GRF's Cybersecurity Guide

Risks & Mitigation Strategies

CPAs & ADVISORS

Contact Us

Melissa Musser
CPA, CITP, CISA
Partner, Risk & Advisory Services
mmusser@grfcpa.com

Darren Hulem
CISA, CEH, Security+
Supervisor, IT and Risk Advisory Services
dhulem@grfcpa.com

Data Security Should Be a Top Priority

Remote work has exposed existing cybersecurity vulnerabilities and created new ones. How is your organization responding?

In this eBook, we provide detail on 20 different risk categories that can impact your organization. For each risk category, we explain the potential weaknesses and vulnerabilities risks that exist and how to identify them in your systems.

These risks are assessed in GRF's Cybersecurity Risk Assessment and Scorecard, a tool that provides a baseline diagnostic to help you analyze your organization's risk and develop an appropriate compliance strategy.

You may be surprised to discover you already have the right tools – you just need to leverage them properly.

Categories of Risk

Safeguard

- Digital Footprint
- Patch Management
- Application Security
- CDN Security
- Website Security

Resiliency

- Attack Surface
- DNS Health
- Email Security
- DDoS Resiliency
- Network Security

Privacy

- SSL/TLS Strength
- Credential Management
- Hacktivist Shares
- Social Network
- Information Disclosure

Reputation

- Brand Monitoring
- IP Reputation
- Fraudulent Applications
- Fraudulent Domains
- Web Ranking

CPAs & ADVISORS

Safeguard

Digital Footprint: What do people see about your organization?

It's crucial for your organization to have an online presence to effectively communicate your brand and your mission. However, you may not be aware of everything that people can see. If end-users are not able to find your organization online – or they find misleading, incorrect, or damaging information – your organization's reputation is at risk. Further, you can be liable for the items you own online.

How do you know if you are at risk? Assessing your digital footprint is an essential first step.

What makes up your digital footprint?

For an organization, a digital footprint is comprised of all the information that can be found online that is associated with your organization's domain name. Many items make up your digital footprint and understanding them is a key step in understanding your cyber posture. Online data is associated with your organization's digital footprint through several unique identifiers:

IP Address – An IP (internet protocol) address is a numerical label assigned to each device connected to a computer network, so devices online can find and send data to one another. IP addresses use the same principle as a street address, so there can only be one address per device, and it must be unique.

Domain – a domain name is a text version of an IP address, making it easier for humans to recognize. For example, it is easier to remember www.GRFCPA.com than 35.227.184.45. A domain can be the name of your website and it can also be everything after the "@" symbol in your email address.

Subdomain – an independent extension of a main domain. For example, if you have an email associated with your domain name, it might use email.yourdomainname.org. They are a part of your main website but found separately by search engines.

DNS Records – the Domain Name System maps a user-friendly web address to its IP address. The DNS routes end users to your website or application by translating the website name (like www.grfcpa.com) into an IP address, and then making the connection.

Patch Management: Eliminating Vulnerabilities

The threat of cyberattacks is frightening, persistent, and can affect any organization, big or small. One way to mitigate this risk is to be sure your computer software and operating systems are up to date. Software vendors regularly release system updates, or "patches," which are designed to improve the security of a system and protect against vulnerabilities.

A 2019 study done by ServiceNow and the Ponemon Institute found that 60 percent of data breaches were due to failure to apply patches for known vulnerabilities. In short, the breaches could have been prevented by conducting regular updates.

In fact, the massive data breach at Equifax in 2017 happened because a widely known vulnerability was not patched. Equifax did not have a policy in place to update their systems. Thus, hackers were able to access Equifax's web portal and other network servers and download large amounts of personal customer information.

Similarly, it's crucial to review your organization's IT assets. Old servers that are no longer supported can give attackers an entry point into your network. If your organization still uses older versions of Microsoft or Linux, then you are susceptible to attacks. For example, Microsoft announced in 2020 that it is no longer supporting the Windows 7 operating system with software updates.

Best Practices and Processes for Patch Management

1. To protect your systems, it is crucial to follow best practices and constantly evaluate your cybersecurity posture.
2. Account for all assets that are on your network.
3. Read the description of the released patch to understand its importance. Does it improve functionality or patch a critical vulnerability?
4. When deploying the patch, first run it on a test system that is identical to your active servers. This will allow you to identify any issues with the update.
5. Before deploying the patch to all your systems, identify a small number of systems to deploy it to, then deploy the rest in stages. The rollout of critical security patches should occur quickly while testing functionality updates can roll out at a slower pace.
6. Make sure your organization has a backout plan to allow for back out of the patch and return to previous operations in case the patch negatively impacts the network.
7. Document patches that you are deploying, the importance of them, and any issues you notice.
8. Stay up to date with patch releases. Account for the most common day of software releases.
9. Continuously monitor your systems to ensure that vulnerabilities are accounted for.

Application Security: Are you protecting important information on your website?

Web applications are a top target for attackers. Hackers are constantly searching the web to find common vulnerabilities that they can use to exploit your website and data. Not having the proper security controls in place can result in an attacker bypassing authorization controls to steal confidential information. To protect your organization, it is crucial to identify and mitigate these vulnerabilities.

Verizon conducted a Data Breach Investigation Report, which found that over 80 percent of hacks came through web application vulnerabilities.

Common Risks and Vulnerabilities

Cross-Site Request Forgery – Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

> *It is also important to talk with your IT or web provider to make sure they are regularly checking these items to make sure they are implemented.*

Clear Text Transmission of Sensitive Information – Communication via the internet can be intercepted easily depending on what network or WiFi you are connected to, especially on public resources such as airports, coffee shops, hotels, etc. Anyone else connected to the same network as you can see or "sniff" your internet traffic. Clear text or HTTP traffic is not encrypted and can be viewed by others. Encrypted traffic (HTTPS) is much more difficult to decipher.

Missing Encryption of sensitive data before storage or transmission – Encryption of sensitive data is extremely important. Is important to know that, just like other technologies, encryption protocols become obsolete and new ones are developed to ensure data is secure. Old, outdated encryption methods give end users a false sense of security. The data is encrypted but it does not secure the data because there are proven methods to decrypt the data.

Mitigating the Risks

While cybersecurity is a holistic approach, there are areas within application security that can be bolstered to minimize the opportunity for a breach. Our recommendations for remediation of common high-risk items include:

1. Always use strong encryption on web applications that require authentication or host sensitive information.
2. Avoid mixing HTTP and HTTPS content. HTTP is not secure and is vulnerable to attacks.
3. Detect and block excessive login or submission attempts. These attempts could be bots that are configured to take down your system with excess requests. Consider putting in a captcha request, so the user must verify that they are not a robot before entering.
4. Consider applying Security Headers to web applications. Security headers are a key piece in website security and protect against a lot of common attacks.

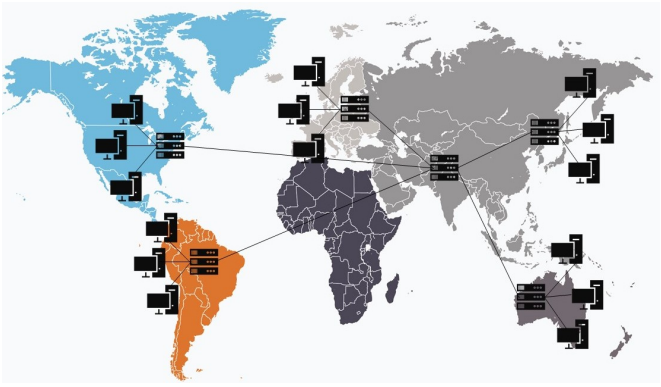
Implementing these approaches to risks can develop a better cyber posture. It is also important to talk with your IT or web provider to make sure they are regularly checking these items to make sure they are implemented.

Content Delivery Network (CDN) Security: What are the risks?

Organizations use their online presence to attract donors, members, and clients from around the globe – often using videos, pictures, and interactive resources to engage these visitors. It is essential for web pages and content to load quickly because delays in load time could mean the loss of a potential client or donor.

Content delivery networks (CDNs) speed upload times. CDNs are geographically distributed servers that work together to provide web content quickly to end users. The network essentially houses copies of a website and its content in multiple data center locations, reducing the load on one server.

CDNs have many benefits. Not having your web content all on one server mitigates the risk of a Distributed Denial of Service (DDoS) attack – when hackers crash a server by sending it a huge volume of traffic all at once. CDNs can also provide important disaster recovery measures. If one server is out of service, the CDN can re-route traffic to other servers. CDNs can also reduce your web hosting costs, as they are set up to optimize the content for distribution, reducing bandwidth.



Common Risks and Vulnerabilities

CDNs are not without risks however, particularly related to the reputation and management of the systems they use.

If your CDN uses a data center that is associated with frequent suspicious behavior, your IP address may be deemed suspicious, even if you've done nothing wrong. Sites like Facebook, Amazon, and many email servers use IP blacklists to protect their users from possible cyberattack or fraud. Having a bad IP or domain reputation can cause your website, emails, and any associated online assets to be blocked entirely by some services.

Further, a CDN using unpatched or outdated systems is vulnerable to attack, making your website and online assets vulnerable too.

Website Security: Is your front door open?

Identifying and mitigating website risks

Data breaches are costly, and the monetary risk is massive. According to a recent IBM report, the average total cost of a data breach in the U.S. is $8.64 million, but even a smaller number can be devastating, depending on the size of your organization. The risk to reputation and loss of trust from your users may be just as damaging and more difficult to restore.

Threat actors will often try to attack through the front door – the homepage of your website. They know they can cause reputation damage if they can access the webpage and deface it or inflict operational damage if they can disrupt your site's functionality.

The nature of cyberattacks is always changing, requiring constant vigilance to monitor what vulnerabilities you have and address potential problems. Do you have the tools you need to secure your website from attacks?

What types of attacks are a threat?

The threat of being attacked by a cyber-criminal has been increasing every year. There are various ways that an attacker may utilize the weaknesses on your website to exploit both your organization and its users. Some common types of attacks include:

Cross-Site Request Forgery – This happens when applications rely only on HTTP (unencrypted) cookies to identify a user request. This creates an opportunity for an attacker to utilize social engineering (like sending a link via chat) to a user. Clicking on the link enables the attacker to execute actions under the guise of that user – often without the user's knowledge. This could allow the attacker to perform state-changing requests such as transferring funds or changing the user's email address.

SQL Injection – This allows for an attacker to run a SQL statement to inject code into your website without you knowing. This typically occurs within places that ask for user input like a user ID/ password field. Through the code they run, they may be able to access your database and gain the usernames/password of users in your organization.

Brute Force Attack – Simply put, this is a trial and error method to guessing login information for a site. If your website does not have a limit on the number of times a user can enter credentials, then the attacker will be able to input as many username/password combinations as they want and try to gain access to your site.

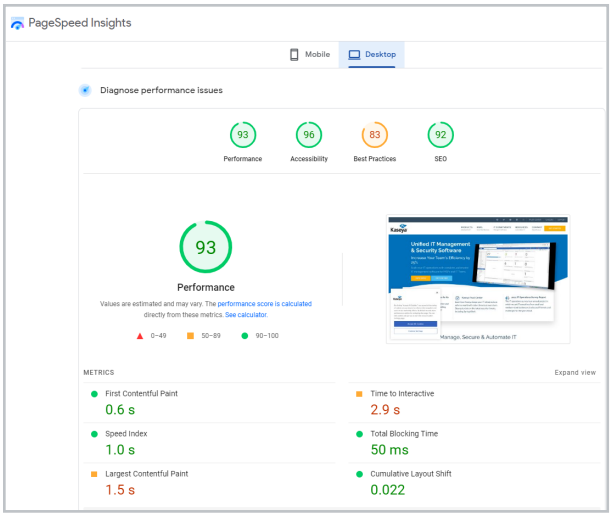
What elements should you monitor?

At GRF, we recommend you review several performance and security risk areas on your website:

SSL/TLS Strength – On your web browser, secured sites are indicated by a lock icon next to the web address. This indicates that the website is secure and is using encryption methods when exchanging and transporting data. User data needs to be protected to avoid attackers from stealing the contents being provided to the website. You should evaluate the SSL/TLS strength of your site against best practices to identify areas for improvement. Some common errors include missing an SSL certificate, not having the correct TLS version enabled, or using outdated cipher suites.

Performance – Users expect websites to deliver content quickly. Look at Google Page Speed Insights to determine how usable your website is from both the desktop and mobile versions. Within the results, there are recommendations for removing or adding certain items to improve your page performance.

Security Headers – Some common attacks including cross-site scripting, clickjacking, and code injection can be mitigated by including security headers within your website. By comparing against best practices, you will be able to see what headers you currently have and the ones that you are missing.



Patch Level – The main server that your website runs on may have vulnerabilities that could leave the website open to malicious attacks. Since Microsoft releases patches regularly, it is important to create a patch management policy to incorporate the new patches. Leaving your server vulnerable could spell trouble for your organization, as some of the biggest data breaches come from a lack of updates through patches.

Code Quality – Look for any mistakes within your HTML codes or redundant coding. Fixing these mistakes will improve the performance of your site.

CPAs & ADVISORS

Privacy

SSL/TLS Strength: Is your encryption up to date?

Most organizations have secured their data with encryption, but security protocols are evolving rapidly in response to sophisticated cyberattacks. Ensuring your organization has the latest SSL/TLS protocols enabled is necessary to help establish trust, ensure data privacy for your users, and to prevent data breaches.

Risks of Man in the Middle Attack (MitM)

If the data on your servers is not encrypted before transmission, attackers can steal information without having to hack into your system. They just need to find a way to intercept the flow of information from the server to a trusted device.

One way is called a "Man in the Middle" attack. The attacker will intercept the data exchange happening between a client device and the server using software. From there, the attacker can copy or modify the data and send it on to the server so that the server does not detect a breach. The server then will respond to the MitM software as if nothing is wrong. The software in the middle may be stealing credentials, modifying information, or collecting the information for unauthorized use which breaches the integrity and confidentiality of the data. Neither the end-user nor the server is aware that a breach has happened.

What is SSL/TLS?

Secure Socket Layer (SSL) is the original protocol that encrypts information that travels across the internet. As vulnerabilities were found in SSL, a new protocol took its place, Transport Layer Security (TLS). TLS evolved from SSL and provides privacy and data security when communicating over the internet. When you input a password or credit card information into a website with encryption, that data is not able to be seen by hackers or eavesdroppers, thus ensuring privacy for your data.

In a report from the NSA, "Eliminating Obsolete Transport Layer Security (TLS) Protocol Configuration", they recommend that only TLS 1.2 and 1.3 be enabled, while other less secure, legacy encryption methods should be disabled.. Many organizations have TLS 1.2/1.3 enabled and believe that they are safe and secure. However, its predecessor, TLS 1.0/1.1 may still be active, which provides a way for hackers to take advantage of the outdated protocols. For example, Google Chrome is updated to only allow users to use the most up to date protocol associated with the web browser, however, if an attacker utilizes an older browser, they can still access the website from the older TLS protocol which would leave your organization vulnerable to sniffing attacks.

SSL Certificates

To enable trust in your website from users, your organization must have an SSL certificate. An SSL certificate provides data security, prevents hackers from creating a fake website, and provides trust from the users when relaying data to your website. To determine whether your website has an SSL certificate attached to it, look in the left side browser and see if your website has a lock next to the address window. If so, then you have a valid certificate attached and shows as trustworthy to users.

As data protection has become more and more important, web browsers have begun to label websites as not secure when there is not a valid SSL certificate. It can affect a user's trust in your website. It can also reduce traffic to your website, because Search Engine Optimization (SEO) is impacted by whether your website can be trusted. If there will be any information transmitted from a user to your website such as passwords or credit card information, then you must have TLS 1.2/1.3 enabled.

Simply put, Identity and Access Management (IAM) is the discipline of allowing the right individuals to have access to the right resources at the right times for the right reasons. As hackers have gotten more sophisticated, organizations must take steps to ensure that users attempting to gain access are authenticated (they are who they say they are), and that they have permission to access the data they are attempting to access.

Identity and Access Management (IAM): Who is accessing your data?

Implementing security best practices and a credential management program is essential to prevent being a victim of an attack. Highly secure databases can still be beached if users' access credentials are not properly secured. In fact, Ubiquiti – a major networking service provider – had a massive breach last year that exposed user credentials for millions of customers. Attackers were able to access Ubiquiti's Amazon cloud servers by stealing an administrator's credentials. Although Amazon secures their server hardware and software, the client is responsible for securing access, which Ubiquiti failed to do.

Privacy and security are two of the top risks facing organizations today, so it is important to understand how the authorization process works and how to manage it.

Access Management

At a high level, access issues fall into a large category. Access issues occur when users can access data that they shouldn't be able to. Permission issues occur when a user has more permissions than they need to do their job, which can lead to an access violation. An access violation occurs when someone accesses or tries to access data that they are not authorized to see. To ensure users only have access to what they need to complete their job, it's a good practice to utilize the method of least privilege. Controlling access within the system is the first step to maintaining a healthy IAM process and continues with identification and authorization.

User Identification

Most users are accustomed logging into a network or system by using a credentials such as a unique username and password, but as security has evolved, organizations are adopting more stringent requirements. Multi-factor authentication is a best practice in creating an effective credential management system and involves using two or more methods as a part of the authentication process.

Multi-factor authentication adds an extra step for a person to verify his or her identity. It may require providing something that you know (e.g., Password, PIN), something that you have (e.g., Smart Card, Common Access Card, or one-time password sent to phone), something that you are (e.g., Fingerprint, facial scan, eye scan), something you do (e.g., Handwriting, picture password), and/or where you are (e.g. Geolocation, inside a secure facility). At least two of these methods must be used to be considered multi-factor authentication. Utilizing MFA can help mitigate the risk of credential breaches that occur to maintain the integrity of your systems and only allow the correct users to log in to your network.

Credential Management

IAM allows for security and protection when accessing and utilizing your systems and network. However, there is a high risk of a data breach occurring due to compromised credentials. *CyberNews* reported that a database of over 3.2 billion unique pairs of clear text emails and passwords have been compiled and shared by hackers. It includes leaks from popular companies including Netflix, Gmail, and Yahoo. If any of your users utilized these websites and re-use their credentials, your company could be at risk of being attacked. An article from *Security Magazine*, states that 53% of people admit to using the same password across accounts which presents a major risk to your organization. Being aware of these leaked credentials is important to maintain an effective security posture.

IAM Security Best Practices

We recommend taking the following steps to make your systems more secure:

1. **Multi-Factor Authentication (MFA)**Passwords are not enough to keep your information safe. By implementing MFA, you add an extra layer of protection to your system, making it difficult for information to be stolen.
2. **Password Policy**
   Maintain a password policy that includes strong password requirements, changing of password at a set interval, and a top-down approach. If top management follows and enforces the policy, then everyone in the company can follow suit. Security needs to be an organizational mindset and not just an IT one.
3. **Password Manager**
   Ensure that employees are using password managers so that all of their passwords are different and strong. Many password managers are free and provide safety in case of a credential breach.
4. **Educate Your Employees**
   Organizations are constantly at risk of becoming a victim of a cyber-attack through phishing, malware, and lack of awareness. It is important to invest in cybersecurity training for all employees, having a cyber-policy, and making all employees aware of the process for reporting suspicious items/activity. No matter how strong your physical security is, all it takes is one click to allow an attacker into your network so investing in training and cyber awareness is essential.
5. **Encrypt Data**
   It is extremely important to protect all data by using encryption, so that if you are a victim of a breach, then your data will not be accessible to anyone who is not authorized to do so.
6. **Monitor Breached Credentials**
   There are over 5 billion breached emails and passwords available on the internet and underground forums. It is important to be aware when your organization's credentials are breached so that passwords can be changed.

Hacktivist Shares: Are you being targeted?

Hackers and malicious attackers will often publicize their targets in various forums or on the dark web, so they can gather support and intelligence for taking down a website or finding vulnerabilities within an organization.

Hacktivists are hackers who are politically and/or socially motivated. Their targets are typically organizations that they disagree with. One of the most well-known hacktivist organizations is Anonymous, which is a decentralized group that performs cyber-attacks on organizations. Their most famous attack was on the Church of Scientology, where the group performed various online attacks to disrupt the church's operations. They are also known for recently hacking into Epik, an internet service provider used by many far right groups, and publicly posting the private data of the company's customers.

Anonymous may be the most famous of the hacktivist groups, but other groups may emerge that are not as famous. There are many dark web forums that share information about target companies, and it is important to know when your organization is being talked about, so you can know if your organization is a target.

How do you know if you are targeted?

To find hackers talking about your organization, you will need to search resources that scan the dark web looking specifically at forums, criminal sites, and hacktivist sites. These can be classified by Hacker forums, Whistle Blowing Sites, and other websites related to hackers targeting companies. By narrowing down your organization's name and web domain(s), you can track whether you are a target of a potential attack as well as seeing if your organization has recently been talked about on underground forums.

Best Practices

- When your organization is identified in underground forums, the best thing to do is review the information that was shared and identify if it is confidential, determine if passwords need to be changed, contacting associated clients, etc.
- Revisit your cyber insurance policy to identify what coverage you have in case of a breach and contact your provider if a breach has occurred.
- If a leak is found from your organization or from a third-party that is associated with you, contact authorities and begin a forensic investigation.
- If you find sensitive content from your organization online, attempt to remove it with the help of the police or the local field office of the FBI.
  - » If the information is posted on your own website, you can immediately remove it. Online data is also stored, or "cached" by servers and search engines. You may need to contact search engines to ensure that they don't archive personal information posted in error.
  - » Search for your company's exposed data online. If information turns up on other websites, contact the administrator of those sites and ask them to remove it.

Social Network: Knowing the Narrative Surrounding your Organization

Social media has allowed organizations to connect with customers around the world, but the wide reach of your social network also presents opportunities for hackers and bad actors to launch attacks or damage your organization's reputation. Properly understanding and managing your social media presence allows you to mitigate risks and build a brand image that people in the community know and respect.

Social Network and Cybersecurity risk?

Many social media applications, such as Twitter, Facebook, Reddit, and Discord give people a way to communicate with many people that they never would have been able to connect with in the past. Hackers capitalize on this by trying to gain publicity and rally a group of people to attack a targeted organization. The attacker's motivation can be anything from disagreeing with your message to just practicing their skills.

The most common cyber-attack that can occur from a social media influence is a denial-of-service attack. A group of attackers attempts to bring down your website by visiting the site or sending a flood of emails all at once, thus negating access to either your corporate network or your website. Being aware of when an attack is coming allows you to prepare by filtering IP addresses to look for legitimate connections.

What are some other social media risks?

While attackers can use social media to gain support for their cause, your users need to be aware of their actions on social media as well. Their actions can have serious risks to both the security and reputation of your organization. For example, security can be compromised when a user gives away too much personal information to someone they do not know, leaving their account potentially vulnerable to being infiltrated. Additionally, a user on social media can post anything that is on their mind, so if they decide to talk poorly about your organization, it can harm how the public view both the organization and the employees. Some other risks include:

- Third-party credential breaches
- Clicking on malicious links to infect computers
- Exposing confidential information
- Phishing
- Brand impersonation

How can you limit these risks and take advantage of social media?

Things that an organization can do to take advantage of social media and reduce their risk include:

1. Create a social media policy that identifies what can be posted about the organization.
2. Screen employee's social media presence during the hiring process.
3. Scan social networks for your organization's name to look for the conversation around your organization.
4. Respond quickly when customers interact with you.

Information Disclosure: Are you up to date on privacy laws?

Securing the privacy of your organization's employee and customer data is critical for maintaining the trust of members and donors – and is increasingly becoming a legal requirement.

What is information disclosure?

Information disclosure occurs when an application reveals sensitive information about its users. Depending on the type of information your organization keeps on its users, this disclosure could include anything from usernames and passwords to financial information. GRF's Cybersecurity Risk Assessment and Scorecard will check to see if your organization is potentially disclosing too much information:

1. Information disclosure controls: You can check whether the local IPs, email addresses, version number, Whois records, or services are being disclosed.
2. Data collection policy controls: This feature compares the privacy policy that your organization has to EU General Data Protection Regulation (GDPR) and other regulatory requirements. With the increase in data protection, many companies must be GDPR compliant.

Why you need a privacy policy

The European Union enacted General Data Protection Regulation (GDPR) laws in 2018 to require organizations to protect the personal information they collect. It sets the guidelines for both the collection and processing of personal information for individuals in the European Union. If a user from the European Union accesses your website and you store their information, you are liable and need to be compliant with GDPR.

Data Collection Policy: GDPR lists six principles of data protection, indicating how information should be collected and maintained.

1. The information must be gathered legally and transparently
2. Gathered for specific reasons
3. Nothing more than necessary for legal can be gathered
4. Accurate information
5. Held for a limited time
6. Processed in a secure way

To be GDPR compliant, you must disclose how you collect the data, what data is being collected, how the data is stored, how the data is used, data rights, and how you share and disclose information to 3rd parties. All of these items need to be noted within your policy – and they must be followed. If your organization does business in the European Union and does not comply with GDPR, you could face legal liabilities.

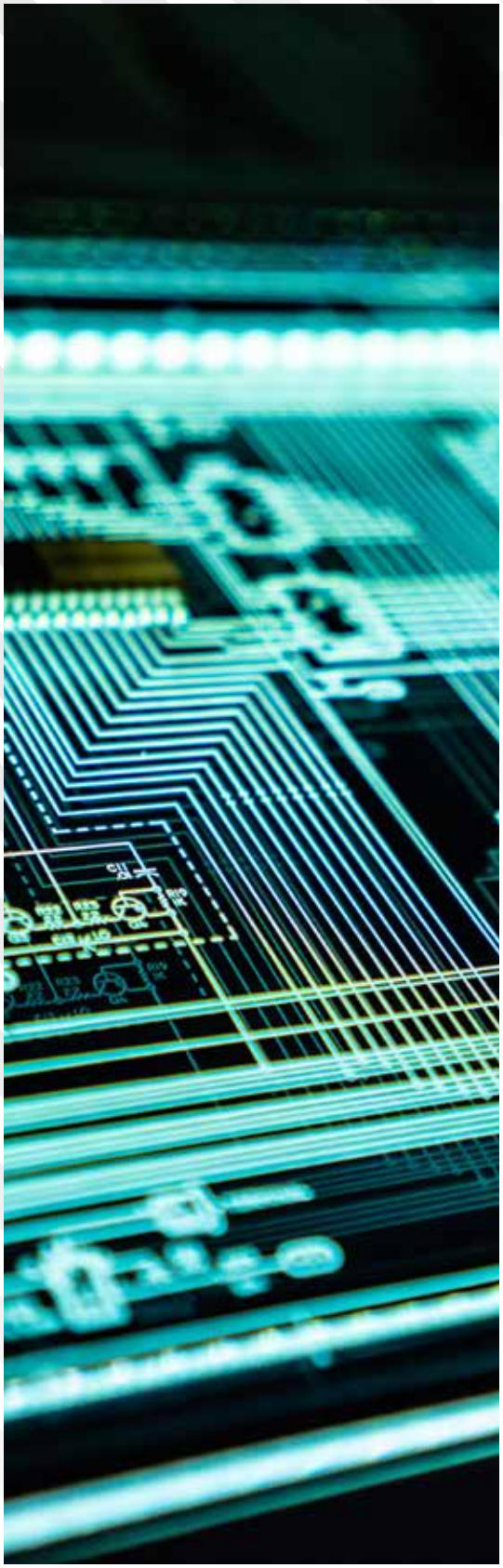
Growing U.S. Privacy Legislation

In the U.S., there are many federal and state regulations surrounding the protection of personal data. Some of the more common regulations are HIPPA (protection of personal health information), Children's Online Privacy Protection Act (COPPA – must be clear in privacy policy about the information collected of users under 13 years of age), and the Gramm-Leach-Billey Act (organizations engaged in financial activities must give clear statements about their information-sharing practices).

States are starting to enact regulations as well. For example, California passed a regulation for online services that collect personal information that they must post a privacy policy and comply with its content, including identifying the personally identifiable information (PII) collected, who the third parties are that the information will be shared with, and more. It also requires a section about how the website responds to "Do not track" within web browsers.

Most recently, Virginia passed the Consumer Data Protection Act (CDPA) that will be effective starting January 1, 2023. While similar to the California Consumer Privacy Act (CCPA) above, there are some key differences.

- The CDPA's opt-out rights include the right to opt-out of not just sales of personal data but also certain profiling activities and targeted advertising.
- The CDPA's provisions requiring consent before processing sensitive data (i.e., affirmative opt-in) are significantly broader and more restrictive than the CCPA's current requirements.
- The CDPA requires that businesses conduct Data Protection Assessments (similar to GDPR's requirement for data protection impact assessments).



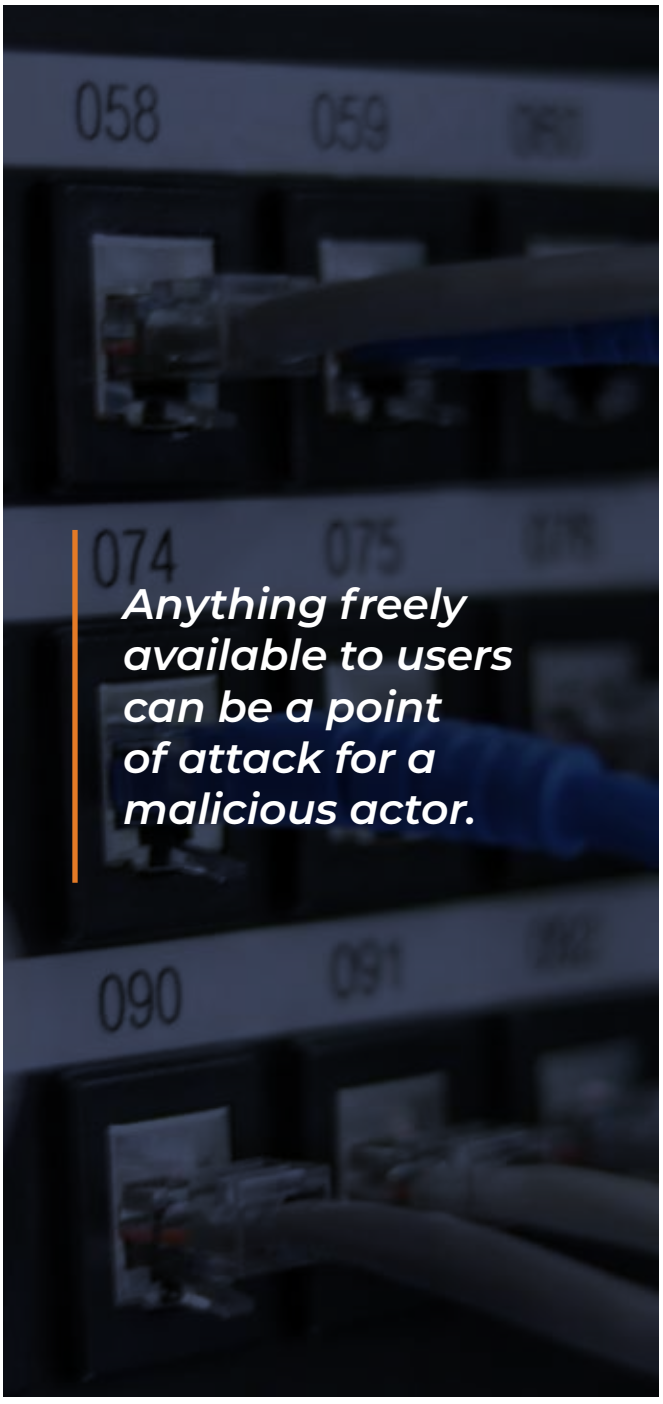
CPAs & ADVISORS

Resiliency

Attack Surface: Are all your systems' access points secure?

Anything freely available on the internet and open to users can be a point of attack for a malicious actor. To prevent unauthorized access to your network and systems, it's crucial to understand the vulnerabilities of your network.

The term "attack surface" refers to the total number of access points into your system. An attacker can scan the internet to look for information about your site and if they see something that looks vulnerable, they could come knocking. Securing your systems from unauthorized access starts with analyzing for open critical ports, outdated services, SSL/TLS strength, and other misconfigurations that can come from unpatched servers or from testing and troubleshooting. Securing all access points, knowing what is vulnerable, and developing a proactive security strategy can help your organization prevent cyberattacks.



Critical Points

While it is important to constantly scan for vulnerabilities on your network and servers, there are places within the network that can be particularly risky if vulnerable.

Open Critical Ports – These are access points, or ports, that are open to the public and allow for remote administration. Some examples of this are Microsoft's

Remote Desktop Protocol (RDP), Virtual Network Computing system (VNC), the Secure Shell Protocol (SSH), the Telnet application, and Simple Network Management Protocol (SNMP). With the shift to remote work and remote administration, these ports are now commonly used, so they need to be locked down to only trusted IP addresses and secured through strong cryptography and security protocols.

Outdated Systems – Having outdated service versions or servers can provide an opportunity for attackers to use a known vulnerability against you. This relates directly to your patch management policy along with tracking end-of-life server versions. Patch management can be done monthly and should be tested before implementation. When the vulnerabilities are known, your organization should be consistently updating versions and applying the appropriate patches. Similarly, if a server is going to be at end of life (such as Server 2008 r2), then you should start planning the migration of the data or applications from that server to a new one.

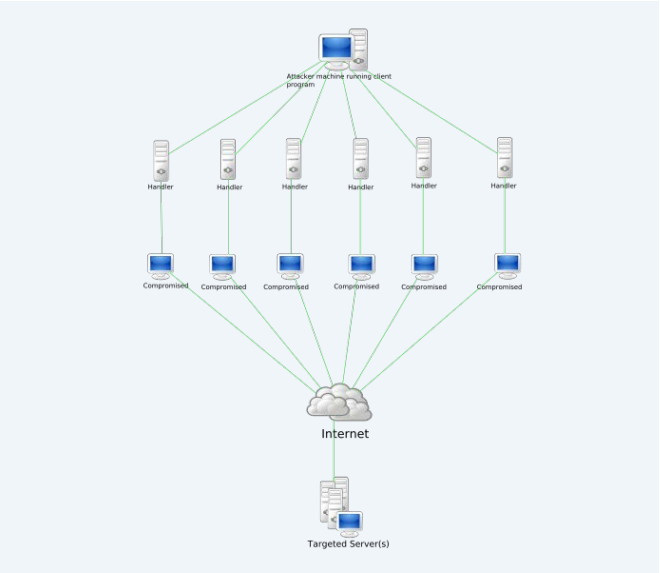
Web applications – Many vulnerabilities can be exploited through a web application. Common exploits include cross-site request forgery, SQL injections, brute force password attacks, and more. Each of these presents the risk of an attacker gaining unauthorized access to your information or systems.

Outdated security protocols – Many web browsers do not allow users to access a site if it is not secure (a secure site has a web address starts with https:// and a lock icon appears in the address window). Even if your site has a valid SSL certificate – indicating that data is properly encrypted on your site – there still may be out-of-date security protocols that make you vulnerable. One of the most common examples is having older Transport Layer Security (TLS) versions enabled. TLS is a protocol designed to encrypt data sent over the internet, but like software, it is regularly updated to address identified vulnerabilities. At this point, TLS 1.2/1.3 are the only TLS versions that should be enabled on your site. Finally, you should verify that the cipher suite you are using is also updated. The cypher suite is the set of algorithms available for networks to secure a connection. Even if you have an updated TLS, using weak ciphers can leave you open to common SSL/TLS attacks.

DNS Health: Ensure your organizations' identity is protected

Your organization's domain name (e.g., "example.com") serves as the base of operations for your online identity – helping interested parties to find you and connect with you online. However, the underlying machine language of the internet is based on numbers. Every site on the internet has a unique location identifier called an IP address. The domain name system (DNS) serves as a translator – mapping the language-based domain names to their corresponding IP addresses and then routing requests accordingly. This makes it easier for people to find websites, companies, and things they are interested in online. Without DNS, we would have to remember hundreds of IP addresses for everything, rather than domain names.

DNS servers make life easier, but they also provide an opening for unwanted attacks. One of the reasons attackers target your DNS is because it is often not secured and successful attacks can be profitable and cause disruption. If your DNS is poorly configured or insecure, it could be an easy target for an attacker. Regularly reviewing your DNS health allows you to identify any missing configurations and create an appropriate defense against attackers who may try to take down your critical business functions.



How are DNS Servers attacked?

Some of the most common attacks include DDoS attacks, domain name hijacking, and DNS amplification attacks.

A Distributed Denial of Service attack (DDoS) or a simple denial of service (DoS) attack is achieved when bad actors send so many requests to your domain server all at once that it is not able to handle them. This causes your website to become unresponsive to legitimate requests (read more on our blog post on DDoS Attacks).

Domain name hijacking occurs when an attacker gains control of your domain name by transferring it from your registrar (for example GoDaddy) to their registrar account. Once this is done, they can simply

redirect your web traffic to a site of their choosing, potentially one that looks exactly like yours but with malicious links and or software. As mentioned previously it is easier for people visiting your website to remember the site name instead of an IP address (104.2.45.186) because of this an attacker can keep your website name the same while changing the IP address on the backend.

DNS amplification attacks are a type of DDoS attack in which a DNS system is exploited and turns smaller requests into larger ones, thus overloading servers. Understanding these types of attacks and scanning your DNS is beneficial in preventing your organization from falling victim.

What items should be scanned for DNS Health?

Some tests that can be run include NS tests, parent server tests, MX tests, WWW tests and SOA tests. Each of these tests help to identify whether your organization is following best practices when setting up and maintaining your DNS. Some common things to review include your domain's MX record redundancy, making sure your WHOIS registry and registrar fields correctly configured, and reviewing DNSSEC records.

MX record redundancy – When your primary mail server is down, it is crucial to have a backup record – called a mail exchange record (MX record) – to allow you to continue to accept mail. Since email is one of the main forms of business communication, having this set up with redundancy will reduce down time in the event of mail server disruption.

DNS Registry and registrar records enable multi factor authentication on your domain name for added security. You can set up alerts, so you are notified if your domain name information is deleted, transferred, or updated. This prevents attackers from secretly hijacking your domain and changing your website to a malicious one.

DNSSEC records help to secure DNS records by adding a layer of trust on top of DNS. They provide authentication of DNS data, ensuring the data integrity is maintained and proper authentication is exchanged between DNS servers and clients.

Email Security: Don't let attackers in through the front door

Your email is a critical business function that needs to be constantly available and secured. Securing your email systems involves looking at the configuration of your email server, your mail exchange (MX) records, and SMTP (Simple Mail Transfer Protocol) to identify any potential vulnerabilities or misconfigurations. Identifying these issues before it is too late could help save your organization from being in the news for the wrong reasons.

When it comes to email security, technologies are only part of the equation. The biggest vulnerability is human error. According to security firm KnowBe4, 91% of successful data breaches begin with a simple email that causes the recipient to inadvertently provide an attacker with unauthorized access.

Phishing

Phishing is one of the most common – and successful – forms of email attack. A hacker will fool recipients with fraudulent emails designed to gain personal information such as email passwords, bank accounts, and more. These attacks have increased during the pandemic, so it is important to know what these attacks are, what they look like, and how to prevent them.

Types of Phishing

HTTPS Phishing – These attacks include a legitimate-looking email with a link that directs users to a fraudulent webpage. With the increase in complexity of these attacks, it is harder to distinguish that the link it is a malicious site, as many attackers set up what looks like a secure website that uses HTTPS.

Spear Phishing – An actor targets a specific person and modifies their attack to be personable and appear legitimate. Making the message look like it is coming from a trusted person makes it harder for the recipient to notice that the email, links, or attachments are fraudulent.

Whaling – A form of spear phishing where an attacker goes after a high-profile target such as the CEO of a company.

Vishing– Also known as voice phishing, this is the act of making phone calls that appear legitimate trying to get you to divulge sensitive or personal information like passwords, credit card information, and social security numbers.

Smishing – A newer form of phishing where a text message is used to entice you to click on a link. In a "Bring Your Own Device" (BYOD) environment where employees use one cell phone for personal and business communication, this is particularly dangerous for employers.

System best practices

All organizations should follow email security best practices to avoid the opportunity for human error in their organizational network. There are many configurations that must be set up and analyzed to reduce the risk of attacks through email. It is in the best interest of the organization to create a system that enforces security but also allows for availability and usability.

1. Ensure that your SMTP configuration is set up appropriately by testing SMTP Open Relay, Authentication and connection.
2. Perform email address spoofing tests.
3. If using web mail, make sure you are using a secure connection like SSL.
4. Make sure that you have a DMARC (email authentication), DKIM (to prevent spoofing), and SPF record (to limit IP addresses that can use your email domain).
5. Have at least two MX servers (email exchange servers) to create redundancy in case one server goes down. This ensures availability of your email.
6. Regularly perform tests against your email security to ensure that there are no vulnerabilities.

End user best practices

1. Always think before you click on a link on an email. Ask yourself: "was I expecting something from this person?"
2. Always check the email sender. The name may appear to be someone you know but look at the actual email address. A sender name can be spoofed, making it dangerous.
3. Report malicious emails to your IT team to allow them to pull it from other user's inboxes or to inform the organization.
4. If you do click on a link or download something that seems to be malicious, contact your IT team immediately, as they will need to track your activity and isolate your machine from your network.
5. Do not send confidential or sensitive information through email. Always make sure that the information is encrypted and sent through a secure portal.

DDoS Resiliency: Protecting Against the Attack of the Robots

Your website is essential for promoting your nonprofit organization's mission. However, bad actors often target nonprofit websites for attack, assuming they are not as protected as commercial sites. One hacker strategy is to bring the site down entirely through a denial of service attack. That's where checking your DDos resiliency comes in.

A distributed denial of service (DDoS) attack is when a malicious actor (or number of actors) overloads your servers to gain access to your website and target your system. This type of brute force attack typically results in blocking access to your applications. Server overloads are not always caused by deliberate attacks. For example, you may experience a website not working when trying to buy a limited-time sale item but the website does not load. This is due to lack of resources on the web server, but the result is the same as a DDoS attack.

Common DDoS Attacks

Volume attacks – These are attacks that send a massive amount of traffic to a site to create either a super slow connection or no connection for legitimate users. This can be done by a coordinated network of attackers visiting your site all at the same time. At GRF, we can help monitor underground forums to learn if your site is are about to be targeted as part of our Cybersecurity Risk Assessment and Scorecard.

Protocol attacks – These attacks overload your server by making numerous server requests. For example, networks often "ping" each other to test connectivity. Hackers can create a "ping flood" to continuously send requests to your server and flood your server with requests, thus causing a volume overload. Another example is a DNS flood, where an attacker sets up pings that target a DNS server (the servers that connect website domain names, or URLs) to the underlying IP addresses. DNS floods disrupt the DNS system, so the website is not reachable.

Application attacks – Attackers can attempt to infiltrate a vulnerability in your application with various attacks. One example is a brute force amplification attack, in which an attacker utilizes a vulnerability in login pages to execute the attack. They will enter in a huge volume of user names and passwords trying to enter your site.

Preventing DDoS Attacks

Common preventative measures you can do to mitigate the risk of DDoS attacks include:

- Patch your system to avoid any potential vulnerabilities.
- Put your web application behind a firewall.Utilize Word Press DDoS applications.
- Limit the number of authentication attempts allowed at sign in pages.
- Analyze traffic to identify if a surge is a real spike or an attack.

Network Security: Building Resiliency

It's not just about disruption or inconvenience. A compromised technology incident can have a detrimental impact on your organization's processes, mission, and reputation. A review of your external network security risk should include looking at any risk that is related to your perimeter network – or how users gain access to your organization's data.

Network Security is comprised of the policies and procedures an organization utilizes to prevent and monitor against unauthorized access, misuse, modification, or denial of a computer network. It also provides procedures for maintaining the confidentiality, integrity, and availability of data.

Most Common Network Attacks

Network attacks attempt to gain access to information or assets that should be confidential. Many network-level problems stem from open critical ports, unprotected network devices, misconfigured firewalls, and service endpoints. There are two types of network attacks: passive and active. A passive attack is when a malicious attacker intercepts data traveling through your network to gain information. An active attack occurs when a malicious attacker runs commands to disrupt the normal operation of your network or to gain access to devices on the network. Some of the most common types of attacks include:

Unauthorized Access
When maintaining confidentiality, integrity, and availability of information, it is important to control who should have access to what information. When a malicious attacker gains access to your network, they can steal, modify, or lock information.

Denial of Service
Malicious attackers can target a network and flood it with service requests. The overload on your servers can cause a denial of service and bring your network or database down. This will not allow legitimate users to access your site which can result in a loss of funding, subscribers, and organizational growth.

Man in the Middle
A man-in-the-middle attack is the interception of traffic between your network and other websites. If the transmitted data is not encrypted, an attacker can gain access to data that is being sent and steal or change the information. For example, an attacker might steal the data being transmitted to gain a user's credentials.

What is at risk from a network attack?

Customer information: When your network is not secure, you risk exposing personally identifiable information about a customer or donor. Attackers can "sniff" your network for vulnerabilities and steal credential information which can leave your organization vulnerable to unauthorized access to organizational, customer, and financial information.

Revenue: If your site is brought down, legitimate users cannot access your site to make donations, register for events, or join as members. Having mitigation procedures in place to avoid the risk of denial of service attacks is critical to ensuring high availability for your website and network.

Mission: Attacks that ruin your organization's reputation can have devastating and long-lasting effects – from loss of donors, to employee turnover, to diminished public support. It is essential to make sure that data is kept in a secure, encrypted space to avoid the risk of losing the public's trust.

Ransomware: If a malicious actor can exfiltrate data due to a vulnerability or a weakness in your network security, your organization risks all of the above. During a ransomware attack, a malicious actor introduces malware to the network to lock critical data and systems, bringing your organization to a screeching halt.

> *Perform regular external network assessments to identify potential vulnerabilities*

Mitigating Network Risks

To understand what a malicious attacker sees, perform regular external network assessments to identify potential vulnerabilities like open ports or services that are missing data encryption. You should also regularly look at your network setup for handling ping floods (attempts at a DDos attack) and firewalls.

When you identify risks and vulnerabilities, there are many ways you can reduce the likelihood that they impact your organization. Some common remediation actions that are utilized after running an external network scan include:

1. Disabling plaintext protocols like telnet or HTTP
2. Monitor publicly available ports and close unused critical ports
3. Having web applications behind a firewall
4. Blocking attacks on your internet network (UDP Flood, ICMP flood, etc.)
5. Disabling Anonymous FTP logins

While this is not everything that you must consider, they are a starting point for preventing some of the most common attacks and risks.

CPAs & ADVISORS

Reputation

Brand Monitoring: Tracking Your Social Footprint

Have you ever wondered how end users view your company? Is your domain seen as safe and trusted? Is your website optimized? These are just some of the areas that business analytics tools assess to evaluate your brand. Every organization is adapting to the changing digital landscape by creating social media accounts and trying new marketing techniques to grow. With the increase in cybercriminals trying to take advantage of these organizational opportunities, it is important to monitor how you are perceived over the internet.

GRF offers a service that combines several assessments to deliver a rating on your brand's online health. Some of the main items that rate your overall online brand include the Web of Trust, Domain Safety, Website Quality and Optimization, and Social Profiles. Each of these tests gives insight into why people may or may not be visiting your website or supporting your business. For example, you can see if your pages are search engine friendly or whether your site is showing as safe. Scanning your organization can identify areas of strength and and areas that may need improvement.

What does GRF monitor?

- **Web of Trust (WOT)** – This security service uses a website's reputation and online reviews to help people make decisions about whether the site can be trusted. WOT looks at vendor reliability, child safety, trustworthiness, and privacy. While your organization may not currently be within the registered database, it is important to keep track how you are viewed.
- **Domain Safety** pulls from blacklist search engines to develop your online reputation and detect fraudulent or malicious websites. You can pull each of the search engines used into a checklist to verify whether your organization is seen as safe across the board.
- **Website Optimization and Quality** looks into the website landing page to monitor items to help optimize your brand. It looks at items such as SEO-friendly web URLs, Google Analytics Tracking, most commonly used words, and more. It can help decide where to put your resources and the content you should add to your website to enhance your brand.
- **Social Profiles** atrributed to your organization, helping to identify a fraudulent page that you did not sanction. Not knowing what information is being posted on social media with your branding creates reputational risk.

How can you improve your Digital Footprint?

1. Utilize the reputation services like the Web of Trust to be correctly categorized and monitor where your reputation ranks.
2. Monitor blacklist websites such as AbuseIPDB to ensure that your organization is not being flagged as spam or malicious.
3. Validate your search engine optimization strategy by working through website optimization and quality improvements.
4. Track social media accounts to ensure that there are no identical and malicious/copycat accounts.

IP Reputation: Are You Being Blacklisted?

Your organization's reputation can be influenced by a variety of factors including brand image, online reviews, social media presence, customer experience, and more. Each of these elements factors into the overall image of the organization. When it comes to your internet reputation, important elements are different and can impact not just how you are seen by the public, but if you are seen at all. Your organizational domain and IP reputation is rated on factors such as presence on blacklists, use of botnets, and the reputation of the URLs owned. Each of these elements creates an overall reputation for your organization and can influence how your website shows up on search results or how your emails are delivered.

Understanding Your Cyber Reputation

To combat the enormous amount of spam email sent every day, Internet Service Providers create blacklist databases that identify IP addresses that send spam, send malicious files, or have been reported for cyber abuse in the past. These lists are used by many organizations to filter out suspicious emails sent to their end-users. If your organization's IP address is listed on an IP reputation database like abuseipdb.com, legitimate emails sent by your employees could be blocked by the recipient organization's email filtering service. Your emails might never make it to the intended recipient.

> *Your IP address could become blacklisted without your knowledge.*

It is important to monitor these IP reputation databases so you can identify possible email delivery issues and try to remove the listing of your IP address if it appears.

Your IP address could become blacklisted without your knowledge. An end-user on your system could accidentally click on a malicious link that downloads a computer virus, giving control to a hacker. The hacker can then use the computer to send emails in the background or add it to a botnet for denial-of-service attack on another computer system.

Some of the riskiest assets that an organization can hold are IP addresses and domains that are not actively managed. For example, if a systems administrator purchases a domain name and associated IP address but forgets about it or does not manage it, this domain could fall victim to a hacker, resulting in a bad cyber reputation for your organization across the internet.

Remediation Steps to Consider

There are several things that your organization can do to build a healthy, trusted cyber reputation. Continuously tracking and understanding where your organization is seen on the internet is the goal of the remediation steps.

- Regularly monitor IP reputation databases. When your domain's IP address is listed on a blacklist database do the following:
  - » Determine if this is a false positive or something malicious.
  - » Contact the site to request your IP address be removed from the list.
- For example, on abuseipdb.com, you can search your IP address, and if it is found, submit a request through their link to have it taken off.
- Set up email filtering and firewalls using the IP address blacklist databases to block spam and malicious traffic coming to your users.
- Make sure that domains that you own resolve back to a trusted IP address.

While you cannot prevent someone from reporting your organization, you can ensure that your organization is not on these databases by monitoring the lists and having your IP address removed if it appears.

Fraudulent Applications: Are Attackers Pretending to be You?

When downloading a new app, be sure it's from a credible source. Hackers can create fraudulent applications that look very similar in name or appearance to well-known apps. To make matters worse, these fake apps can sometimes be found on trusted sites like the Apple or Google Store as well as being available as a download from the internet. Once these applications are loaded onto a user's computer, they can perform many attacks to gain data and information and potentially spread their impact across your network.

Attacks from Fraudulent Applications

Fake applications can have a devastating impact on the end-user by launching several kinds of attacks:

- **Trojan Horse** – This virus performs a script that can infect the computer or network with malware. Because it looks authentic, the user won't realize it is a virus, which makes this very dangerous.
- **Keylogger** – This application enables an attacker to track everything a user types, including usernames, passwords, and other sensitive information. They can use the information to harvest the user's credentials which can lead to unauthorized access to the systems.
- **Viruses** – These malicious codes can be executed to perform a range of harmful programs that can damage the computer.

How to Mitigate and Reduce Risk

Fake apps that use your logo, name, and brand can fool people into thinking the app is legitimate, resulting in not just a breach of security for the end-user, but a reputation risk for your organization. Follow these best practices to reduce the risk of fraudulent applications affecting you.

1. Continuously scan and monitor app stores and the internet to see if there is a new application that is using your organization's name or logo.
2. If pirated apps are found, contact the app store or hosting providers to let them know that the app is fraudulent and should be taken down.
3. Monitor your online brand and cyber posture to make sure there aren't domain names, social media accounts, and other online entities that are very similar to yours. These can be used to target victims.
4. Educate your employees so they remain vigilant to potential fraudulent apps.

Fraudulent Domains: Are You a Victim of Typosquatting?

Fraudulent domains look very similar to your organization's domain name and are used to fool people into thinking they are interacting with you. These domains are often used in phishing attacks, which according to CSO Online, account for more than 80% of all reported security incidents. Many phishing attempts come from emails that look legitimate in an attempt to defraud recipients – a tactic commonly referred to as typosquatting. For example, a company name "Example" has an email address of name@**example.com**. The attacker buys a domain name that closely resembles example.com, such as **exammple.com**, and sends a malicious email to your employees trying to get them to disclose credential information or pay fake invoices. This is an easy way for malicious attackers to target your organization and potentially cause monetary and reputational harm.

How can you identify these domains?

Two common identifiers of a fraudulent domain are the Levenshtein Distance, a calculation that assesses how close the name is to yours, and Fraudulence Possibility, an indicator that looks at the digital footprint when the domain was created and other domain information which may indicate a malicious intent. Domains that have a fraudulence possibility of over 75% are typically ones that you want to monitor.

To find these domains, we can use a tool from ICANN (The Internet Corporation for Assigned Named and Numbers) called WHOIS. This database holds all domains used on the internet. It can be used to test and compare domain names close to yours. While this is a tedious process if done manually, GRF can help by running an external scan and providing a list of the most-likely fraudulent domains.

> *GRF can help by running an external scan and providing a list of the most likely fraudulent domains.*

Best Practices to Avoid Fraudulent Domains

One way to prevent being a victim of a fraudulent domain scam is to register all common typos of your domain name yourself. However, not every organization has the means to buy every possible domain name that is like theirs. At GRF, we recommend the following steps to mitigate the risk:

1. Scan your domain against the 300 million + domains in circulation.
2. Get a fraudulence possibility score to identify which are the most likely to be dangerous.
3. Review the highest risk domains to see what their website is showing.
4. Ask these questions of the domains:
   - Is the webpage similar or nearly identical to ours?
   - Is it a parked website? These are typically sites with the main page saying, "Coming Soon" or "Under Construction".
   - Could someone mistake this domain name for our organization's?
5. Once you identify the sites that are not legitimate and are risky, you can take action. The most common actions against fraudulent domains include:
   - Report the domain to the domain registrar noting that it is replicating your website and is not legitimate.
   - Buy the domain name if possible.
   - On your email server, block emails from being sent to your users from the risky domains.
   - Track the domains going forward and do at least a quarterly audit to make sure these domains are not replicating your site.

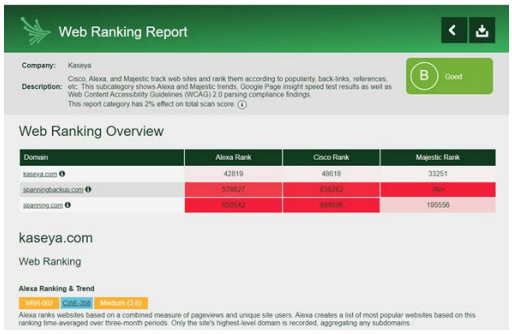
Web Ranking: How Do You Measure Up?

While web ranking is not necessarily a security concern, having insight into the popularity of your website helps measure the success of ad campaigns, assess visitor engagement with your content, and identify opportunities for growth. Web ranking sites include Alexa, Cisco, and Majestic, and each site ranks on different criteria. Alexa ranks websites based on a combined measure of page views and unique site users. The Cisco Ranking creates a list of the most popular brands and websites. The list contains the most queried domains and differs from Alexa. Majestic ranks every website in the world based on the number of citations or links from other websites.

Web ranking includes all websites in the world, so it may be difficult for smaller organizations to break into the top rankings, but you can still see where you stand and see improvements over time.

Along with web ranking, another beneficial tool is Google Page Speed Insights, which is used to measure the website's performance and usability. It measures desktop speed, mobile speed, and mobile usability. Each is used to give a ranking 0-100 and can be summed up by:

- **Good** – The page applies the most performance best practices and delivers a good user experience.
- **Needs work** – The page is missing common performance optimizations that may result in a slower experience.
- **Poor** – The page is likely to deliver a slow performance.



Screenshot of the web ranking report

Google PageSpeed measures a site's performance and usability.

When comparing to best practices, Google Insights will assess the items that you are currently using and list tools you're not using but should, so you can improve your website experience for users.

Increasing traffic

The best way to increase your web ranking is to increase your web traffic. This can occur through ads or search engine optimization. There are many things that your organization can do, but this article from HubSpot helps to outline 7 things to increase your online presence.

- **Encourage visitors to search for your brand**
  Many nonprofits have a niche target audience, but there are keywords that you can use to gain the attention of a larger audience and drive traffic to your website.
- **Update your content**
  Search engines are continually improving their algorithm to find relevant searches for users. If your content is old and rarely updated, it will be hard for your organization to show up on the top search results page. It is crucial to use new information and statistics and regularly update your content and webpage.
- **Analyze keywords beyond search volume**
  You may think that certain keywords have the most potential to drive traffic to your site, but it is important to do your research before targeting a keyword to write content about. It is good to recon and test the topics actual opportunity to drive traffic. Certain words may already have a connotation to other organizations, so it is important to know what words can positively impact your organization.
- **Prioritize internal linking**
  Within your content, there should be logical linking to help Google understand what words relate to one another.
- **Form strong relationships with your developers and designers**
  SEO is dependent on the content that is being created, and if you have a good relationship with your web designer, then you can work better with them to increase your online presence and make your content SEO friendly.
- **Prune content after long periods of growth**
  If you are constantly churning out content, it may be a good idea to remove or refresh your old articles on your website to increase the speed and performance.
- **Optimize search-friendly content**
  When the opportunity to drive organic traffic is greater than the time invested, then you should focus on that. Since search engines won't look for your ads or landing pages, having search-friendly content can drive them to your page to help market your organization.

There is always room for improvement in increasing traffic to your website. Read more tactics to improve your search engine results.

Areas of opportunity

Google offers in-kind advertising for eligible 501c3 organizations. Google Ad Grants provide nonprofit organizations with $10,000 per month in search ads shown on google.com. This is an opportunity for eligible nonprofits to take advantage of and help grow their organization. The steps for applying are included here.

1. Apply for Google for Nonprofits
2. Activate Ad Grants
3. Launch a successful Ad Grants campaign

Various Google certifications can be obtained to help improve your Google Ads campaigns and drive traffic to your website. Utilizing these can help you make the most of the opportunity.

CPAs & ADVISORS

How GRF Can Help

GRF Cybersecurity Risk Assessment and Scorecard

The GRF Cybersecurity Risk Assessment and Scorecard identifies possible vulnerabilities and weaknesses of an organization by evaluating 19 security related categories and one informational category. Each of the categories impact the score and help to create an easy-to-read report. The report will identify possible risks, remediation steps, and best practices to increase your score.

Scope of Work

GRF uses the latest technology to evaluate the security posture of your organization based on your organization's domain name using open-source intelligence (OSINT) to gather the information. We will begin the scan as soon as we receive your signed agreement and will provide the results within 5 business days.

Watch The Video

Deliverables

- Compiled results in a simple, readable report with letter-grade score to help identify and mitigate potential security risk
- Summarized technical details and related standards along with mitigation suggestions for top risk items identified
- 30-minute consultation to discuss report results

Results

With the results from the scorecard combined with GRF's consultation, your management will develop an understanding of the organization's risk exposure and be better positioned to deal with cyber threats now and in the future. We want to help, so we offer a very easy and affordable way to learn where you're vulnerable.

GRF's Cybersecurity Solutions

GRF is dedicated to safeguarding the integrity of our client's information technology systems. Our service approach is systematic and heavily focused on timely, responsive, and clear communications. Performed by CISA-certified auditors, our in-depth understanding of the cyber risk landscape, pressing regulations, and recommended frameworks assures you of an accurate and value-added assessment. We evaluate each client's cybersecurity posture and overall IT risk against changes relating to digital transformation, emerging threats, and the increasing regulatory environment. Our practical, right-sized solutions are based on your organizational context to address your most important issues.

Strategy

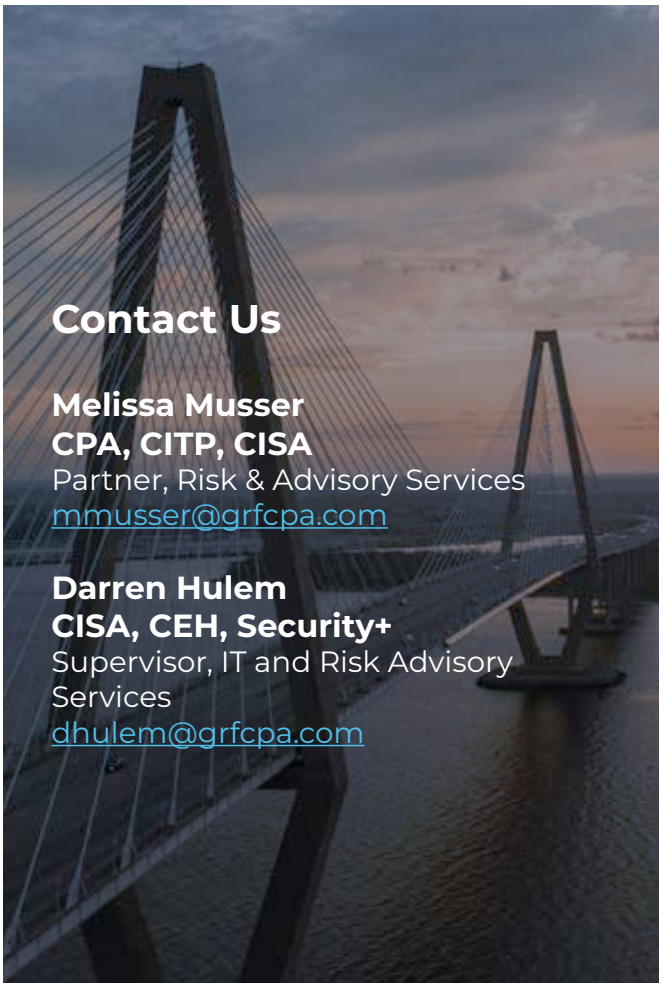
- Compliance framework benchmarking
- Policy and procedure development
- Data privacy and protection
- Virtual CISO
- Third party risk management
- IT strategy assessment
- IT mentoring

Security

- Cybersecurity audit
- Cyber risk assessment and scorecard
- Internal threat assessment
- Cyber training
- Identity and access management

Resiliency

- Incident response planning
- Disaster recovery planning
- Business continuity planning
- Tabletop exercises
- Penetration testing
- Data loss prevention



Contact Us

Melissa Musser
CPA, CITP, CISA
Partner, Risk & Advisory Services
mmusser@grfcpa.com

Darren Hulem
CISA, CEH, Security+
Supervisor, IT and Risk Advisory Services
dhulem@grfcpa.com