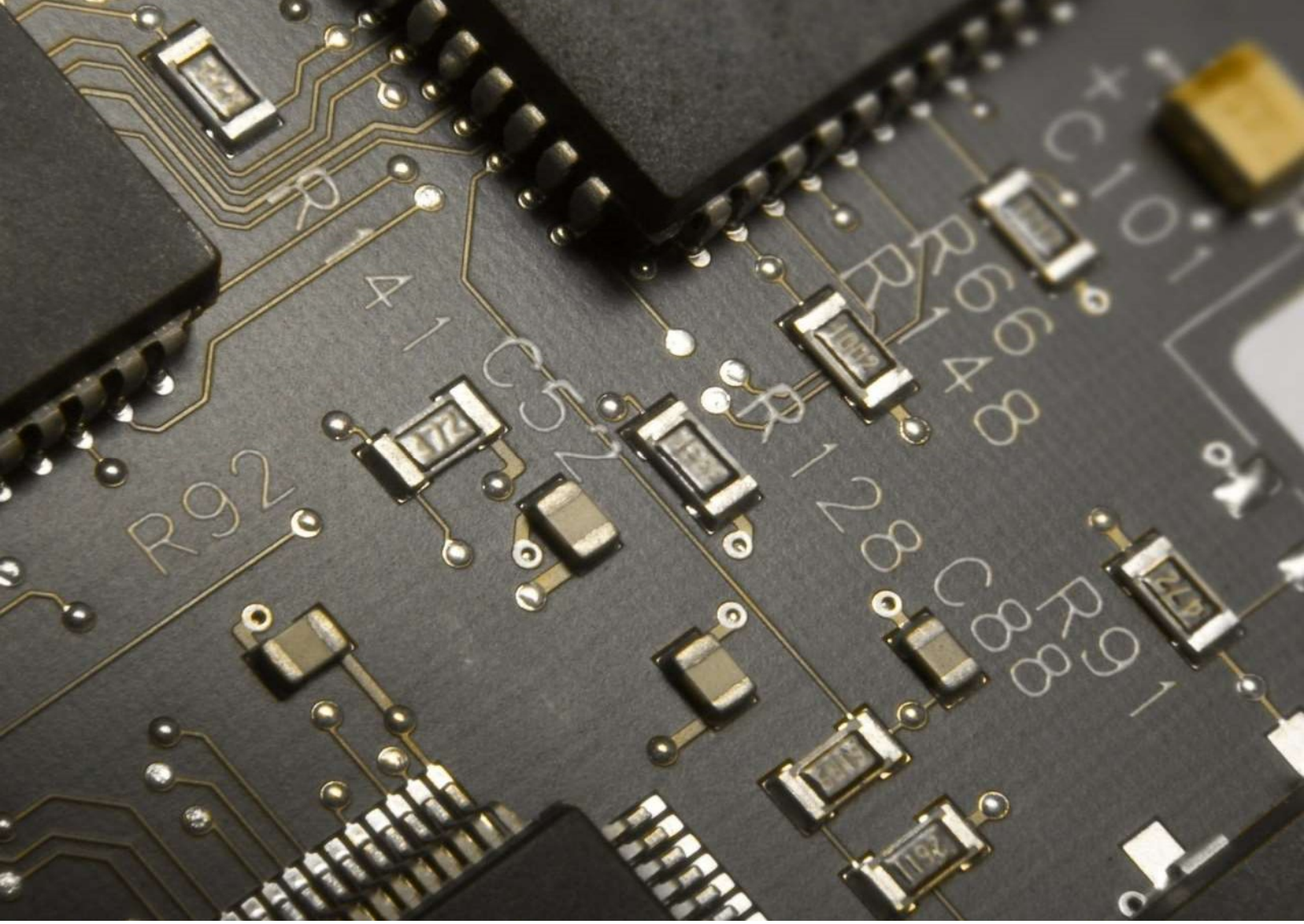


A Solution to Organizational Cyber Security Threat

RIDGE GLOBAL

AUGUSTUS FEDERAL LLC

The Cyber Threat

Every day millions of drivers enter their vehicles confident that they are invulnerable from accidents despite statistics showing that vehicular collisions are very common. To lessen the risks, individuals purchase insurance and take part in training to obtain a license.

Similarly, individuals and businesses have a high degree of confidence that the technologies they utilize keep their identities and information safe from cyber attacks despite facts such as a 2015 Verizon report that concluded that an average of "5 malware events occur every second."[1] and an *ISACA/RSA Conference State of Cyber Security* study that found that "74% of security professionals expect a cyberattack in 2016 and 30% experience phishing attacks every day."[2] Unlike driving, individuals and businesses who utilize networked technology are not required to obtain insurance or participate in training. This lack of training increases the likelihood that risks will go unrecognized, unmitigated and unaddressed.

A false sense of security may originate from the belief that cyber incidents are limited to general attacks by generic technologies focused mainly on governments and large corporations. In fact, 70-90% of malware samples are unique to an organization and this combined with the sheer volume of attacks indicates that cyber attacks should be seen as a top threat to businesses.[3] Another misperception is that large businesses are the main target of cyber attackers. These actors are opportunistic and seek out targets that are easy to exploit and since many small businesses do not perceive that they could be a target they take little to no steps to address these vulnerabilities. This threat is especially relevant to smaller organizations, as 60% of small businesses close within six months of a cyber attack and even large organizations are not immune from a cyber attack's devastating effects, as seen through examples such as Sony Studios, Home Depot and Target Corporation.[4]

The majority of cyber attacks are not targeting new vulnerabilities and the statistics of cyber security related incidents continue to fall into similar categories. These attacks can be divided into two general categories.

The first category is **Technical Attacks**, which is generally what most people think of when imagining a cyber attack. A technical attack focuses on exploiting software glitches or mistakes that allow a malicious actor to gain access through a system by using loopholes in the software and hardware monitoring a system. Generally technical attacks are combatted by intrusion detection, firewalls, encryption and up-to-date patches.

The second category of attacks is Non-Technical and usually seeks to exploit the ignorance or lack of training in the personnel that are operating the system. Whistleblower Edward Snowden is one of the most recognized attackers who used a **Non-Technical Exploitation**. Snowden acquired passwords and accessed highly classified systems and information through faults in individual operational security lapses. To thwart this non-technical insider threat, organizations must set clear user policies with ongoing education and have effective leadership and enforcement. The weakness personnel bring to the cyber security equation cannot be understated as 99.9% of exploited vulnerabilities were compromised more than a year after they were discovered and reported in the "Common Vulnerabilities and Exposures" (CVE).[5] The strongest defense against cyber attacks includes both technical and non-technical elements to make every aspect of the organization as impenetrable as possible.

To address this evolving threat, it is critical that an organization implements a unified

[1] Verizon. *Data Breach Investigations Report.* 2015.
[2] Cyber Security Nexus. *State of Cyber Security Implications for 2016.* 2016.
[3] Verizon. *Data Breach Investigations Report.* 2015.
[4] Small Business Committee
[5] Verizon. *Data Breach Investigations Report.* 2015.

Augustus Federal helps businesses to be prepared for both, **Technical** and **Non-Technical** cyber-attacks, through using the best **technological solutions** and providing ongoing **company-wide training**.

and proactive defense policy to ensure that the data and information safety is maintained on a regular basis. This security is achieved through:

a. Technology: using cyber security software that minimizes gaps and identifies breaches when they occur,
b. Training: employees must have ongoing training so they understand their role in keeping the organization safer. The continuous training must emphasize that reckless actions on any given network and system can provide a gap in the security continuum and provide access to a cyber attacker to penetrate and manipulate a system.

The bad news is that the cyber threat is increasing exponentially. Governments, individuals, and coordinated teams work 24 hours, 7 days a week searching for vulnerabilities they can exploit. The good news is that with nominal effort, individuals and companies can implement cyber security strategy backed by technology and policy that will help minimize their exposure.

Juniper Research projects the cost of cybercrime amounting to $2.1 trillion USD by 2019.

Our Team

To address global cyber security issues, Ridge Global and Augustus Federal have joined to offer a continuum of solutions to address cyber threats. The Ridge Global and Augustus Federal teams offer world class cyber security and protection services that take an enterprise-wide approach based on the thesis that any weak point in the system might be the opening for cyber attackers to exploit.

Tom Ridge, CEO of Ridge Global, was the first Secretary of the U.S. Department of Homeland Security (DHS), where he worked with more than 180,000 employees from a combined 22 agencies to create a department that facilitated the flow of people and goods; instituted layered security at air, land and seaports; developed a unified national response and recovery plan; protected critical infrastructure; integrated new technology; and improved information sharing worldwide. After DHS, Mr. Ridge founded Ridge Global and assembled a team of globally recognized experts to offer strategic counsel on identifying, preparing for and mitigating cyber risk.

The Augustus Federal team is comprised of numerous security and business professionals who deliver seamless solutions to keep information secure.

Eugene Carpino, the CEO of Augustus Global (Augustus Federal's parent company), has over 25 years of experience in business development, security & governmental affairs. Mr. Carpino worked in the national security

sector serving both local and federal government agencies, and supporting counterterrorism and U.S intelligence initiatives for the U.S. government and private sector.

Bob Luby, CEO of Augustus Federal, has over three decades of IT, Supply Chain, Cyber, and Insider Threat experience in both public and private sectors. His clients have included the Department of Defense, Defense Intelligence Agency, Department of Homeland Security, FEMA, National Security Agencies, Defense Logistics Agency (DLA), and many others.

Alec Bierbauer brings more than 25 years of experience in conducting and managing special military and government operations. Mr. Bierbauer currently serves as the Augustus Federal President.

Dale Pupillo is a senior advisor and brings 31 years of experience in the United States Secret Service.

Brian Cairns is the Director of Business Development. Mr. Cairns was a founding member of the Department of Homeland Security and has deep solution development expertise having worked at both IBM and SAIC. Mr. Cairns was the Deputy Chief of Staff at the Department of Homeland Security under Secretary Tom Ridge.

Harvey Morrison brings expertise in Data Loss Prevention, Big Data, Analytics and MRO.

Algirde Pipikaite, Vice President of International Relations at Augustus Global, brings more than 10 years of public private partnership experience. Most recently Ms. Pipikaite has spent a year at John F. Kennedy School of Government, Harvard University focusing on cyber security strategy and digital transformation policy.

Our team is uniquely equipped to combat the challenges of cyber security from the most complex multinational companies to small and medium size enterprises (SMEs). Our experts can quickly address cyber security issues, respond to breaches, and assist in implementing security technologies and policies that reduce exposure to infiltrations.

Our Approach

Ridge Global and Augustus Federal offer an effective, unique and comprehensive approach to addressing cyber security. We take an enterprise-wide perspective on the **technical** and **non-technical** aspects to ensure complete and secure coverage of organizational assets. We begin with an in depth security assessment where we identify and gauge threats and breach risks. This information allows us to create a strategic threat and capabilities assessment that determines the most effective course of action.

Following the initial assessment, the breach response planning takes place, where we establish incident response and crisis management plans to approach cyber incidents with precise methodology and practices. High security risks are identified and mitigated according to a developed action plan, and we determine insurance and breach response services to provide clear direction in combating cyber incidents.

Our focus on governance compliance is accomplished by determining clear roadmaps and strategy that best address cyber security risks. In addition, our approach includes cyber insurance and effective breach response systems to establish efficient and swift protection services. We have also characterized our approach with a focus on continual maintenance, especially in regards to personnel, which is one of the greatest risks to an organization's cyber security. The need for teams and groups to communicate via technology has created avenues for attackers, especially exploiting emails and social media tools. In light of this important risk, we emphasize training and education in our continual maintenance to ensure secure communication and distribution of data and intellectual property. However, maintaining current security measures is not limited to non-technical aspects, as we continually work to improve technical efforts and keep patches and all lines of defense up-to-date. From top to bottom, our approach is characterized by an

organic procedure that begins with an assessment and planning, which produce security measures to suit organizational needs by minimizing risks and threats.

Our Methodology

During all of our interactions regarding cyber security, we operate through a methodology that is designed to inform, assess and act.

Informing organizations is essential for a robust cyber defense and we want to equip companies with the knowledge to fully understand threats and solutions available to them. Understanding the threat is vital when establishing effective security measures based on education and training. We prioritize the delivery of information to the board and senior management, enabling the creation of an enterprise-wide intelligence aware of specific security risks across the organization. Informed assessment custom to an organization as well as good controls leads to reduced cost and more powerful cyber security. After informing and assessing an organization, we establish a technical incident response using CyFir technology, which is based off of a prioritized assessment. This method allows us to provide solutions in days, instead of weeks or months. We tailor education and training based on the prior assessment. We design programs that are appropriate to individual audiences all the way from the boardroom to the work force. This three stage methodology creates clear strategy to find risks and threats and establishes enterprise-wide defense intelligence.

Complete Portfolio of Solutions

Ridge Global and Augustus Federal have come together to offer a complete portfolio of solutions to help protect businesses from cyber threats. Combining innovative technology with an integrated cyber security planning, we help keep organizations secure. Our solutions include protection, insurance, education and response plans, and each of these are tailored to the individual needs of a company or organization.

Protection

Cyber attacks occur constantly and without a solid protection plan, sensitive data is vulnerable to breaches. In a previous era, cyber attacks usually sought to bring down a corporation through the deletion of data or the disruption of software. As Internet has evolved and economy became more digital, the sophistication of cyber-attacks has increased, leaving businesses more vulnerable than ever. Companies can now have their bank records, customer's information and other sensitive information stolen and their reputation destroyed. Having a robust cyber security plan is an essential component of running a business that is operating in today's marketplace.

The Ridge Global and Augustus Federal process begins with an aggressive assessment evaluating and managing the risks and vulnerabilities a company faces. Once the situation is analyzed and understood, we utilize a variety of cutting edge technologies for rapid threat detection, identification and response. These technologies give us an insider threat and data protection platform for complete data visibility, control and loss prevention.

CyFIR

As part of our protection offering, we utilize CyFIR, a solution offered by CyTech Services that focuses on increasing the speed to resolution of cyber security issues. Founded in 2002, CyTech quickly established a respected reputation for technical data collection, exploitation and forensics. CyTech supports a client base focused on the Department of Defense, but also has significant experience working with other government, commercial and legal clients. CyFIR delivers customized solutions in the form of processes, people, infrastructure and support that leverage both state of the art technology and superior service standards.

When encountering a cyber intrusion, one of the most important factors is the speed at which the incident can be detected so that resolution can be achieved as promptly as possible. Often malicious code can enter an organization's network and remain hidden for months. Recent studies show that it took organizations a median of over 200 days to discover incidents after the event of intrusion, and even then, notification came by way of a third party.[6] CyFIR dramatically shortens this time frame by quickly identifying, isolating, remediating and removing threats from an organization's system.

Rapid and thorough detection requires a powerful tool that will seek out and find intrusions and potential points of entry. CyFIR can quickly be deployed to find critical information so decisions can be made in minutes and hours, not days and weeks. A traditional system can take weeks to analyze as a whole, whereas CyFIR depends only on the time necessary to analyze an individual endpoint, allowing for significantly quicker scan times. This is possible because of the distributed nature of the CyFIR software, which allows each endpoint to self-assess and report. 100% of the endpoints in a system can be concurrently searched, which enables a dramatically faster incident response time. Additionally, since the assessment is distributed to the individual endpoints, there is no requirement for constant or concurrent connection to successfully perform an assessment. An individual workstation will initiate a scan, and then report back once it is able. Threats can be detected on an individual level, independently of the state of the system.

The CyFIR databases and malware detection capabilities represent the most updated and comprehensive information in the world. Our sources provide information that ensures CyFIR will find new, old, and persistent threats. CyFIR determines good processes, bad activity, and unknown processes that demand further investigation. CyFIR provides a complete picture of all system activities.

Moreover, other methodologies depend on a centralized processing architecture that is inefficient and time consuming. Only a handful of computers are inspected at a time, which delays investigations and prolongs the time between detection and response. Conversely, CyFIR utilizes a distributed processing architecture, where endpoints themselves become forensic level investigation systems. Investigators now have total visibility of running processes, open sockets, open files and more. Analysis, searches and file review can occur live, in real time remotely without indexing delays.

Moreover, these processes can be actively running while users perform daily activities on devices without interruption. CyFIR enables the detection of threats across an entire enterprise in mere seconds, with no delay.

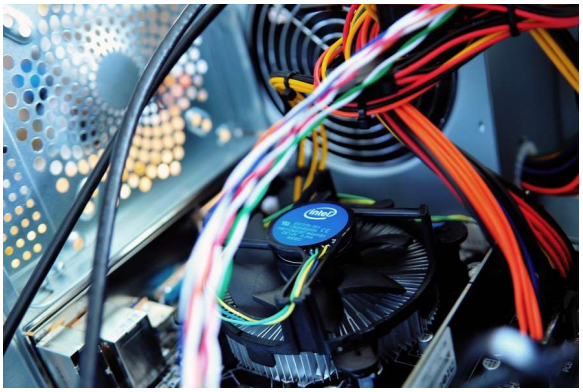
The speed of CyFIR is especially helpful in the case of an intrusion or when incident is actually occurring. Traditional system analysis and forensics can take months, but with CyFIR an intrusion can be quickly understood, and steps can be taken to neutralize the risk. Speed is central to CyFIR's effective action plan.

[6] Mandiant. *M-Trends(registered) 2015: A View From the Front Lines*. 2015.

Undetected intrusion can go on for weeks, months or even years, inflicting massive damage and loss of information, but CyFIR reduces reaction time and begins finding answers almost immediately.

Insider Threat Detection

One of the key features of CyFIR is the insider threat detection capability. Insider threat presents unique cyber security challenges, as the malicious actors are intimately familiar with proprietary information and the internal system. External cyber attacks are more easily identified because of their foreign signature on a system, but an insider attack can be harder to recognize. CyFIR's ability to completely monitor an entire system in near real time reveals activity from an insider threat much more quickly than traditional tools. Additionally, the robust technology provides very detailed information that can be used to effectively carry out an insider threat investigation.



Encryption

In order to keep sensitive data safe and out of the hands of malicious actors, encryption is a common historical solution. However, as technology has evolved, traditional encryption has lost some of its power because of the faster processors and cloud computing which is able to "crack" the code of encryption. To keep information safe, we use even more advanced tools that make deciphering data impossible without special access. We use technology from CertainSafe® to securely store information in a way that still allows the user to access it.

The process starts with "MicroTokenization," in which the data being transmitted or stored is converted into a MicroToken that contains none of the original data. This MicroToken is then encrypted and is free to be used and transmitted. When the appropriate end user receives the MicroToken, it can only be deciphered through the use of the CertainSafe® MicroToken engine. If the token were to fall into the hands of an attacker, deciphering it would reveal nothing of the sensitive data for which it acts as placeholder.

The CertainSafe engine replaces sensitive information with MicroTokens and simultaneously encrypts and stores the sensitive information on the CertainSafe secure server. This enables an organization without a robust security infrastructure to safely communicate and store data through a third party.

Managed Payment Card Industry

Payment Card Industry Data Security Standard (PCI DSS) compliance is designed to protect businesses and their customers against payment card theft and fraud. Our experts work with a company to ensure the security of their systems, transactions, and valuable information are safeguarded even beyond industry compliance standards. Our managed PCI program assesses any gaps in compliance by undergoing a penetration test of current systems to identify risks and non-compliance issues. Following this assessment, a remediation plan and roadmap are created and a Qualified Security Assessor (QSA), an independently certified individual, virtually joins organization to assist with planning and execution. After non-

compliance issues are addressed, efforts shift towards instituting and maintaining efficient and cost-effective PCI compliant operations before the final assessment and report of compliance. Even in the event of an unpredictable change, where a non-compliance issue can surface, the QSA works with the organization for up to 45 days to correct any issues, apply for an extension, and/or issue a report of non-compliance. Overall the program is divided into three phases over the course of the year.

Phase 1:

- Length: one to two months
- Onsite gap assessment (typically 2-3 days)
- Penetration Test
- Formulate remediation plan/roadmap

Phase 2:

- Monthly subscription (typically 4 hours per month)
- Certified QSA virtually joins organization assisting planning and execution

Phase 3:

- Final Assessment
- Report of Compliance

Predictive Analytics

Just as it is imperative to have formidable protection in light of potential cyber threats, an organization must understand the behavior of the attackers themselves to develop robust cyber resiliency. To this end, Augustus Federal and Ridge Global have teamed with Syntasa to offer powerful tools to translate big data into effective analysis that informs established cyber security strategy. Most other methods of analysis are mainly historical in nature where insight is only retrospectively available. We recognize the need for a timely technique and Syntasa offers data analysis and visualization in real time. Moreover, Syntasa's predictive analytics capabilities are utilized in Federal and Financial settings including applications in threat and fraud detection. These services in tandem with Syntasa's big data analysis are powerful in providing predictive analytics to organizations that desire to better understand and prepare for cyber security incidents.

Mobile Security

We recognize the current "bring your own device" era of enterprise mobility, and implement industry-leading tools and technologies for enterprise application and device management. Our partnership with Apperian (www.apperian.com) provides enterprise-grade security and management for mobile apps and data. We offer secure data distribution and application management to both managed and unmanaged mobile devices, supporting the extended enterprise of employees, contractors and dealers. Our security allows for geo-fencing, network restrictions, and app-level VPN. We also install app-level security, policy and governance to ensure a strong and resilient cyber defense.

Insurance

Companies must protect their assets and brands from the growing threat of cyber attacks. Depending on the nature of a successful attack, a company runs the risk of losing business through the damage to their reputation, loss of important information or actual theft of funds. To address the damage of a cyber attack, Ridge Global and Augustus Federal offer best in class insurance solutions.

To address the potential damage of a cyber attack, Augustus Federal and Ridge Global, together with Lloyd's of London, offer best-in-

class informed assessments aligned to cyber insurance. This approach offers a superior integrated risk management and insurance offering as it identifies specific threats and vulnerabilities. This identification enables an organization to take risk-reducing corrective action that may reduce insurance premiums. We offer tiered solutions to match the different drivers within markets based on size and exposure. Some of our policy highlights include limits up to $50 million USD, ongoing monitoring and risk management, worldwide coverage and multi-year terms. Additionally, our coverage includes privacy liability, privacy regulatory claims and security breach costs. This approach allows leaders to understand the return on investment that an informed, end-to-end, tailored cyber protection strategy brings to the organization.

Policy Highlights:

- Limits up to $50 million
- Available coverage includes Privacy Liability (Including Employee Privacy)
- Privacy Regulatory Claims, Security Breach
- Response, Security Liability, Multimedia Liability
- Ongoing monitoring and risk management
- Risk management budget available
- Worldwide coverage
- Multiyear terms available

Coverage is offered through Ridge Global and is combined with segment-specific risk management and other pre-breach services to ensure that organizations efficiently and effectively create a culture of cyber resilience. Ridge Global addresses the different drivers and circumstances within the marketplace by offering tiered solutions with the Enterprise Plus, Enterprise and Professional packages.

Cyber Insurance is an essential part of any cyber protection plan.

Education and Training

A major element of cyber security is the human element, as human error contributes to at least 95% of security incidents.[7] While an attacker might be able to infiltrate a system using a purely technical process, this is much more difficult to accomplish than exploiting human error to gain access. As a recent study demonstrated, 25% of security professionals lack faith in their team's ability to respond to cyber incidents. Within this number, 6 in 10 believe their staff is not capable of handling anything beyond simple intrusions and attacks.[8]

Because the use of technology is widespread within companies and society we believe training is essential at every level. Effective leadership and enforcement is crucial in maintaining security measures, and part of our training efforts focus on helping senior executives and board members understand the critical concepts for managing cyber risk and leading a culture of resiliency. In addition, we provide technical training and certification programs for IT and cyber security employees to ensure that the first responders are confident in their ability to address cyber incidents on a variety of scales. We also design programs to educate technical and business unit managers on how to lead cyber security programs within their areas of responsibility. More generally, we believe that all endpoint users must be trained in

[7]ThreatTrack. The People Problem: Cyber Threats Aren't Just a Technology Challenge. 2015.

[8] Cyber Security Nexus. *State of Cyber Security Implications for 2016.* 2016.

cyber policy and risk-avoidance, as they are often the first points of contact with potential cyber incidents. Knowledge and understanding of best practices in cyber security are some of the most powerful weapons to combat attackers.

***25%** of security professionals lack faith in their team's ability to respond.*

Our training programs are created with engaging content in close collaboration with leading experts at NAVEX Global, a company that has worked with more than 12,500 organizations to protect and defend against a variety of internal and external threats. We utilize professional actors and scriptwriters to make content engaging and relevant. Our unique and compelling video scenarios and interactivities are designed to simulate real world situations to ensure that a company's personnel are equipped to provide effective defense against any attempted cyber attacks or data breaches.

Our Training Solution:

- Engages learners
- Raises awareness of relevant high risk cyber threats
- Drives behavior change
- Assists in building a culture of security and resilience
- Helps prevent future mistakes and mitigate risk areas
- Creates an overall more cyber-secure environment

Response

Cyber threats and attacks are inevitable, so it is important for organizations to take steps to defend against them as well as have plans in place for how to respond and recover from an attack. With no response plan, a security breach or attack can spiral out of control and can cause much more damage than if it was dealt with in a timely, effective and controlled manner. Quick, decisive and informed action can dramatically limit the damage done by an intrusion or breach. A cyber-attack can sound intimidating, but with the proper procedures in place anyone can be equipped to respond to an incident.

Ridge Global and Augustus Federal offer strategic advice to support enterprise operations before, during and after a breach occurs. We offer robust response and recovery services to meet evolving threats, constant threat monitoring identification & mitigation, leading cyber forensics, and we support investigation, prosecution, and remediation. Moreover, we work with the leadership to make sure communication plan is prepared properly and main stakeholders, investors and customers are not kept in the dark, if a cyber-attack happens.

Conclusion

Cyber security is a critical topic that all organizations must address in today's digital marketplace. The advent of technology such as cloud based computing and collaborative documents presents an enormous opportunity for businesses to streamline their processes and increase productivity. However, if an increase in technology use is not accompanied by commensurate protective cyber security measures, the organization will likely become the victim of a successful cyber attack.

As technology advances, cyber security will be more important than ever.

For companies with no core competency in cyber security or companies that would like to confirm their security, their best option is to partner with a dedicated cyber security firm. This partnership allows an organization to have a team of experts take an unbiased look at current systems and policies to determine how vulnerable an organization is. It is important to provide uniquely tailored solutions that are specifically designed to protect the individual needs of different companies.

At Ridge Global and Augustus Federal, we combine leading cyber security expertise with a team dedicated to ensuring clients' operational success. We provide a complete suite of services that are designed to offer comprehensive protection from cyber threats.

Sources

1. Business Continuity Institute. *Horizon Scan Report*. 2016.
2. Cyber Security Nexus. *State of Cyber Security Implications for 2016.* 2016.
3. Juniper Research. *Cybercrime and the Internet of Threats*. 2015.
4. Mandiant. *M-Trends(registered) 2015: A View From the Front Lines*. 2015.
5. Small Business Committee: http://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=325034
6. ThreatTrack. *The People Problem: Cyber Threats Aren't Just a Technology Challenge*. 2015.
7. Verizon. *Data Breach Investigations Report*. 2016.
8. Verizon. *Data Breach Investigations Repor*t. 2015.