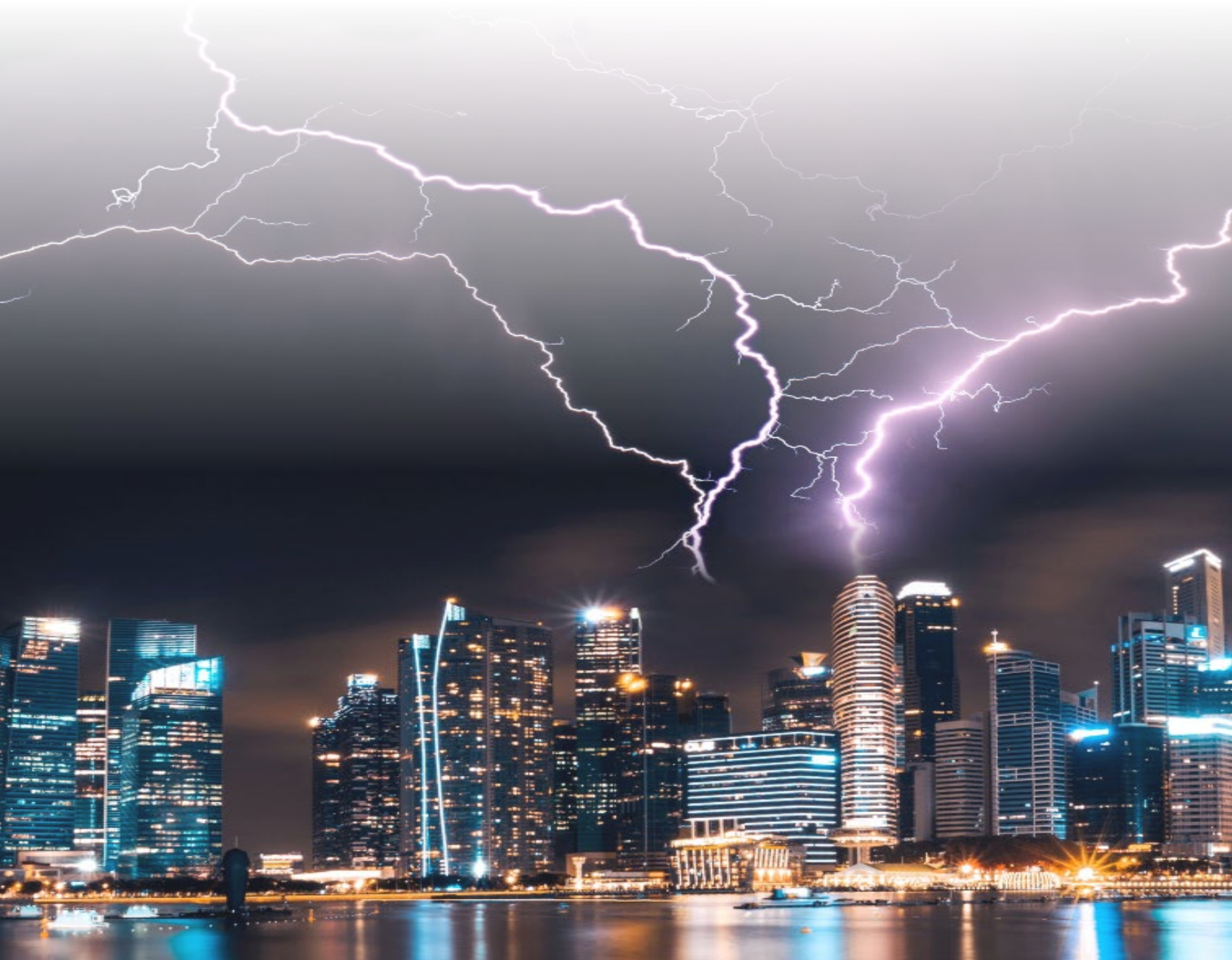
# Elements of Successful Cybersecurity



# Elements of Successful Cybersecurity

Businesses and nonprofits alike are more reliant on technology than ever before for day-to-day operations. The integration of digital technology into all aspects of the organization, or digital transformation, provides a number of new opportunities, but it also opens the organization up to new and emerging security issues.

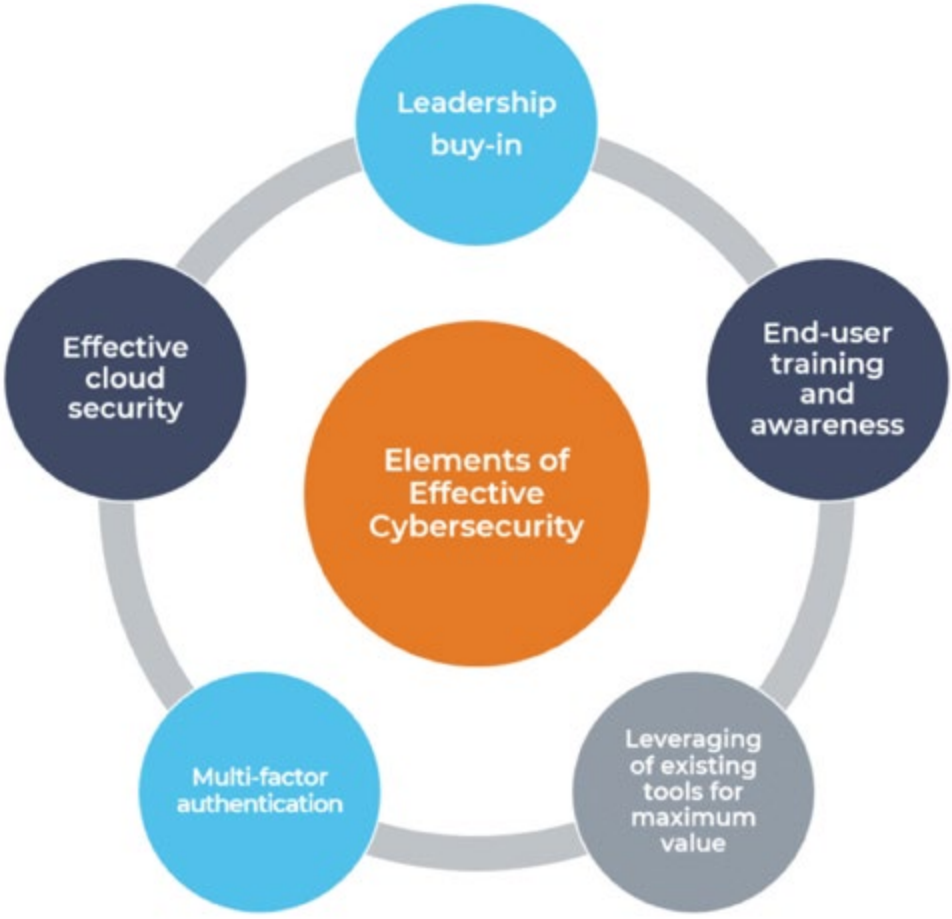
Digital transformation means that organizations must be proactive about their cybersecurity. Not only are there more ways to be attacked than ever before, cybersecurity breaches are constantly changing and hackers are becoming more sophisticated. Without proper cybersecurity, the organization's critical activities are at risk and the potential for reputational damage is real.

*"Contrary to popular belief, you do not need to spend a lot of money to protect your organization. Start with reviewing the products and services already in use, and evaluate whether these existing solutions are being deployed to their full potential."*

Smaller organizations are particularly vulnerable due to budget constraints and staff resources, but they can benefit from adopting proven best practices from their larger counterparts. Many are surprised to learn they already have most of what they need to protect their organization and a large investment of capital is not needed to achieve effective cybersecurity.

## Characteristics of Successful Cybersecurity Programs

Successful cybersecurity programs include a combination of these elements.




### Leadership Buy-In

Arguably, one of the most important aspects of cybersecurity for an organization is leadership buy-in and support. While effective cybersecurity to protect the organization may seem like an obvious priority, in many cases there are detrimental enforcement issues. The cybersecurity "shield" may be in-place, but exceptions are made for specific users creating a weakness in the organization's security posture. Common examples of these exceptions include exemption from the password policy, exclusion from multi-factor authentication or failure to complete cybersecurity training. Leadership support allows the organization's information technology (IT) team to enable the appropriate cybersecurity measures and enforce critical policies and procedures.

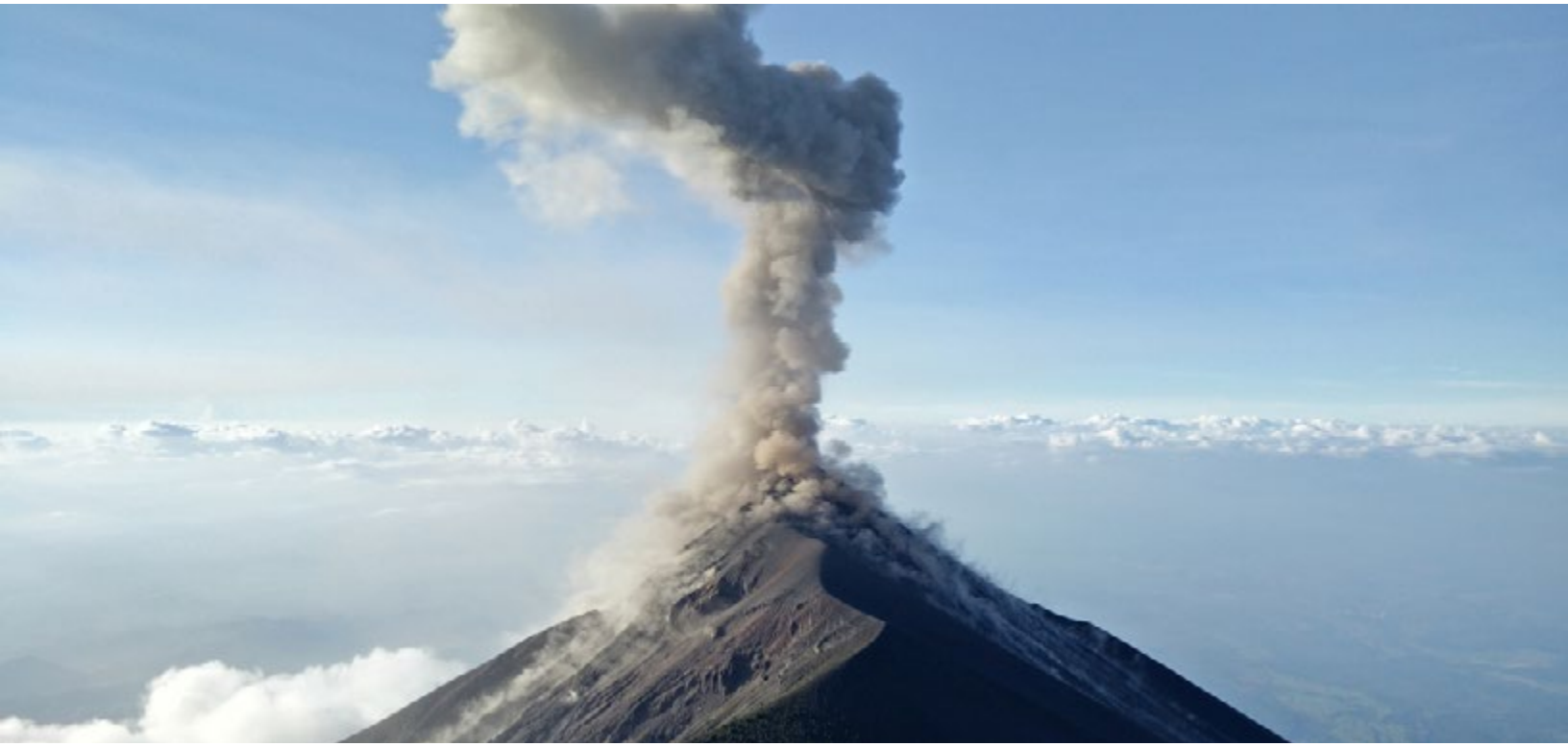
## End-User Training and Awareness

Equally important as leadership buy-in, end-user training and awareness is essential to the success of every cybersecurity program. While many organizations have employed spam filters, the best technology products still cannot stop every phishing attack. According to Verizon's 2019 Data Breach Investigation's Report, 94% of malware was delivered via email. Additionally, Symantec's 2019 Internet Security Threat Report stated that, "65% of groups used spear-phishing as the primary infection vector." With email being the primary form of communication for most organizations, it is critical to have continuous education for end-users.

Effective cybersecurity training and awareness programs focus on awareness and hold all users to the same standard. This includes everyone from the C-suite and the IT department to anyone accessing the organization's network resources.

## Leveraging of Existing Tools for Maximum Value

When organizations get serious about cybersecurity, the conversation typically starts with a well-publicized breach and/or introduction to an advertised product or service. Contrary to popular belief, you do not need to spend a lot of money to protect your organization. Start with reviewing the products and services already in use, and evaluate whether these existing solutions are being deployed to their full potential. For example, does your organization require password complexity? Does it require passwords change after a certain period of time? Is there a policy that will lock the account after a pre-set number of failed login attempts? Many existing security features are disabled for convenience but they can leave a large gap in your organization's cybersecurity posture.

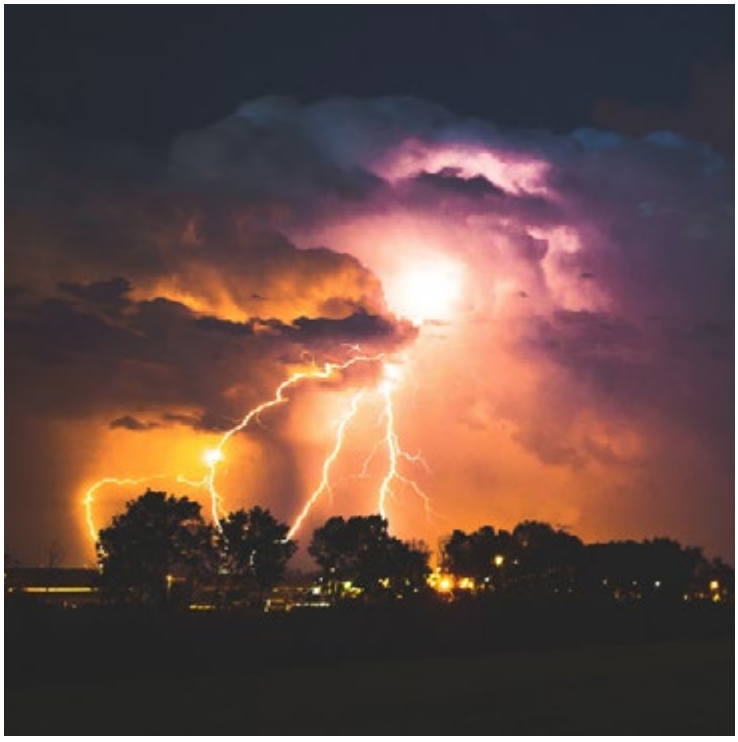


## Implementation for Multi-Factor Authentication

One of the best values among the services available for cybersecurity is multi-factor authentication. Multi-factor authentication requires a second confirmation of the identity of the person accessing the system. For it to protect the organization though, all entry points into the network must require this additional form of identity verification.

If your organization currently uses Microsoft Office 365, multi-factor authentication is included in your license. If not, there are effective, third-party multi-factor solutions available for purchase including Duo, RSA and Yubikey. A little research for the right solution will go a long way toward ensuring your peace of mind that the organization's network has protection.

## Effective Cloud Security



You have moved everything to the cloud so your cloud provider now handles your organization's cybersecurity. Not so fast! Even though Amazon Web Services, Azure or Google Cloud is supplying infrastructure as a service, your organization is still responsible for configuration and proper set-up. They will not manage your operating system updates, nor will they lock down your network. In addition, if your configuration is incorrect, your data can be open to anyone online.

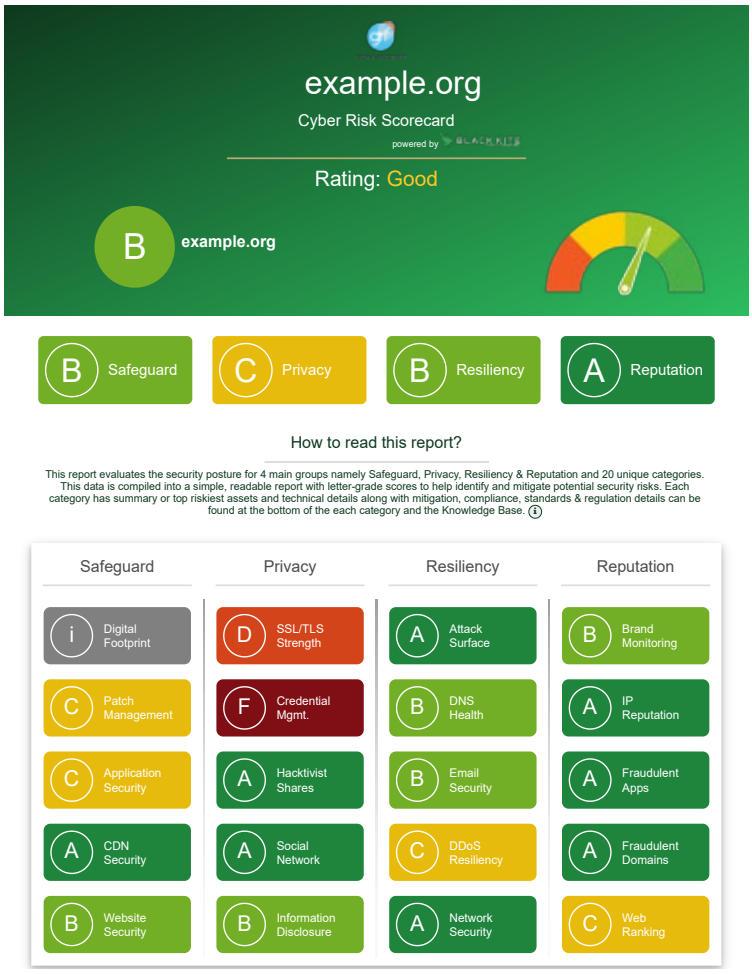
Cloud services are complex and very powerful, but misconfigurations can be catastrophic. By default, newly created S3 buckets in AWS block public access, but any slight misconfiguration can potentially open this storage to anyone. According to security firm Skyhigh Networks, 7% of all S3 buckets (storage in AWS) have unrestricted public access and 35% are unencrypted. Some of these storage buckets have intended unrestricted access, but a large number of customers are unaware that they are not protected. In addition, just because public access is initially blocked by default does not stop someone from changing the access level later.

## Assessing Your Risk with a Cybersecurity Risk Assessment and Scorecard

GRF has designed affordable packages to allow organizations to identify possible weaknesses and/or vulnerabilities by evaluating 19 security-related categories and one informational category, as shown below on a continuous basis. Many vulnerability reports are shown as a point in time often requiring the purchase another scan to see if remediation steps corrected the issues. GRF's Cybersecurity Risk Assessment and Scorecard will scan continuously for 60 days or for an entire year. This allows internal IT or outsourced IT department's ample time to resolve any weaknesses. The scan also brings awareness to potential weaknesses that arise from newly discovered vulnerabilities or possible misconfigurations during the remediation process.

Each category provides specific information about an aspect of an organization's cybersecurity posture. The security-related categories are divided into four main groups:

**Safeguard:** Digital Footprint, Patch Management, Application, Website, & CDN Security
**Resiliency:** Attack Surface, DNS Health, Email Security, DDoS Resiliency, Network Security
**Privacy:** Credential Management, Information Disclosure, Hacktivist Shares, Social Network, SSL/TLS Strength
**Reputation:** Brand Monitoring, Web Ranking, IP/Domain Reputation, Fraudulent Domains, Fraudulent Apps



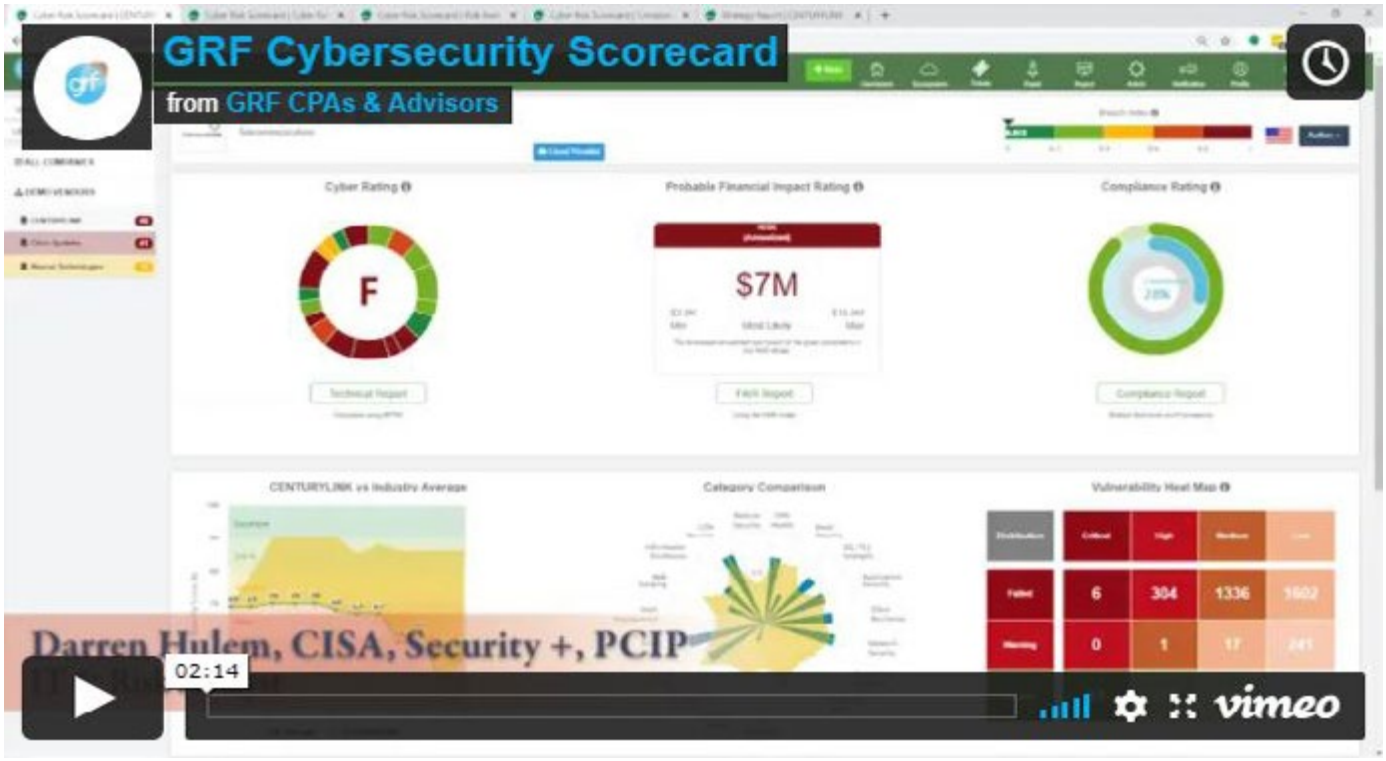

Deliverables include compiled results in a simple, readable report with a letter-grade score to help identify and mitigate potential security risk. The report summarizes technical details along with mitigation plans to improve the organizations cyber posture and compliance with stands for top risk items identified. This also includes a results debrief. Discussing these risks and your existing tools with a certified cybersecurity professional will help you develop the right cybersecurity plan to meet your organization's goals and objectives.

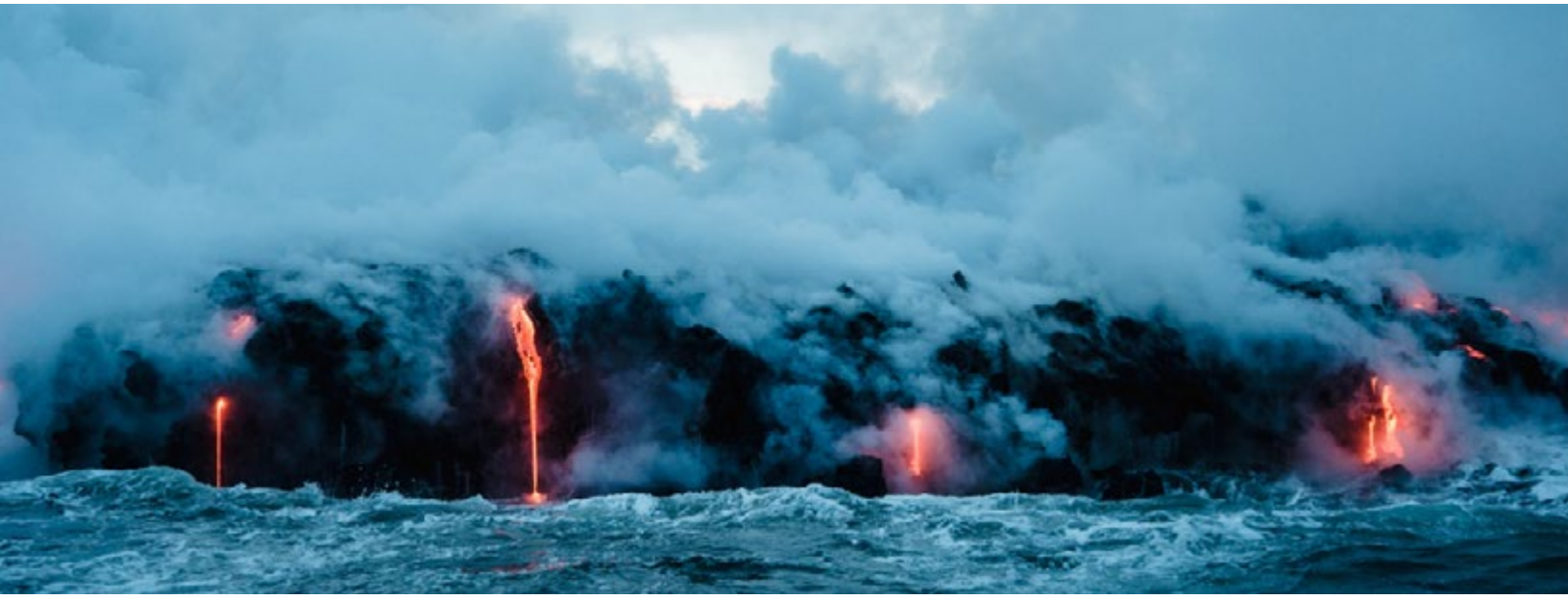
**Explore Supplemental GRF Resources:**

Be on High Alert for Ransomware Attacks

## Cybersecurity Scorecard

GRF's Cybersecurity Risk Assessment and Scorecard provides valuable information in the form of a detailed report with observations and recommendations related to vulnerabilities with respect to 20 security related categories (including fraudulent domains, patch management issues, SSL/TLS strength, IP reputation, and others). For your benefit, the results are also provided in an easy-to-understand scorecard summary which gives you a letter grade score to see where you stand against your peers. Watch the demo for more information and request a quote.



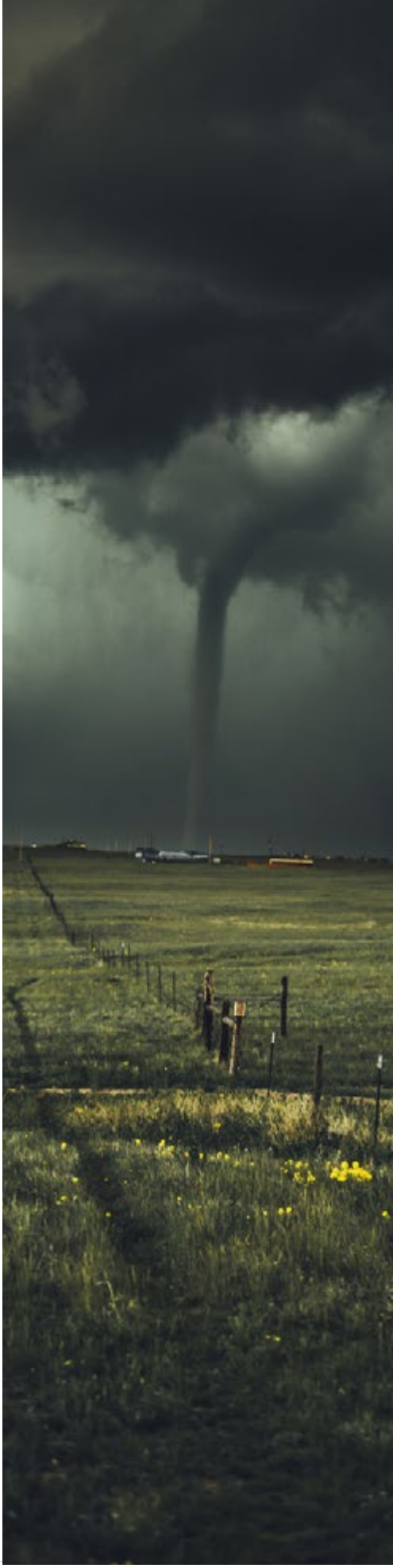



## Resources

The elements described above should be part of every organization's arsenal to prevent a potential cybersecurity breach. While this list is not all-inclusive, it can be a useful starting point for any organization concerned about cybersecurity.

These characteristics represent best practices that should be part of a sophisticated and effective cybersecurity program, but they don't necessarily require a large capital investment. Many businesses and nonprofits are surprised to learn that a number of these elements are already present in their organization and just awaiting deployment with the help of cybersecurity expertise.

For more resources regarding cybersecurity, including recent blog posts on the case for virtual chief information security officers and vulnerability scanning and penetration testing, visit our Resources page. If you have questions regarding your organization's security posture or security policies and procedures, contact Melissa Musser, Risk & Advisory Services Principal, or Darren Hulem, Senior IT & Risk Analyst at 301-951-9090 or via email at mmusser@grfcpa.com and dhulem@grfcpa.com.



## Authors


### Melissa Musser, CPA, CITP, CISA

Risk & Advisory Services Principal

mmusser@grfcpa.com



### Darren Hulem, CISA, Security+, PCIP

Senior IT & Risk Analyst

dhulem@grfcpa.com


## About GRF CPAs & Advisors

Our risk experts work with organizations to provide support for complex decision-making over a wide range of business and financial issues.

Services include Enterprise Risk Management (ERM), third-party risk assessment, internal audit, cybersecurity, privacy, fraud support, compliance consulting, and financial systems optimization. For more information on how our experts can support your organization, visit our website at **https://www.grfcpa.com/accounting-services/advisory-services/**

Headquartered in the Washington, DC metropolitan region serving clients locally, nationally and around the world. GRF CPAs & Advisors is a full-service professional services firm providing clients with audit, accounting, tax and advisory solutions.