Guidepost

CYBERSECURITY CONSULTING

Nearly every aspect of life is connected to the digital landscape. This means your business can face a host of security risks, liabilities, and challenges. To guard against sophisticated cyberthreats, you should be thinking about a comprehensive security plan to protect your network and data and mitigate exposure to a potential breach.

An effective cybersecurity program starts with a framework that includes a strong governance model, comprehensive policies and procedures, and a commitment to adhere to industry best practices and standards. It includes regular penetration testing to identify and evaluate gaps in network security, and a plan to make the digital environment more predictive and secure.

Every organization must determine what cybersecurity processes are right for its business. In some industries, the processes that an organization must implement are guided by industry requirements, federal regulations or both. Our team understands how compliance with NIST CSF/800 Series, CIS, ISO, PCI-DSS, COBIT, SOC 1, SOC 2, SOC 3, NYDFS Part 200/Part 500, Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST) certification, Service Organization Control 2 (SOC 2) audits, and other evaluations against established frameworks and standards are critical to an organization's success.

We treat cybersecurity with an integrated approach to protect against the full spectrum of cyber and physical security issues. These innovative capabilities are specifically designed to improve cyber defense capabilities and prevent or remediate cyber security incidents when they occur.

Information Security Program Assessment + Maturation

The success of security policies and systems depends, in part, on their proper implementation and use. A continuous improvement process is needed to sustain a security program on a day-to-day basis.

Our information program assessments and maturation services lend an objective, expert eye to current and future system needs. We will help evaluate and implement all the facets of an efficient and optimized information security plan that is tailored and designed to grow as business needs change.

Our services include:

- Comprehensive guidance to help craft the right processes and controls for information security management system
- Assistance with the creation or modernization of information security policies
- System updates and patch management analysis and implementation strategies
- Insight into the necessity and priority-order of potential upgrades, updates, and maintenance
- A gap analysis to help identify and measure risk exposure with metrics management

Cybersecurity Governance

There are more security governance measures influencing businesses than ever before. Without proper management and oversight, it's easy to overlook an aspect of the governance framework. Daily operations may carry on as if the proper systems are in place to manage compliance only to find out something has failed during a compliance audit.

Our cybersecurity governance remediation services provide peace of mind. We've built our process around existing and evolving regulatory requirements and procedural requirements. We can set up the most cost-effective and efficient systems and procedures for maintaining compliance and tailor them to suit the realities of any business.

Application Security Threat Evaluations

The risks associated with regulatory violations, security breaches and data leaks are very real, and it is essential to understand the systems and standards external technology providers operate within to control and mitigate exposure. Your third-party IT and software developers need to operate within standards that meet regulatory guidelines. If you are outsourcing even a fraction of your application services, managing several independent developers and service providers can seem like an impossible task.

We can evaluate business partners, vendors, and anyone else with whom sensitive data is shared to ensure they meet industry and security application standards. Additionally, we can assist with overseeing design and control measures to ensure that new and continuing providers meet security requirements.

Our services include:

- Third-party review to ensure software code meets industry and compliance requirements
- Evaluation of third-party developers, manufacturers, and integrators to ensure they follow secure software coding principles and regulatory guidelines
- Objective analysis and testing of application code for potential bugs, holes, and weak points
- Manual penetration testing for software, systems, and code
- Insight on the most cost-effective solutions for ensuring external providers meet or exceed internal standards and industry regulations

Operations Security Design + Project Management

Operations and system management activities collectively make up the operational security design. From data loss prevention and email spam protection to denial of service and data breach or leakage, there's an infinite number of challenges to address on an ongoing basis.

We offer a production-oriented, third-party perspective to objectively evaluate current systems and processes. Using our holistic methodology and comprehensive approach, we can help assess vulnerabilities and suggest realistic need-

based solutions.

Our services include:

- Threat prevention tactics and recommendations
- Solutions to help protect against credible threats and fill risk gaps
- Suggestions for improving cyber security incident management

Remediation Services

Once a data breach or system compromise has been contained, the critical mission becomes remediating the damage, improving technical security and updating policies and procedures to minimize the risk of recurrence. The comprehensive services we offer make us uniquely qualified to assist in the transition from short term reaction and response to long term security — strengthening human and digital operations.

Virtual Chief Information Security Officer – VCISO

Sourcing, hiring, and paying the right Chief Information Security Officer and cybersecurity team can be impractical, daunting, and expensive.

Through our vCISO program, you have access to a full team that is quickly scalable and makes sense for you practically, operationally and financially.
Our vCISO team provides you with the same level of expertise, services and benefits of seasoned, highly certified cybersecurity experts and a CISO.

Security and compliance risks will be identified and mitigated as if you had a full team in-house, but at a fraction of the cost.

Our vCISO team helps with:

- Cybersecurity Roadmap
- InfoSec Policy Development
- Security Compliance Standards
- DevSecOps
- Security Remediation Tracks Intelligence
- Security Tech Product Evaluations
- Secure Architecture Development
- Risk Management
- Hands-On Technical Support
- Risk Management Model

Cyber Investigations

Our computer forensics solutions can help you strengthen a case, avoid pitfalls, identify opportunities, and make informed decisions. The team includes investigators who have served as federal and local prosecutors and law enforcement agents, digital forensic experts and reverse malware engineers, forensic accountants, data and intelligence analysts, and former federal agents from the U.S. Department of Homeland Security, Central Intelligence Agency, Federal Bureau of Investigation, Drug Enforcement Administration, Internal Revenue Service, U.S. Secret

Service, and the U.S. Marshal Service.

Our unique capabilities, relationships, tools, and ability to convert "tech speak" into valuable information for attorneys and in-house counsel, enhance responsiveness and investigative efficiency when responding to complex cyber challenges.

Our team includes experts in the forensic analysis of data from Windows, Mac, and Linux computers and servers, mobile devices, and Cloud-based platforms and applications. Specialists regularly testify as experts in state and federal courts, liaise with law enforcement and regulators, and work with investigative professionals to provide a seamless investigation

Data Protection

A data breach or leak can devastate even the most well-regarded company and compromise its reputation, costing potential customers, investors, and partners.

Our team of information security specialists can assist with enterprise-level data protection tailored to where and how you conduct your business. From meeting technical and governance requirements for each country in which the company operates, to developing solutions for controlling vulnerabilities, we assist with every security challenge.

We can help you:

- Meet the data encryption, storage, and sharing requirements of various regulatory statutes
- Earn the trust and positive regard of customers, employees, business partners, and investors
- Implement data protection measures for both U.S.-based and international offices
- Maintain compliance through dynamic risk control measures designed to grow with the business
- Ensure third-party suppliers are adhering to data protection standards