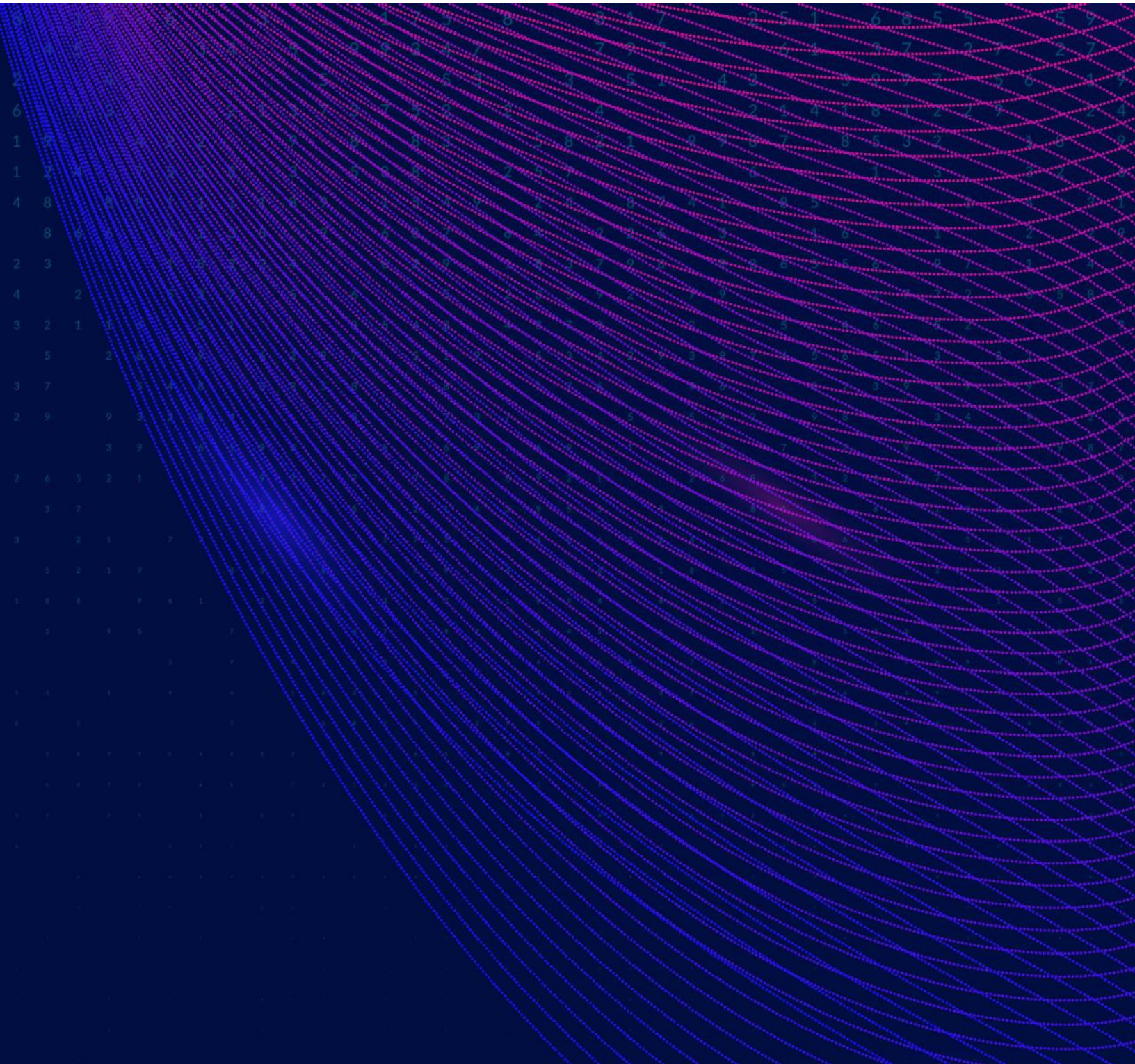
Cybersecurity Risk & Readiness

What it means to be ready and why it is important

Created by

Gray Analytics



Gray Analytics

Cybersecurity Risk & Readiness

What it means to be ready and why it is important

Gray Analytics' team of cybersecurity experts welcomes the opportunity to get to know your organization and help you prevent, mitigate, and recover from your key risks and vulnerabilities.

We have prepared this high-level document to provide some helpful, introductory guidance on a sampling of important questions related to how organizations can protect against today's growing cybersecurity threats facing all industries and be prepared for when an attack occurs.

For additional reference, we also provide a number of real-world examples of why these items matter.

Every organization is different, and the solution for ensuring protection will vary based on a vast number of variables. Gray Analytics has the knowledge and expertise to develop an effective plan of attack specific to your organization that will help you build a secure foundation to defend against cyber threats.

The Big 3: People, Process, and Technology

Comprehensive assessments of people, process, and technology are paramount to understanding the ability of an organization to detect, defend, and recover from a cyberattack. Gray Analytics provides the depth and breadth of expertise to review and understand your organization's cyber landscape in all three domains.

In today's interconnected information economy, the protection of customer information, employee assets, and intellectual property requires the proven expertise that Gray Analytics offers. From assessing the perimeter of your network to the health of your endpoints and all in-between, we analyze, recommend, and implement defense-in-depth strategies to ensure the right technology is effectively deployed against the threats.

Engaging with Gray Analytics' team of experts to perform a comprehensive assessment of your operation can help you feel confident that risks to your business are clearly identified and effectively mitigated.

In This Introductory Report

Eleven basic questions designed to help you better understand what your company is doing now to protect itself and why these items are important for every organization to consider—asking if your company:

- Provides training services related to IT security for your employees
- Has a formal incident response plan
- Has a well-defined password management policy
- Uses multi-factor authentication
- Has an acceptable use policy for information technology
- Has a formal change management process
- Has a defined hardware and software hardening and patching program
- Has an intrusion detection/prevention system
- Uses specific endpoint protection solutions
- Has backups for your systems and data
- Needs to comply with any cybersecurity and/or data privacy regulations

Does your company provide training services related to IT security for your employees?

Training for IT security is paramount in today's world as the "Human Firewall" is likely the most important line of defense against future cyber incidents. Having a well-trained and aware organization provides a level of defense that cannot be present without adequate training. Constantly reminding employees what to look for, what not to do, and what to do both proactively and in the event of a cyber incident will significantly reduce the risk of cyber-related incidents to organizations.

Assessing the readiness of human capital and providing improvement strategies is the single most important factor in reducing the occurrences of cyber incidents across an organization. Our extensive knowledge and experience in how people react to threats such as phishing attacks or business email compromise (BEC) help you create solutions that provide the first line of defense against cyber threats.

Real-World Examples

The FBI has identified business email compromise (BEC) fraud as the #1 financial threat to businesses in the U.S. (LINK). A typical BEC scam attempts to trick an employee into wiring money to the attacker's bank account. A single email can steal $500,000 in less time than it takes to read a blog post. BEC scams have caused upwards of $10.2 billion in global losses since 2015 (LINK).

Negligent employees are the top cause of data breaches at small- and medium-sized businesses across North America and the UK, according to a 2017 study (LINK). Of the 1,000 IT professionals surveyed, 54% said careless workers were the root cause of cybersecurity incidents, followed by poor password policies.

While cyberattacks on big, brand name companies are the ones that make the news, small businesses are becoming a favorite target of cyber criminals and are typically the least prepared to defend themselves. 43% of cyberattacks are aimed at small businesses, but only 14% of those small businesses are prepared to defend themselves. Regrettably, 60% of small businesses go out of business within six months after a cyberattack due to the rising cost—upwards of $200,000 on average—of an attack (LINK).

Does your company have a formal incident response plan?

A formal incident response plan is vital to organizations today. Almost every organization is at risk of having an adverse cyber incident and should be prepared in the event one occurs. Employees should know what to do and say, when to do it, and how to execute well-defined responsibilities. Organizations run the risk of not being able to mitigate and ultimately not being able to recover from a cyber incident if an incident response plan is not in place prior to an attack. Further, companies introduce risk of reputational harm if employees are not trained in who to talk to and what to say after an incident.

Real-World Example

Unfortunately, Yahoo didn't have an incident response plan in place, according to an internal investigation. The internet pioneer, which reported a massive data breach involving 500 million user accounts in 2017, actually knew an intrusion had occurred in 2014 but allegedly mishandled its response. It was discovered that Yahoo's security team and senior executives knew that a state-sponsored actor had hacked certain user accounts in 2014, but even as the company took some remedial actions, such as notifying 26 users targeted in the hack and adding new security features, some senior executives allegedly failed to comprehend or investigate the incident further (LINK).

Does your company have a well-defined password management policy?

A formal policy that includes mandatory password parameters is essential. Without such a policy and the technical controls to execute this policy, users may choose weak passwords and may or may not change these passwords with frequency. It is usually not a good idea to leave these decisions in the hands of the users. The absence of a formal password policy introduces elevated risk for cyber incidents.

Does your company use multi-factor authentication?

Multi-factor authentication (MFA) is a method of confirming a user's identity and granting system access only after presenting two pieces of evidence to an authentication mechanism (e.g., using a password and a cloud generated electronic push notification to a smart device). MFA can reduce the risk of unauthorized access to an organization's systems by a factor of 10x. Further, the use of MFA guards against credentials harvesting and satisfies compliance requirements. MFA is an absolute must for organizations today.

Why Cybersecurity Matters

- 467,361 total cybersecurity incidents in 2019—up 32% from 2018
- 5 billion records exposed in 2018
- $8 billion in financial losses from ransomware attacks in 2018—up 60% from 2017
- 12% year-over-year rise in business-targeted ransomware attacks
- $10.2 billion in global business email compromise (BEC) losses since 2015

Real-World Example

In 2017, the Guardian reported that the accounting firm Deloitte was hit in 2016 by a cyberattack that exposed the confidential emails and plans of at least six of its clients. The attackers gained access to Deloitte's systems in October or November of 2016, the report states, but the company did not discover the breach until March of 2017. Notably, the account was password-protected but did not have multi-factor authentication (LINK).

Does your company have an acceptable use policy for information technology?

It is essential for organizations to implement policies that define what company employees can and cannot do as it relates to network and computing resource access. In an overarching policy, employers must be clear about expectations for handling information, accessing the network, protecting assets, and ensuring privacy. Organizations that have no such policy set themselves up for heightened risk of cyber-related incidents based on the lack of governance for who, what, when, and how users interact with the network and information resources.

Real-World Example

Threats are always changing. For now, users and their devices are ground zero. Phishing has turned to spear phishing and whaling exploits that are well-researched and convincing enough that they are able to get even corporate executives to click links and download attachments that open enterprises up to critical risks (LINK).

Does your company have a formal change management process?

A formal change management process is very important to an organization's ability to prevent potential self-inflicted issues, such as a bad patch from a vendor, and to be able to understand when unauthorized changes have been made to a system. This process reduces risk in that all material changes to a system will be planned, approved, and documented by the correct chain of command and, as a result, can provide a measure of reliability of the information assets. Without such a process, an organization runs a higher risk of cyber incidents from insiders through, for example, poorly planned and executed changes or updates or through malicious, intentional changes to systems.

Real-World Example
The name, mobile number, and account PIN for 14 million Verizon customers were discovered unsecured online in June 2017. The leak was due to a server misconfiguration by a third-party vendor (**LINK**).

Does your company have a defined hardware and software hardening and patching program?

Hardening and patching are critical steps in maintaining an up-to-date and secure operating environment. Patching involves keeping systems, firmware, and applications up to date with the latest versions and vendor releases. Hardening limits points of entry into a system to mitigate potential risk through unauthorized access. Internal vulnerability scanning platforms help keep you up to date through scheduled network scans that alert users to vulnerabilities and necessary software updates.

Patching machines, software, and applications is one of the most basic elements of good cyber hygiene and can deter many would-be cyber incidents when executed with discipline and regularity. Having no defined patching program introduces one of the greatest risks to any organization related to potential attacks on information technology resources.

Real-World Example
Equifax, one of the largest credit bureaus in the U.S., announced in 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 143 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May (**LINK**).

Does your company have an intrusion detection/prevention system (IDS/IPS)?

All organizations need systems in place to prevent and/or detect unauthorized network access or use. IDS and IPS systems, used separately or in conjunction with each other, are cornerstones to being able to defend against both known attacks and those of a zero-day nature, which are generally attacks that occur prior to someone realizing a vulnerability is present.

Real-World Example
The need for intrusion detection/prevention capabilities cannot be overstated. The ability to detect and identify the source and analyze the extent of a compromise is crucial to rapid incident response, minimizing loss, mitigating exploited weaknesses, and restoring services. Early detection of an incident can limit or even prevent possible damage to control systems and reduces the effort required to contain, eradicate, and restore affected systems. Auditing and logging with host-level Domain Name Service (DNS) resolution capabilities are essential for improving detection and determining the scope of any compromise (**LINK**).

Does your company use specific endpoint protection solutions?

Endpoint protection is a must for every organization. It typically involves centrally-managed security solutions that monitor endpoints such as servers, laptops, and mobile devices. This level of protection is considered basic hygiene for any organization with computing resources. An effective endpoint solution guards against the most common kinds of malware and viruses, and the absence of endpoint protection increases the risk of an adverse cyberattack significantly.

Real-World Example
Consider commercial antivirus protection wisely to ensure you are getting maximum value for your investment. One advantage of commercial packages is that they update themselves regularly to stay ahead of evolving cyber threats. Plus, they usually come with spam-blockers, identity protection, and other helpful features (**LINK**).

Does your company have backups for your systems and data?

Data backups are important to aid in the restoration of data critical to your business or operation. In the event of a failure, data backups allow you to restore information from its last known good state. Data can become corrupt or lost due to hardware or software failures, natural disasters, human error, or malicious attacks (e.g., virus, malware, ransomware). Backups should be kept separate, when possible, from the rest of your system architecture, which aids in preventing corruption of the data backups in the event your system architecture has been infected by a virus or malware. Offsite backups are preferred.

Real-World Example
According to Cybersecurity Ventures, ransomware is expected to attack a business every 11 seconds by the end of 2021, and damage costs are predicted to reach $20 billion (**LINK**). The federal Cybersecurity and Infrastructure Security Agency lists backing up your data as the first action to take today to make sure you are not tomorrow's headline (**LINK**).

Does your company have to comply with any cybersecurity and/or data privacy regulations?

One of the more challenging aspects of regulatory compliance is keeping up with constantly evolving rules and understanding what applies to you. Our team offers a vast amount of experience wading through a variety of government regulations (e.g., NIST 800-171 and CMMC) and implementing practical solutions to ensure ongoing compliance. In today's world, where it seems a new requirement is released monthly, our experience and expertise allows us to stay up to speed on breaking developments and distill extensive legislation down to what really matters and what needs to be done.

Gray Analytics is proud to be authorized as a **Registered Provider Organization** by the Cybersecurity Maturity Model Certification (CMMC) Accreditation Body to provide advice, consulting, and recommendations related to CMMC requirements.
Learn more at the CMMC-AB site

Gray Analytics Can Help

Real Problems, Real Solutions: Gray Analytics Is Meeting The Need

What would you do if a cyberattack shut down your business today? Every organization, no matter the size or focus, is continually at risk of a cyberattack. In the global economy operating in the digital information age, the opportunities for bad actors to do grave and sometimes-irreparable damage are numerous.

The bottom line: those with malicious intent are out to access, steal, alter, disable, or destroy what does not rightfully belong to them. From nation-state groups to hacktivists, cybercrime to cyberwarfare, phishing attacks to denial-of-service, the tactics, techniques, and procedures (TTPs) are ever-changing and growing exponentially. Every organization requires a solution based on understanding a complex array of cyber threats and creating the best defenses against them.

We have the knowledge and expertise to guide you and your organization down the pathway to cybersecurity health. Reach out today to discuss how we can help assess your current operation to identify your key vulnerabilities and develop an effective plan of attack to secure your operation and critical resources.

Why Gray Analytics?

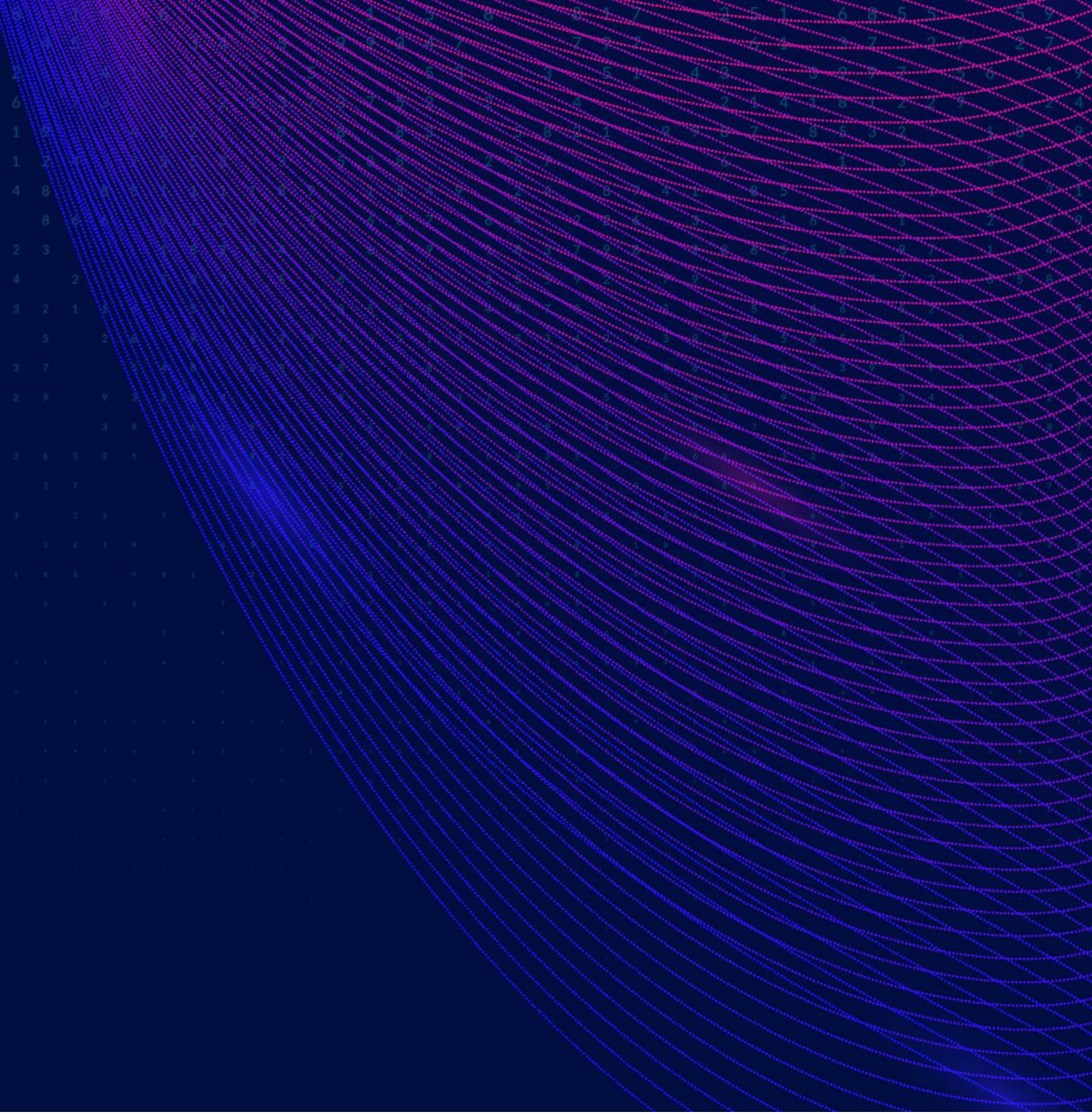
Our mission is to help our clients defend against cyber threats and solve challenging technology problems.

- We provide an independent perspective and expertise grounded in deep public sector and government experience, including work with the Department of Justice and Department of Defense.
- Our leadership team brings to bear over 125 years of experience in cybersecurity, IT, digital forensics, engineering, and technical support.
- We are honored to have earned the distinction of being named a Founding Industry Partner to the FBI National Defense Cyber Alliance.

Honesty and integrity are paramount at Gray Analytics. Our only goal is to solve our clients' real-world problems.

Our Firm's Promise

To operate with the utmost professionalism, honesty, and integrity. We promise to give the best effort with the best service possible. And we promise to treat your needs as if they are our own, because we believe that improving your security is a shared responsibility.



Gray Analytics

For more information:
256.384.GRAY
GrayAnalytics.com
info@grayanalytics.com