URL filtering enabled checks its local cache of URL categories to categorize the site. If the firewall doesn't find the URL's category in the cache, it performs a lookup in the Firewall providers' URL database. By default, the Firewall allows the user's web request during this cloud lookup and enforces policy when the server responds.

SUGGESTION: If you have any questions about your current web URL and content filtering solution or managed services provider, or would like to entertain new bids for your business, we work with two great firms who we know will do a great job for you:

Web Filtering

Do you segment your network based on the classification level of information stored on said systems?	**No**

FINDING: Network segmentation (also known as network partitioning or network isolation) is the practice of dividing a computer network into multiple subnetworks to improve performance and security. By isolating (or segmenting) the network into separate contained parts, network segmentation effectively prevents a single point of failure. It makes it difficult for unauthorized users to compromise the entire network. You need to take this essential step to protect your network. To give you some guidance on how to do this right, we've compiled a list that you can use with your internal team and/or third-party managed services provider.

NETWORK SEGMENTATION BEST PRACTICES: There are a few ways to segment your network. Typically segmentation is done through a combination of **firewalls**, Virtual Local Area Networks (**VLANs** - smaller network segments that connect hosts virtually), and Software-Defined Networking (**SDN**). Regardless of how you segment, here are some best practices that will ensure the maximum level of security:

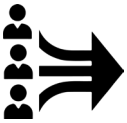
Network Segmentation Best Practices

Follow Least Privilege. When segmenting your network, it's important to minimize who and what has access within and across systems according to actual need. In other words, not everyone needs access to every part of the network. By following the principle of least privilege and role-based access, you can limit hosts, services, users, and networks from accessing data and functions that are outside their immediate responsibility.

Limit third-party access. A recent report found that 44% of organizations experienced a breach in the last 12 months, with 74% saying it resulted from giving too much privileged access to third parties. One way to do this is to **create isolated portals** for third parties that need access to your network to provide services. This keeps their access limited to just those necessary areas of your network.

Audit and monitor your network. Segmenting your network is just the first step to a strong segmentation strategy. The next step is continually monitoring and auditing your network to ensure the architecture is

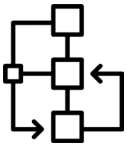
secure and identify gaps in your subnetworks that could be exploited. Monitor your network to identify and isolate traffic or security issues quickly. Then conduct regular audits to surface architectural weaknesses.



Make legitimate paths to access easier than illegitimate paths. When evaluating and planning your architecture design, pay attention to how you plot access and what paths users will take to connect to your network. While it is important to create secure access points for your users, pay attention to how bad actors might try to access those same subnetworks illegitimately. Design your network to make legitimate paths easier to navigate than illegitimate paths to shore up your security.

Combine similar network resources. Save time and reduce security overhead by combining similar network resources into individual databases. Categorize data by **type** and degree of **sensitivity as you review your network**. Segmenting your network this way allows you to apply security policies while protecting data more efficiently quickly.

Don't over-segment. Gartner notes that one of the most common errors organizations make when segmenting their networks is over-segmenting or creating too many zones. Having too many segments adds unnecessary complexity and makes it harder to manage your network as a whole. Oversegmenting can quickly expand the scope of your security management, making it costly and inefficient.



Visualize your network. To design an effective and secure network architecture, you first need to understand your users, what components make up your network, and how all the systems relate to one another. In other words, without a clear picture of your current state, it will be difficult to plan and achieve your desired state. Visualize your network with a network diagram to get a bird's eye view of all the moving parts and identify who needs access to what data so you can map your network successfully

SUGGESTION: As you begin to put together your network segmentation plan, you may consider bringing in a managed security provider to help make sure you've done everything correctly, or just to offload this task to keep your IT team focused on other more pressing issues. Here are two consulting firms that we know will do a great job helping you segment your network.

Do you ensure employees utilize least privilege at all times, and never operate as the local administrator?	**Yes**

FINDING: Applying the principle of least privilege is hard, even for organizations with high incentives to be secure. It requires constant testing of security boundaries and the monitoring of privileged access. But the benefits are huge: It will help you defend against external attacks and insider threats, comply with regulatory requirements, and simplify change and configuration management. Congratulations on taking this very important step to protect your network. Just as a quick best practices check, we've compiled a list that you can compare against your current strategy to make sure you didn't miss anything:

ACCESS CONTROL BEST PRACTICES: To implement the principle of least privilege, you need to set up different types of account for different purposes. These include user accounts, privileged accounts, and shared accounts:

Understanding Types of Accounts

User accounts — Most people in your network should get a regular user account with the access required to perform their normal duties.

Privileged accounts — A privileged account with elevated privileges. There are two main types. The first is accounts that enable specific users, such as accounting executives, to access critical data and services. The other is **administrator accounts**, which grant special admin rights on the network. In a Microsoft environment, the most important administrative account is the **Domain Admin account**. While a local admin account grants complete control of a single machine, a Domain Admin account has total control across your network — which means **attackers often seek to gain Domain Admin privileges**. Because of their power, privileged accounts should be used only when necessary, and their activity should be carefully monitored. Domain Admin accounts, in particular, must be very closely controlled. Administrators should generally have both a user account and a privileged account. They should use their least-privileged user accounts unless they need to perform a specific task that requires their administrative privileges.

Shared accounts (generic accounts) — Using shared accounts is usually not recommended; the preferred method is to have each individual use their account. However, in some limited situations, it may be acceptable

to create accounts that are shared among a group of users. For example, most organizations of any significant size have outsiders who need to access their network, such as clients, contractors, or business partners visiting for a brief period of time. **Creating guest accounts with bare minimum privileges** can be an expedient way to enable these users to complete basic tasks.

Service accounts — Humans are not the only entities that might require privileged access to network resources. You might have **software that needs to access** your network without human intervention, such as database services that start when their machine boots up. **These services require their own accounts**. One common but dangerous practice is to assign these services to a Domain Admin account. If attackers compromise an application running as a Domain Admin, they immediately get administrative access to the system. Application security best practices require organizations to determine what access each application requires to run correctly and create service accounts with just enough privileges for the applications to accomplish their required tasks; limiting the access that applications have to your network will go a long way toward protecting it from abuse. Active Directory provides a service account with a very strong password that is automatically changed.

Privilege Management

User Groups – A better access control strategy is to place users into groups based on their job roles and then to manage privileges for those groups. Suppose a user transfers from one department to another. In that case, you can simply remove them from certain groups and add them to others, rather than having to manually remove dozens or hundreds of specific access rights and add a similar number of new ones.

Assigning User Working Hours – For employees who work a relatively consistent schedule, another layer of least privilege is to restrict the use of accounts to the **individual's normal working hours**. For example, if a given employee generally works from 8 a.m. to 5 p.m., their account should not be usable at 1 a.m. Of course, people fluctuate a bit, so you might want to set up this hypothetical account to be operational from 7 a.m. to 7 p.m.

Using Location-based Restrictions – In many cases, you can also **limit which locations** an account can be used from. For instance, an account might work fine in the San Francisco office but not work at all from the Los Angeles office.

Using Machine-based Restrictions – Machine-based restrictions are a special type of location-based control. For instance, you can keep a user who works in the accounting department on the 4th floor from using machines on the 10th-floor software development area. Again, not all accounts can be locked down like this; for example, some technical support personnel might need to work from almost any computer on the network.

SUGGESTION: If you're experiencing any difficulty at all with your current Least Privilege plan, or want to meet with an expert to look for possible optimization strategies, here are some consultants who would give you excellent advice.

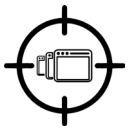
Do you currently have a solution in place to defend against a DDoS attack?	**No**

FINDING: The best time to fortify your defenses is now, NOT in the wake of (or during) an attack, but rather beforehand to ensure a quick and effective response. What exactly is a DDoS attack? It's an attack intended to take your organization or service offline or otherwise render your resources unreachable and/or unusable, which originates from (or appears to originate from) multiple hosts. The "multiple hosts" part of the attack is what makes it "distributed," making the attack more difficult to defend against. An attack originating from a single host or IP address can be easily blocked with a simple router access list or firewall rule. There are multiple best practices that you can follow to further improve your ability to withstand a DDoS attack which we'd like to share with you here:

DDoS PREVENTION BEST PRACTICES: There are three main types of DDoS attacks that you need to be prepared for:

Types of DDoS Attacks

Volumetric attacks. Over 50% of the attacks launched last year were volumetric attacks, where attackers focus on filling up a victim's network bandwidth. Volumetric attacks were also the weapon of choice for pro-Russian cyber warfare units against Ukrainian government websites and applications. Among the most common volumetric attacks are User Datagram Protocol (UDP) flood attacks, where an attacker sends a large number of UDP packets to random ports on a remote host



Protocol attacks (sometimes also called state-exhaustion attacks) target a weakness in how a protocol operates. A well-known protocol attack is the **SYN flood**, which targets the three-way handshake mechanism in **TCP**. When a server receives an SYN packet, this is a signal to the server that another machine wants to open a TCP connection. In an SYN flood attack, an attacker sends a rapid succession of TCP SYN requests--typically from spoofed source IP addresses--to open a connection to a network server. The server sends SYN ACK packets back to the source addresses, which never reply with an ACK. The server keeps the half-open TCP connections around, using up resources until the server can no longer accept any new connections.

Application attacks target weaknesses in how an application works. One well-known application attack is Slowloris, which targets web servers. In a **Slowloris** attack, the attacker sends HTTP requests to a web server without completing the requests. Periodically (and slowly--hence the name), the attacker will send additional headers, thus keeping the request "alive" but not finished. Like an SYN flood, this forces the web server to maintain open connections for these partially completed HTTP requests, eventually preventing it from accepting any new connections.

As we mentioned above, your organization should start planning for DDoS attacks in advance. It is much harder to respond after an attack is already underway. While DDoS attacks can't be prevented, **steps can be taken to make it harder** for an attacker to render a network unresponsive.

Defending Against DDoS Attacks

Architecture. To fortify resources against a DDoS attack, it is important to make the architecture as resilient as possible. Fortifying network architecture is an important step in DDoS network defense

and ensuring business continuity and protection from any kind of outage or disaster situation.

The following steps will help disperse organizational assets to avoid presenting a single rich target to an attacker:

- Locate servers in different data centers.
- Ensure that data centers are located on different networks.
- Ensure that data centers have diverse paths.
- Ensure that the data centers, or the networks that the data centers are connected to, have no significant bottlenecks or single points of failure.

Ensure that resources are **geographically dispersed** and not located in a single data center. If resources are already geographically dispersed, it is important to view each data center with more than one pipe to the Internet and ensure that not all data centers are connected to the same Internet provider.

Hardware. Deploy appropriate hardware that can handle known attack types and use the options that are in the hardware that would protect network resources. In particular, certain types of DDoS attacks have been in existence for quite some time, and a lot of network and security hardware is capable of mitigating them. Most modern hardware, **network firewalls**, **web application firewalls**, and **load balancers** will generally have a setting that allows a network operator to start closing out TCP connections once they reach a certain threshold.

Outsourcing: Traffic Scrubbing. Several large providers specialize in scaling infrastructure to respond to attacks. These providers can implement **cloud scrubbing services** for attack traffic to remove the majority of the problematic traffic **before** it ever hits your network. These providers specifically work in DDoS mitigation. During an attack, these services reroute traffic destined for the victim's network to the mitigation center, where it is scrubbed, and legitimate traffic is then forwarded to the organization. These DDoS mitigation providers have the type of scalable and dynamic load balancing available to respond to the unprecedented levels of traffic that often result from a DDoS attack.

SUGGESTION: If you'd like to build up your DDoS defenses with carefully configured firewalls, traffic scrubbers, data centers with redundant paths, or any other idea we listed here, we've got two DDoS Mitigation firms that we work with you can help you:

Do you have an employee Password Policy in place?	**Yes**

FINDING: Excellent, you have a password policy in place! This is important because every data privacy compliance standard has questions about this because it drastically minimizes the chances that you'll experience a breach due to a compromised password. Just as a reality check, we've put together the following best practices so that you can ensure your current plan checks all of the 'boxes'.

PASSWORD POLICY BEST PRACTICES: Here are some tips for creating strong passwords. Take a moment to review these, and consider strengthening some of your passwords if they fall short.

Password Policy Best Practices

Diversity of characters: create unique passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters.

Do not use your network username as your password.

Don't use easily guessed passwords, such as "password" or "user."

Do not choose passwords based upon details that may not be as confidential as you'd expect, such as your birth date, your Social Security or phone number, or the names of family members.

Do not use words that can be found in the dictionary. Password-cracking tools freely available online often come with dictionary lists that will try thousands of common names and passwords. If you must use dictionary words, try adding a numeral to them, as well as

punctuation at the beginning or end of the word (or both!).

Avoid using simple adjacent keyboard combinations: For example, "qwerty" and "asdzxc" and "123456" are horrible passwords and are trivial to crack.

Complexity is nice, but length is key. Some of the easiest to remember passwords aren't words at all but **collections of words** that form a **phrase or sentence**, perhaps the opening sentence to your favorite novel or the opening line to a good joke. Just remember that **each character you add to a password or passphrase makes it an order of magnitude harder** to attack via brute-force methods.

Avoid using the same password at multiple Web sites. It's generally safe to re-use the same password at sites that do not store sensitive information about you (like a news Website), provided you don't use this same password at sites that are sensitive.

Never use the password you've picked for your email account at any online site: If you do, and an e-commerce site you are registered at gets hacked, there's a good chance someone will be reading your email soon.

Don't store your list of passwords on your computer in plain text. The most secure method for remembering your passwords is to create a list of every Web site for which you have a password, and next to each one, write your login name and a **clue** that has meaning only for you. If you forget your password, most Websites will email it to you (assuming you can remember which email address you signed up with).

Store passwords in the cloud secured with a Master Password. Several online third-party services can help users safeguard sensitive passwords, including **LastPass**, **DashLane**, and **1Password** that store passwords in the cloud and secure them all with a master password. If entrusting all your passwords to the cloud gives you the creeps, consider using a local password storage program on your computers, such as **Roboform**, **PasswordSafe,** or **Keepass**. Again, take care to pick a **strong master password**.

SUGGESTION: With these Best Practices in mind, if you would like some additional help examining your current password policy, we've got some great consultants who can advise you:

Password Policy

Does your company carry Cybersecurity Insurance?	Yes

FINDING: Excellent! You have an insurance policy in place! This will help cover the financial losses that result from cyber events and incidents you may experience. In addition, cyber-risk coverage helps with the costs associated with remediation, including payment for legal assistance, investigators, crisis communicators, and customer credits or refunds.

MORE BACKGROUND ON CYBERSECURITY INSURANCE: The most common question we hear is "What is covered and not covered by cyber insurance?" If you're wondering if your current policy is in-line with the "norm," we'd like to share with you some observations from what we've seen in the marketplace. **This is NOT a guarantee, as rates and coverage vary wildly**:

Cyber Insurance Plans Typically Cover:

- Meeting extortion demands from a **ransomware attack**
- **Notifying customers** when a security breach has occurred
- **Paying legal fees** levied as a result of privacy violations
- **Hiring computer forensics experts** to recover compromised data
- **Restoring identities** of customers whose PII was compromised
- **Recovering data** that has been altered or stolen
- Repairing or replacing damaged or **compromised computer systems**
- Cost of providing **credit monitoring services** for customers affected

Cyber Insurance Typically DOES NOT Cover Incidents Caused By:

- **Poor configuration** management

- **Careless** mishandling of digital assets
- **Preexisting or prior breaches or cyber events**, such as incidents that occurred before the policy was purchased
- Cyber events initiated and **caused by employees or insiders**
- **Infrastructure failures** *not* caused by a purposeful cyber attack
- **Failure to correct a known vulnerability**, such as a company that knows that a vulnerability exists, fails to address it and is then compromised from that vulnerability
- **The cost to improve technology systems**, including security hardening in systems or applications

SUGGESTION: Because cybersecurity insurance is new, **policies will vary widely from one provider to the next**. When your policy comes up for renewal, you should closely review policy details to ensure it contains the updated protections and provisions. In the meantime, you should evaluate whether your current policy protects against **known** *and* **emerging** cyber incidents and threat profiles. If you'd like to have a second pair of eyes current policy or would like to begin planning for your renewal, we work with two specialists who can help:

Security Assessment: DATA PRIVACY COMPLIANCE

Ensuring your company is in compliance with data privacy laws not only ensures you follow the best practices to prevent a ransomware attack and/or data exfiltration, it also prevents your company from having to pay hefty fines. This section highlights the data compliance regulations that your company needs to be following, according to your feedback.

ADBNA	**Alabama Data Breach Notification Act** (for Alabama residents)	**Yes**

FINDING: The Alabama Data Breach Notification Act of 2018 (2018-396) (the Act) requires a business entity to notify its consumers of a breach in security that results in the "unauthorized acquisition of sensitive personally identifiable information." Since you do business in Alabama, the Alabama Data Breach Notification Act is something you need to comply with or face heavy fines from the Attorney General. You indicated that your confidence level with your current compliance is a 1 out of 10.

It sounds like there is a lot of room for improvement. Below we've compiled some information to help you understand exactly what the ADBN Act is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help put together an ADBN Act plan for you.

ALABAMA DATA BREACH NOTIFICATION ACT CHECKLIST: The Alabama Data Breach Notification Act can be broken down into a few basic parts, all meant to protect user's personal information. Details of each of these regulations can be found on the Alabama Office of Information Technology website: https://oit.alabama.gov/621-breach-notification/

Below we've summarized the law for easy reading:

Definition of "Personal Information"

Personal information or "sensitive personally identifying information" as it is called by the Alabama law, is defined as an Alabama resident's **first name** or first initial and **last name** in combination with one or more of the following with respect to the same Alabama resident:

- A non-truncated **social security number** or **tax identification numbe**r;
- A non-truncated **driver's license number**, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual;

- A **financial account number**, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account;
- Any information regarding an individual's **medical history**, mental or physical condition, or medical treatment diagnosis by a healthcare professional;
- An individual's health insurance policy number or subscriber identification number and any unique identifier **used by a health insurer** to identify the individual;
- A **username** or **email address**, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

Reasonable safeguard (security) requirements

The Alabama law also imposes a reasonable security requirement for covered entities and their third-party vendors. Security measures include:

- **Designation of an employee(s)** to coordinate the reasonable security measures;
- **Identification** of internal and external risks of a breach of security;
- **Adoption** of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards;
- **Retention** of service providers, if any, that are contractually required to maintain appropriate safeguards;
- Keeping management of a covered entity, including its **board of directors**, appropriately informed of the overall status of its security measures;

Notably, the law also requires covered entities to **conduct an assessment** of its security based upon the entity's security measures as a whole and placing emphasis on data security failures that are multiple or systemic, including consideration of all the following:

- The **size** of the covered entity.
- The **amount** of sensitive personally identifying information and the type of activities for which the sensitive personally-identifying information is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the

covered entity.

- The covered entity's **cost** to implement and maintain the security measures to protect against a breach of security relative to its resources.

Notification Guidelines

- The law **requires** a covered entity that experiences a data breach to notify affected Alabama residents "as expeditiously as possible and without unreasonable delay," taking into account a reasonable time to conduct an appropriate investigation, but **not later than 45 days** from the determination that a breach has occurred and is reasonably likely to cause substantial harm, with certain exceptions. (this includes third-party breaches)

- **If more than 1,000 state residents are impacted** by the breach, the state attorney general and consumer reporting agencies must be notified. Following a number of other states, the Alabama law also sets forth specific content requirements for the notices to individuals and the Attorney General.

Enforcement / Violations

A violation of the Alabama Data Breach Notification Act is also considered a violation of the Alabama Deceptive Trade Practices Act. However, criminal penalties are not available. The Office of the Attorney General maintains the exclusive authority to bring an action for civil penalties – there is no private right of action.

Failure to comply with the Alabama law could result in fines of up to **$5,000 per day**, with a cap of **$500,000 per breach**

*NOTE: Such penalties are reserved for failure to comply with the law's notification requirements, and it is not clear to what extent such penalties would apply for failure to comply with the law's reasonable security requirements.

* Source: https://www.natlawreview.com/article/alabama-becomes-final-state-to-enact-data-breach-notification-law

If you are like many companies who use third party email or cloud storage services, it **does not absolve** you from ensuring that personal data is processed in accordance with the ADBN Act. Unless you can clearly demonstrate that it was "not in any way responsible for the event giving rise to the damage," you will be fully liable for any infringement caused by a non-compliant third party.

For this reason, it's important to carefully vet any third-party / cloud services you use to make sure they have a good track record for security.

SUGGESTIONS FOR THE ADBN ACT COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in the Alabama Data Breach Notification Act that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two Compliance Firms (shown below) to make sure your organization fully complies with this law so that you'll pass any audit that may come and so that you'll be ready, with a plan, should a breach occur.

MASS93H	Massachusetts General Law Chapter 93H	Yes

FINDING: The Massachusetts General Law Chapter 93H gives consumers more control over the personal information that businesses collect about them and provides guidance on how to implement the law. Since you do business in Massachusetts, General Law Chapter 93H is something you need to comply with or face heavy fines from the state's Attorney General. You indicated that your confidence level with your current compliance is a 1 out of 10.

It sounds like there is a lot of room for improvement. Below we've compiled some information to help you understand exactly what Massachusetts General Law Chapter 93H is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help put together a compliance plan for you.

GENERAL LAW CHAPTER 93H CHECKLIST: Most state data privacy and security laws can be broken down into six basic sections. Details of each of these sections can be found on the Massachusetts legislature website: https://malegislature.gov/laws/generallaws/parti/titlexv/chapter93h

Below we've summarized your responsibilities for easy reading:

Definition of "Personal Information"

Personal information or "sensitive personally identifying information" as it is called by most state laws, is defined as a resident of the commonwealth's **first name** or first initial and **last name** in combination with one or more of the following with respect to the same state resident:

- A non-truncated **social security number** or **tax identification numbe**r;
- A non-truncated **driver's license number**, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual;
- A **financial account number**, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account;
- Any information regarding an individual's **medical history**, mental or physical condition, or medical treatment diagnosis by a healthcare professional;
- An individual's health insurance policy number or subscriber identification number and any unique identifier **used by a health insurer** to identify the individual;
- A **username** or **email address**, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

Reasonable safeguard (security) requirements

Massachusetts General Law Chapter 93H imposes a reasonable security requirement for covered entities and their third-party vendors. Security measures include:

- **Designation of an employee(s)** to coordinate the reasonable security measures;
- **Identification** of internal and external risks of a breach of security;
- **Adoption** of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards;
- **Retention** of service providers, if any, that are contractually required to maintain appropriate safeguards;

- Keeping management of a covered entity, including its **board of directors**, appropriately informed of the overall status of its security measures;

Notably, the laws also require covered entities to **conduct an assessment** of its security based upon the entity's security measures as a whole and placing an emphasis on data security failures that are multiple or systemic, including consideration of all the following:

- The **size** of the covered entity.
- The **amount** of sensitive personally identifying information and the type of activities for which the sensitive personally-identifying information is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity.
- The covered entity's **cost** to implement and maintain the security measures to protect against a breach of security relative to its resources.

Notification Guidelines

- Massachusetts state law **requires** a covered entity that experiences a data breach to notify affected commonwealth residents "as expeditiously as possible and without unreasonable delay," taking into account a reasonable time to conduct an appropriate investigation, but **not later than 45 days** from the determination that a breach has occurred and is reasonably likely to cause substantial harm, with certain exceptions. (this includes third-party breaches)
- Massachusetts state law **requires** a covered entity that experiences a data breach to notify the Director of Consumer Affairs and business regulation.
- **If more than 1,000 state residents are impacted** by the breach, the state attorney general and any relevant consumer reporting agencies must be notified. Most states set forth specific content requirements for the notices to individuals and the respective state's Attorney General.

Enforcement / Violations

A violation of the Massachusetts Data Privacy and Security Law usually falls under the state's Deceptive Trade Practices Acts, but criminal penalties are usually not available. In Massachusetts, the Office of the Attorney General maintains the exclusive authority to bring an action for civil penalties – there is no private right of action.

The Massachusetts Data Privacy and Security Law permits the Attorney General to seek injunctive relief, a **$5,000 penalty for each violation**, and reasonable costs and attorney's fees.

*NOTE: Such penalties are reserved for failure to comply with the law's notification requirements, and it is not clear to what extent such penalties would apply for failure to comply with the law's reasonable security requirements.

* Sources: https://www.bakerlaw.com/datamap_ajax.aspx?statename=MA
https://www.mass.gov/doc/frequently-asked-questions-regarding-data-breach-notifications-and-changes-to-the-data-breach-notification-law-mgl-chapter-93h/download

If you are like many companies who use third party email or cloud storage services, it **does not absolve** you from ensuring that personal data is processed in accordance with the Massachusetts Data Privacy and Security Law. Unless you can clearly demonstrate that it was "not in any way responsible for the event giving rise to the damage," you will be fully liable for any infringement caused by a non-compliant third party.

For this reason, it's important to carefully vet any third-party / cloud services you use to make sure they have a good track record for security.

SUGGESTIONS FOR MASS93H COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in the Massachusetts Data Privacy and Security Law that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two Compliance Firms (shown below) to make sure your organization fully complies with MASS93H so that you'll pass any audit that may come and so that you'll be ready to handle residents of the commonwealth's personal information properly.

PCI	**Payment Card Industry** (for anyone processing Credit Cards)	**Yes**

FINDING: The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store, or transmit **credit card information** maintain a **secure environment**. PCI Compliance means that your systems are secure, and your customers can trust you with their sensitive payment card

information; trust leads to customer confidence and repeats customers. As you try to meet PCI Compliance, you're better prepared to comply with additional regulations, such as HIPAA, SOX, and others.
Since your company processes credit cards, PCI is something you need to comply with.

In the questionnaire, you indicated that your confidence level with your current PCI compliance is a 3 out of 10. It sounds like there is a lot of room for improvement. Below we've compiled some information to help you understand exactly what PCI is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help put together a great PCI compliance plan for you.

PCI COMPLIANCE CHECKLIST: In an effort to enhance payment card data security, the PCI Security Standards Council (SSC) provides comprehensive standards and supporting materials, which include specification frameworks, tools, measurements, and support resources to help organizations ensure the security of cardholder information at all times. The PCI DSS has outlined twelve main requirements for PCI compliance.. Details of each of these regulations can be found on this website: https://www.pcisecuritystandards.org/

Below we've summarized your responsibilities for easy reading:

PCI Compliance Checklist

Use and maintain firewalls. Firewalls essentially block access to foreign or unknown entities attempting to access private data. These prevention systems are often the first line of defense against hackers (malicious or otherwise). Firewalls are required for PCI DSS compliance because of their effectiveness in preventing unauthorized access.

Proper password protections. Routers, modems, point of sale (POS) systems, and other third-party products often come with generic passwords and security measures easily accessed by the public. Too often, businesses fail to secure these vulnerabilities. Ensuring compliance in this area includes keeping a list of all devices and software which require a password (or other security to access). In addition to a device/password inventory, basic precautions and configurations should also be enacted (e.g., changing the password).

Protect Cardholder Data. Card data must be encrypted with certain algorithms. These encryptions are put into place with encryption keys — which are also required to be encrypted for compliance. Regular maintenance and scanning of primary account numbers (PAN) are needed to ensure no unencrypted data exists.

Encrypt Transmitted Data. Cardholder data is sent across multiple ordinary channels (i.e., payment processors, home office from local stores, etc.). This data must be encrypted whenever it is sent to these known locations. Account numbers should also never be sent to locations that are unknown.

Use and Maintain Anti-Virus. Installing anti-virus software is a good practice outside of PCI DSS compliance. However, antivirus software is required for all devices that interact with and/or store PAN. This software should be regularly patched and updated. Your POS provider should also employ anti-virus measures where it cannot be directly installed.

Properly Updated Software. Firewalls and anti-virus software will require updates often. It is also a good idea to update every piece of software in a business. Most software products will include security measures, such as patches to address recently discovered vulnerabilities, in their updates, which add another level of protection. These updates are especially required for all software on devices that interact with or store cardholder data.

Restrict Data Access. Cardholder data is required to be strictly "need to know." All staff, executives, and third parties who do not need access to this data should not have it. The roles that do need sensitive data should be well-documented and regularly updated.

Unique IDs for Access. Individuals who do have access to cardholder data should have individual credentials and identification for access. For instance, there should not be a single login to the encrypted data with multiple employees knowing the username and password. Unique IDs create less vulnerability and a quicker response time in the event data is compromised. — as required by PCI DSS.

Restrict Physical Access. Any cardholder data must be physically kept in a secure location. Both data that is physically written or typed and data that is digitally kept (e.g., on a hard drive) should be locked in a secure room, drawer, or cabinet. Not only should access be limited, but anytime the sensitive data is accessed, it should be kept in a log to remain compliant.

Create and Maintain Access Logs. All activities dealing with cardholder data and primary account numbers (PAN) require a log entry. Perhaps the most common non-compliance issue is a lack of proper record-keeping and documentation when it comes to accessing sensitive data. Compliance requires documenting how data flows into your organization and the number of times access is needed. Software products to log access are also needed to ensure accuracy.

Scan and Test for Vulnerabilities. All ten of the previous compliance standards involve several software products, physical locations, and likely a few employees. There are many things that can malfunction, go out of date, or suffer from human error. These threats can be limited by fulfilling the PCI DSS requirement for regular scans and vulnerability testing.

Document Policies. Inventory of equipment, software, and employees that have access will need to be documented for compliance. The logs of accessing cardholder data will also require documentation. How information flows into your company, where it is stored, and how it is used after the point of sale will also all need to be documented.

* Source: https://digitalguardian.com/blog/what-pci-compliance

PCI Non-Compliance: Fines and Negative Consequences*

MONTHLY PENALTIES

PCI Non-Compliance can result in penalties ranging from **$5,000** to **$100,000** per month by the Credit Card Companies (Visa, MasterCard, Discover, AMEX). Penalties depend on the volume of clients and transactions; these volumes can help to determine what level of PCI DSS compliance a company should be on.

Example: A level-1 company that has not met its PCI DSS requirements for over seven months can be fined up to $100,000 per month.

DATA BREACHES

PCI DSS Compliance does not prevent data breaches; companies that meet PCI DSS requirements can suffer attacks and data loss. If a company is compliant and suffers a data breach, **it can still be responsible for paying penalties.** However, the card brands may significantly lower or eliminate fines if the company in question has taken all the necessary steps to be PCI DSS compliant.

- Average cost of a breach is **$150 per record**, according to the Ponemon Institute's 2019 "Cost of a Data Breach" report;
- Costs of card replacement or issuing, between **$3 to $10 per card**;
- Increased rates charged by banks and/or processors
- Termination of Merchant Relationship with the credit card brands;

- Lawsuit by the clients whose information has been breached;
- Security costs related to mandatory credit monitoring for customers whose data was compromised, identity theft repair, etc.;
- Costs of the forensic investigation in order to determine the causes of the data breach.

LEGAL ACTION

Lawsuits against your company can be a common outcome. In 2007, TJX Companies (best known as the holder of Marshalls and T.J. Maxx) had to pay $40.9 million for a data breach which put an estimated 100 million bank cards at risk. In 2014, 1.1 million clients of Neiman Marcus were affected by another data breach.

DAMAGED REPUTATION

Putting clients' bank card information at risk can result in irreversible damage to a **company's reputation**; this is in addition to any of the elevated costs that would be incurred by the organization. Once your security has been endangered, it will be very difficult for your clients to start trusting you again.

REVENUE LOSS

In addition to loss of brand reputation, a merchant can expect their revenue to drop drastically due to the loss of clients followed by a security breach. In 2013, Target was sentenced to $18.4 million for a data breach that affected more than 41 million customers. This led the merchant to a $440-million-loss of revenue in the first quarter following the breach.

* Source: https://blog.repay.com/5-consequences-to-pci-non-compliance

SUGGESTION FOR PCI COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in PCI DSS that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two Compliance Firms (shown below) to make sure your organization fully complies with this law.

HIPAA	Health Insurance Portability & Accountability Act	Yes

FINDING: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the creation of national standards to protect sensitive **patient health information** from being disclosed without the patient's consent or knowledge. The law is broken up into two main pieces: **Privacy** and **Security**. Entities that fall under this law are:

Healthcare providers: Every healthcare provider, **regardless of the size** of practice, who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has established standards under the HIPAA Transactions Rule.

Health insurers/plans: Entities that provide or **pay the cost** of medical care. Health plans include health, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies).

Healthcare clearinghouses: Entities that **process** nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.

Business associates: A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include **claims processing**, data analysis, utilization review, and **billing**.

As a healthcare provider or associate, complying with HIPAA is critical. In the questionnaire, you indicated that your confidence level with your current HIPAA compliance is a 2 out of 10. It sounds like there is a lot of room for improvement. Below we've compiled some information to help you understand exactly what HIPAA is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help put together a great HIPAA compliance plan for you.

HIPAA COMPLIANCE CHECKLIST: The US Department of Health and Human Services (HHS) issued the HIPAA **Privacy Rule** to implement the requirements of HIPAA. The HIPAA **Security Rule** protects a subset of information covered by the Privacy Rule. The details of each of these regulations can be found on the U.S. Centers for Disease Control: Public Health Professionals website: https://www.cdc.gov/phlp/publications/topic/hipaa.html

Below we've summarized your responsibilities for easy reading:

HIPAA Privacy Rule*

The Privacy Rule standards address the use and disclosure of individuals' health information (known as "protected health information") by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities." The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used.

Permitted Uses and Disclosures: A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

- **Disclosure to the individual** (if the information is required for access or accounting of disclosures, the entity MUST disclose to the individual)
- **Treatment**, **payment**, and healthcare **operations**
- **Opportunity to agree or object** to the disclosure of PHI (Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object)
- **Public interest and benefit activities**—The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes external icon:
- When required by **law**
- **Public health** activities
- **Victims of abuse** or neglect or domestic violence
- **Health oversight** activities
- **Judicial** and administrative proceedings
- **Law enforcement**
- Functions (such as identification) concerning **deceased persons**
- Cadaveric organ, eye, or tissue **donation**
- **Research**, under certain conditions
- To **prevent** or lessen a **serious threat** to health or safety

- **Essential government functions**
- **Workers compensation**
- Limited dataset for **research**, public health, or healthcare operations

HIPAA Security Rule

This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing. To comply with the HIPAA Security Rule, all covered entities must do the following:

- Ensure the **confidentiality**, **integrity**, and **availability** of all electronic protected health information
- Detect and **safeguard** against **anticipated threats** to the security of the information
- Protect against anticipated **impermissible uses** or disclosures
- **Certify compliance** by their workforce

Covered entities should rely on professional ethics and best judgment when considering requests for these permissive uses and disclosures. The HHS Office for Civil Rights enforces HIPAA rules, and all complaints should be reported to that office. HIPAA violations may result in civil monetary, or criminal penalties.

* Source: https://www.cdc.gov/phlp/publications/topic/hipaa.html

HIPAA VIOLATIONS: The HHS Office for Civil Rights enforces HIPAA rules, and all complaints should be reported to that office. HIPAA violations may result in civil monetary or criminal penalties. A violation may be deliberate or unintentional. An example of an unintentional HIPAA violation is when too much PHI is disclosed, and the minimum necessary information standard is violated.

Consequences for violating HIPAA

Penalties for HIPAA violations can be issued by the Department of Health and Human Services' Office for Civil Rights (OCR) **and** state attorneys general. In addition to **financial penalties**, covered entities are required to adopt a **corrective action plan** to bring policies and procedures up to the standards demanded by HIPAA.

HIPAA VIOLATION CLASSIFICATIONS*

TIER 1	**Lack of Knowledge**. A violation that the covered entity was unaware of and could not have realistically avoided had a reasonable amount of care had been taken to abide by HIPAA Rules
TIER 2	**Reasonable Cause.** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
TIER 3	**Willful Neglect.** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation
TIER 4	**Willful Neglect (not corrected within 30 days).** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

*In the case of unknown violations, where the covered entity could not have been expected to avoid a data breach, it may seem unreasonable for a covered entity to be issued with a fine. OCR appreciates this and has the discretion to waive a financial penalty. The penalty cannot be waived if the violation involved willful neglect of the Privacy, Security, and Breach Notification Rules.

HIPAA VIOLATION PENALTY STRUCTURE*

Each category of violation carries a separate HIPAA penalty. It is up to OCR to determine a financial penalty within the appropriate range. OCR considers a number of factors when determining penalties, such as the length of time a violation was allowed to persist, the number of people affected, and the nature of the data exposed.

TIER 1	Minimum fine of **$100** per violation up to **$50,000**
TIER 2	Minimum fine of **$1,000** per violation up to **$50,000**
TIER 3	Minimum fine of **$10,000** per violation up to **$50,000**
TIER 4	Minimum fine of **$50,000** per violation

The above fines for HIPAA violations are those stipulated by the HITECH Act. It should be noted that these are adjusted annually to take inflation into account.

* Source: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

A fine may also be applied on a **daily basis**. For example, if a covered entity has been denying patients the right to obtain copies of their medical records, and had been doing so for a period of one year, the OCR may decide to apply a penalty per day that the covered entity has been in violation of the law. The penalty would be multiplied by 365, not by the number of patients that have been refused access to their medical records

Attorneys General Can Also Issue HIPAA Violation Fines

Since the introduction of the HITECH Act (Section 13410(e) (1)) in February 2009, **state attorneys general have the authority** to hold HIPAA-covered entities accountable for the exposure of the PHI of state residents and can file civil actions with the federal district courts. HIPAA violation fines can be issued up to a **maximum level of $25,000** per violation category per calendar year. The **minimum** fine applicable is **$100 per violation**.

Can HIPAA Violations be Criminal? (YES!)

Criminal Liability. When a HIPAA-covered entity or business associate violates HIPAA Rules, civil penalties can be imposed. When healthcare professionals violate HIPAA, it is usually their employer that receives the penalty, but not always. If healthcare professionals knowingly obtain or use protected health information for reasons that are not permitted by the HIPAA Privacy Rule, they **may be found to be criminally liable** for the HIPAA violation under the criminal enforcement provision of the Administrative Simplification subtitle of HIPAA.

Criminal HIPAA violations are prosecuted by the Department of Justice, which is increasingly taking action against individuals that have knowingly violated HIPAA Rules. There have been several cases that have resulted in substantial fines and prison sentences.

Criminal HIPAA violations include theft of patient information for financial gain and wrongful disclosures with intent to cause harm. A lack of understanding of HIPAA requirements may not be a valid defense. When an individual "knowingly" violates HIPAA, knowingly means that they have some knowledge of the facts that constitute the offense, not that they definitely know that they are violating HIPAA Rules.

Criminal Penalties for HIPAA Violations*

Criminal penalties for HIPAA violations are divided into three separate tiers, with the term – and an accompanying fine – decided by a judge based on the facts of each individual case. As with OCR, a number of general factors are considered which will affect the penalty issued. The tiers of criminal penalties for HIPAA violations are:

TIER 1	Reasonable cause or no knowledge of violation – **Up to 1 year in jail**
TIER 2	Obtaining PHI under false pretenses – **Up to 5 years in jail**
TIER 3	Obtaining PHI for personal gain or with malicious intent – **Up to 10 years in jail**

* Source: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

SUGGESTION FOR HIPAA COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in HIPAA that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two Compliance Firms (shown below) to make sure your organization fully complies with this very important law.

NIST800	NIST Special Publication 800-53	Yes

FINDING: The NIST 800 series is a set of documents that describe United States federal government policies, procedures, and guidelines for information system security. The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL, 800-53 was developed by the Joint Task Force Interagency Working Group. The group includes representatives from the civil, defense, and intelligence communities.

The use of NIST 800-53 controls is mandatory for federal information systems in accordance with the Office of Management and Budget (OMB) and the provisions of the Federal Information Security Modernization Act [FISMA], which requires the implementation of minimum controls to **protect federal information** and information systems.

As a U.S. **federal government contractor**, you need to comply with the NIST 800-53 risk management framework.

In the questionnaire, you indicated that your confidence level with your current NIST 800-53 compliance is a 5 out of 10.It sounds like you're content but not comfortable with your current standing and may be looking for ways to improve. Below we've compiled some information to help you understand exactly what NIST 800-53 is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help you put together an improved NIST 800-53 compliance strategy.

NIST 800-53 COMPLIANCE CHECKLIST: NIST 800-53 has 20 families of controls comprising over 1,000 separate controls. Each family is related to a specific topic, such as access control. The details of each of these regulations can be found on the NIST website: https://www.nist.gov/

The entire NIST 800-53 risk management framework whitepaper can be downloaded here: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Security and Control Families

NIST 800-53 controls are allocated into the following 20 families:

ID	Family Name	Examples of Controls
AC	Access Control	Account management and monitoring; least privilege; separation of duties
AT	Awareness and Training	User training on security threats; technical training for privileged users
AU	Audit and Accountability	Content of audit records; analysis and reporting; record retention
CA	Assessment, Authorization, and Monitoring	Connections to public networks and external systems; penetration testing
CM	Configuration Management	Authorized software policies, configuration change control
CP	Contingency Planning	Alternate processing and storage sites; business continuity strategies; testing
IA	Identification and Authentication	Authentication policies for users, devices and services; credential management
IP	Individual Participation	Consent and privacy authorization
IR	Incident Response	Incident response training, monitoring and reporting
MA	Maintenance	System, personnel and tool maintenance
MP	Media Protection	Access, storage, transport, sanitization, and use of media
PA	Privacy Authorization	Collection, use and sharing of personally identifiable information (PII)
PE	Physical and Environment Protection	Physical access; emergency power; fire protection; temperature control
PL	Planning	Social media and networking restrictions; defense-in-depth security architecture
PM	Program Management	Risk management strategy; insider threat program; enterprise architecture
PS	Personnel Security	Personnel screening, termination and transfer; external personnel; sanctions
RA	Risk Assessment	Risk assessment; vulnerability scanning; privacy impact assessment

SA	System and Services Acquisition	System development lifecycle; acquisition process; supply chain risk management
SC	System and Communications Protection	Application partitioning; boundary protection; cryptographic key management
SI	System and Information Integrity	Flaw remediation; system monitoring and alerting

Tips for NIST 800-53 Compliance

The following best practices will help you select and implement appropriate security and privacy controls for NIST SP 800-53 compliance.

- **Identify your sensitive data.**
  Find out what kind of data your organization deals with, where it is stored, and how it is received, maintained, and transmitted. Sensitive data can be spread across multiple systems and applications; it is not necessarily only where you think it is.

- **Classify sensitive data.**
  Categorize and label your data according to its value and sensitivity. Assign each information type an impact value (low, moderate, or high) for each security objective (confidentiality, integrity, and availability), and categorize it at the highest impact level. Consult FIPS 199 for appropriate security categories and impact levels that relate to your organizational goals, mission, and business success. Automate discovery and classification to streamline the process and ensure consistent, reliable results.

- **Evaluate your current level of cybersecurity with a risk assessment.**
  At a high level, risk assessment involves identifying risks, assessing the probability of their occurrence and their potential impact, taking steps to remediate the most serious risks, and then assessing the effectiveness of those steps.

- **Document a plan to improve your policies and procedures.**
  Select controls based on your specific business needs. The extent and rigor of the selection process should be proportional to the impact level of the risk being mitigated. Document your plan and the rationale for each choice of control and policy.

- **Provide ongoing employee training.**
  Educate all employees on access governance and cybersecurity best practices, such as how to identify and report malware.

- **Make compliance an ongoing process.**
  Once you have brought your system into compliance with NIST 800-53, maintain and improve your compliance with regular system audits, especially after a security incident.

SUGGESTIONS FOR NIST 800-53 COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in NIST 800-53 that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two NIST 800-53 Compliance Firms (shown below) to make sure your organization fully complies with this very important law.

CMMC	Cybersecurity Maturity Model Certification	Yes

FINDING: The CMMC is an amalgam of multiple frameworks and standards, including NIST SP 800-171, the NIST Cybersecurity Framework, ISO 27001, and others. Developed by the DoD in conjunction with academia (Carnegie Mellon and Johns Hopkins Universities), the CMMC leverages a combination of practices (what most CSPs will recognize as controls) and processes that gauge the maturity level of a given practice.

Recognizing that not all contractors need to have the same cybersecurity program maturity as a prime, the DoD will include which of the five maturity tiers a given contract will require at the time of a request of information (RFI).

A contractor's tier score will be assessed and audited via third-party CMMC assessments

and auditors. These third-party assessment organizations will be appointed by the CMMC Accreditation Board, and the CMMC certification for a given tier will last for three years.

As a **government contractor**, you need to comply with CMMC.

In the questionnaire, you indicated that your confidence level with your current CMMC compliance is a 5 out of 10. It sounds like you're content but not comfortable with your current standing and may be looking for ways to improve. Below we've compiled some information to help you understand exactly what CMMC is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help you put together an improved CMMC compliance strategy.

WHAT IS THE CMMC FRAMEWORK? The CMMC framework is composed of 17 domains, with each tier layering in more practices and processes for each domain. In this infographic, we'll be taking a high-level view of each of the domains and what to expect when working to meet your CMMC requirements.

CMMC Framework*

- **Access Control**
  This domain requires your organization to establish who has access to your systems and what their requirements are to operate effectively. As well who has remote access, internal system access, and the limitations of their roles in the system.

- **Asset Management**
  This domain asks that you locate, identify, and log inventory of the assets to your organization.

- **Audit & Accountability**
  This domain requires that you have a process in place for tracking users that have access to your organization's CUI and performing audits of those logs to ensure they are held accountable for their behavior. You will need to define the requirements of each audit, have a method to perform the audit, protect and secure the results of that audit and manage audit logs.

- **Awareness & Training**
  This domain requires that you have training programs in place for all personnel and conduct security awareness activities.

- **Configuration Management**
  This domain asks that you establish configuration baselines as a measure to judge the efficiency of your systems. This is necessary to conduct audits and accurately measure the posture of your systems.

- **Identification & Authentication**
  This domain ensures the proper roles within your organization have the correct level of access and can be authenticated for reporting and accountability purposes.

- **Incident Response**
  For this domain, your organization will need an Incident Response Plan. The ability to detect and report events, develop and implement response to a declared incident, perform post-incident reviews and test your response in an effort to measure your entity's preparedness in the event of a cyber attack.

- **Maintenance**
  This domain requires you to have a maintenance system in place to maintain and effectively operate your systems.

- **Media Protection**
  For this domain, your organization will need to prove it has its media identified and appropriately marked for ease of access. Additionally, it asks that you provide evidence of a media protection protocol, sanitation protocol, and transportation protection in place.

- **Personnel Security**
  Your personnel will have to have been properly screened and have background checks run. Also, you will need to provide evidence that your CUI is protected during personnel activity such as employee turnover or transfer.

- **Physical Protection**
  Your organization will need to provide evidence of the physical security surrounding your assets and prove that they are protected.

- **Recovery**
  This domain requires that you keep and log backups of media necessary to your organization. These need to be logged for the purpose of continuity among backups and mitigate lost data.

- **Risk Management**
  Risk Management is the process of identifying and evaluating the risk that affects your company using periodic risk assessments and vulnerability scanning. This includes your own organization's risk as well as that of your vendors.

- **Security Assessment**
  For this domain, you will need a system security plan in place. Additionally, you will need to define and manage controls and perform code reviews for your organization.

- **Situational Awareness**
  You will need evidence of a threat monitoring system. This helps supplement other domains and keeps your organization secure in the event of a cyber incident.

- **System & Communication Protection**
  You will need to define the security requirements of each system and communication channel your organization uses to provide evidence your organization has control of communications at system boundaries.

- **System & Information integrity**
  System and information integrity require you to identify and manage flaws within your system, identify hazardous and malicious content in-system, implement email protections and monitor your network and system.

* Source: https://www.cybersaint.io/blog/cmmc-domains-explained

SUGGESTION FOR CMMC COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in CMMC that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two CMMC Compliance Firms (shown below) to make sure your organization fully complies with this very important law.

DFARS	Defense Federal Acquisition Regulation Supplement	Yes

FINDING: The Defense Federal Acquisition Regulation Supplement (DFARS) is a set of cybersecurity regulations that the **Department of Defense** (DoD) now imposes on external contractors and suppliers. The DFARS is intended to maintain cybersecurity standards according to requirements laid out by the National Institute of Standards and Technology (NIST), specifically NIST SP 800-171.

These standards were constructed to protect the confidentiality of CUI ("Controlled Unclassified Information") and had given DoD contractors until December 31, 2017, to meet the requirements necessary to be classified as DFARS compliant. Failure to meet these requirements could have resulted in the loss of current DoD contracts. All DoD contractors must meet the minimum requirements and show proof to the Department of Defense for all contracts moving forward.

As a **Department of Defense contractor**, you need to comply with DFARS.

In the questionnaire, you indicated that your confidence level with your current DFARS compliance is a 2 out of 10. It sounds like there is a lot of room for improvement. Below we've compiled some information to help you understand exactly what DFARS is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help put together a great DFARS compliance plan for you.

WHAT ARE THE MINIMUM REQUIREMENTS FOR DFARS? Currently, to be certified DFARS compliant, a business must pass a readiness "self-assessment" that proves compliance to NIST 800-171. Typically, it takes an organization anywhere from 6-10 months to complete the process and requires submission of documentation to the DoD as well as the possibility of a DoD audit. On the horizon, however, is a new, tiered certification system that will function similarly to ISO certification procedures involving 3rd party auditing, etc.

The entire certification standard can be found here: https://www.acquisition.gov/dfars

DFARS Compliance Checklist

DFARS compliance is issued to companies that prove they meet NIST 800-171 via an extensive self-study. When the self-study is completed, the document is submitted to the DoD. The DoD might also perform an audit at random as well. There are 14 requirements that must be met and properly documented:

- **Regulate Access Control:** Access must be limited to authorized users. This simply means that you are giving your employees just enough access to CUI to conduct their daily job tasks, nothing more and nothing less.

- **Ensure Awareness and Training:** Adequate security training to all employees must be provided on a regular basis, by following a regimented time schedule, such as monthly, quarterly, or semi-annually. Obviously, the more training you can provide, the better. The training must include everybody, from C-Level Executives down to administrative assistants.

- **Ensure Audit and Accountability Controls:** Have appropriate controls in place in order to prevent, investigate and mitigate any malicious activity. This would include monitoring Firewalls, Network Intrusion Devices, Routers, and other security devices you have deployed to fortify your cyber defense, as well as responding to warnings or alerts from such systems.

- **Maintain a Configuration Management System:** All "baseline configurations" of IT systems must be documented. For example, when you deploy any new security tools, the IT security staff must document the initial configurations. Over time, this is expected to change, and any new configuration updates must be included in this documentation as well throughout the lifecycle of the security tools.

- **Implement Adequate Identification and Authentication Systems**: Any user trying to gain logical access must be positively authenticated. In other words, you must make sure that an employee requesting access is who they claim to be. This is done by deploying Multi-factor Authentication (MFA) systems, such as passwords, challenge-response questions, RSA tokens, Biometric Technology, etc.

- **Enforce an Incident Response Plan:** Your company must implement a plan detailing how potential incidents will be documented and mitigated and practice this plan at regular time intervals. The timing of this can be either quarterly or semi-annually at the minimum.

- **Establish a Regular Maintenance Schedule:** All IT systems must be properly maintained and operating in optimal condition. Checks should be done daily, using software automation packages and IT staff monitoring that keeps track of the health of your entire IT infrastructure in real-time.

- **Protection of Media Devices:** Any media device issued to or used by your employees must be adequately protected. For example, if you issue portable storage devices to your employees, the device must have enough layers of encryption embedded so that any CUI will be rendered useless (in an indecipherable format) if this device is lost or stolen, or somehow falls into the hands of a malicious third party.

- **Conduct Extensive Background Checks:** Potential new employees must pass an extensive background check. The level of background check should include at minimum a deep investigation into any previous criminal activity. Drug screenings should also be included in the background check.

- **Enforce Adequate Physical Access Protection:** Ensure that only authorized personnel and registered visitors are allowed onto the actual physical premises of the business. This includes securing all entrances to facilities, implementing a visitor registration system, etc. Like controlling logical access, this involves positively confirming the identity of the individual in question, whether through smart cards, Biometric Technology, etc.

- **Maintain a Regular Risk Assessment Schedule:** A schedule must be in place so that IT systems can be audited on a regular basis. The primary goal here is to scan for any vulnerabilities, gaps, or weaknesses that may reside in any information system, and if detected, action is taken to rectify the issues.

- **Implement a Security Assessment Schedule:** You must conduct regular audits on all IT controls that are in place to safeguard the CUI. The timeframe should be on a monthly, or at minimum, on a quarterly basis.

- **Enforce a Communications Protection System:** All lines of communication, both internal and external to the business, must be secure. For example, if you employ remote workers or third-party contractors, they should be issued equipment that already has safeguards in place in order to ensure that any information and data that is transmitted is encrypted. Also, there should be controls in place on this equipment that can confirm the integrity of any transmitted message after it has been sent to the receiver and vice versa.

- **Establish a System and Information Integrity Check:** You must ensure that the IT Staff is monitoring and responding to any alerts and notifications. In other words, any warning messages that are transmitted from security tools should be addressed on a proactive basis, and any alerts that are deemed critical in nature must be attended to immediately, as well as any remediative efforts required to resolve the situation.

* Source: https://evestigate.com/dfars-compliance-and-certification/

Maintaining your DFARS Certification

Once your organization has achieved DFARS compliance, steps must be taken such that compliance is maintained. This is accomplished by:

- **The Establishment of a Governance Program:** This involves conducting a thorough gap analysis of your existing IT Infrastructure and identifying/correcting any hidden weaknesses that have been discovered.

- **The Implementation of a Data Classification Strategy:** Once you get access to CUI that the DoD shares with you, your organization must develop a classification scheme for it.

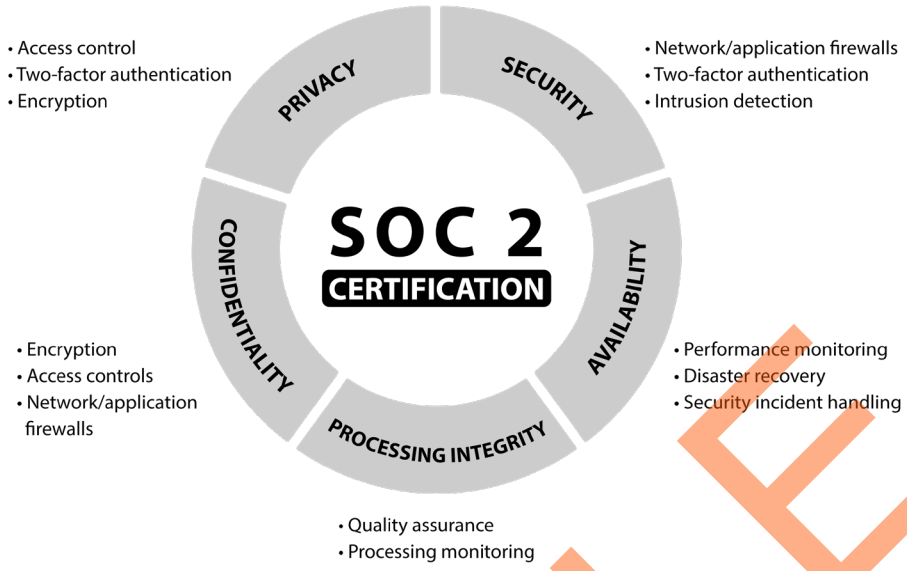
- **Cloud Usage:** If you store the datasets in the Cloud, you must prove to the DoD that you have a well-crafted, implemented security plan.

SUGGESTION FOR DFARS COMPLIANCE: Finally, we want to remind you that this assessment is not legal advice. There are dozens of provisions in DFARS that apply only in rare instances, which would be counterproductive to cover here. We advise that you check with the two DFARS Compliance Firms (shown below) to make sure your organization fully complies with this very important law.

SOC2	**Service Organization Control 2 (SOC2)**	**Yes**

FINDING: Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy.

Specifically, SOC 2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your organization and the privacy of its clients. For security-conscious businesses, SOC 2 compliance is a minimal requirement **when considering a SaaS provider**.



Unlike PCI DSS, which has very rigid requirements, SOC2 reports are unique to each organization. In line with specific business practices, each designs its own controls to comply with one or more of the trust principles.

If you are a SaaS provider and want to engender trust with your user base, you should consider getting SOC2 certified.

In the questionnaire you indicated that your confidence level with your current SOC2 compliance is a 2 out of 10. It sounds like there is a lot of room for improvement. Below we've compiled some information to help you understand exactly what SOC 2 is, how to get (and stay) in compliance, the penalties for non-compliance, and we finish with a list of MSPs who can help put together a great SOC 2 compliance plan for you.

WHAT ARE THE REQUIREMENTS FOR SOC 2? SOC 2 certification is issued by outside auditors. They assess the extent to which a vendor complies with one or more of the five trust principles based on the systems and processes in place.

The entire certification standard can be found here: https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations

SOC 2 Certification

Trust principles are broken down as follows:

Security

The security principle refers to protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information. IT security tools such as network and web application firewalls (WAFs), two-factor authentication, and intrusion detection are useful in preventing security breaches that can lead to unauthorized access of systems and data.

Availability

The availability principle refers to the accessibility of the system, products, or services as stipulated by a contract or service level agreement (SLA). As such, the minimum acceptable performance level for system availability is set by both parties. This principle does not address system functionality and usability but does involve security-related criteria that may affect availability. Monitoring network performance and availability, site failover, and security incident handling are critical in this context.

Processing integrity

The processing integrity principle addresses whether or not a system achieves its purpose (i.e., delivers the right data at the right price at the right time). Accordingly, data processing must be complete, valid, accurate, timely, and authorized. However, processing integrity does not necessarily imply data integrity. If data contains errors prior to being input into the system, detecting them is not usually the responsibility of the processing entity. Monitoring of data processing, coupled with quality assurance procedures, can help ensure processing integrity.

Confidentiality

Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organizations. Examples may include data intended only for company personnel, as well as business plans, intellectual property, internal price lists, and other types of sensitive financial information. Encryption is an important control for protecting confidentiality during transmission. Network and application firewalls, together with rigorous access controls, can be used to safeguard information being processed or stored on computer systems.

Privacy
The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information in conformity with an organization's privacy notice, as well as with criteria set forth in the AICPA's generally accepted privacy principles (GAPP). Personally identifiable information (PII) refers to details that can distinguish an individual (e.g., name, address, Social Security number). Some personal data related to health, race, sexuality, and religion is also considered sensitive and generally requires an extra level of protection. Controls must be put in place to protect all PII from unauthorized access.

* Source: https://www.imperva.com/learn/data-security/soc-2-compliance

What happens during the SOC 2 audit?*

Before the audit, your auditor will likely work with you to set up an audit timeframe that works for both parties. They may also talk you through the audit process. This will ensure that you know what to expect. The auditor may even ask for some initial information to help things go more smoothly. Once they arrive, here's the general process:

1. **The security questionnaire**
   Many auditing firms start by administering a questionnaire to you and your team. This contains many questions regarding company policies, procedures, IT infrastructure, and controls. Getting your team into good security habits as early as possible before the audit helps out here. They'll be able to answer questions with confidence.

2. **Gathering evidence of controls**
   Next, auditors will ask your team to furnish them with evidence and documentation regarding the controls within your organization. You need proof of every policy and internal control to demonstrate that things are up to par. The auditors use this as part of their evaluation to understand how controls are supposed to work.

3. **Evaluation**
   During the evaluation, the auditors might ask the owners of each process within your SOC 2 audit scope to walk them through your business processes to understand them better.

4. **Follow-Up**
   SOC 2 audits are intensive. As a result, auditors often uncover matters for which they need more evidence, despite all the prep work. They may ask your team for clarification on processes or controls, or they may want additional documentation.

In some cases, if the auditor notices obvious compliance gaps that can be fixed relatively quickly, they could ask you to remedy those before proceeding. The auditors will document their visit as well, just in case, further follow-up is needed.

5. The SOC 2 report

When the audit concludes, the auditing firm will issue you a SOC 2 audit report. There is no formal SOC 2 certification. Instead, the main portion of the report contains the auditor's opinion regarding the effectiveness of your internal controls as they pertain to your specified trust principles.

* Source: https://secureframe.com/blog/soc-2-audit-checklist

SUGGESTIONS FOR SOC 2 COMPLIANCE: You have a lot ahead of you when preparing for your SOC 2 audit. It will take a significant investment of time, money, and mental energy. However, following the steps laid out in this checklist can make that journey a little clearer. However, if you'd like hands-on guidance and a consultant that cuts your prep time from months to weeks, we have two that can help:
