Guidepost

CYBER SECURITY CONSULTING

The e-commerce revolution has brought speed and convenience to all industries and sectors, but it's also brought a host of security risks, liabilities, and challenges. Beyond considering physical risks, a plan is required for network and data protection to mitigate exposure of a potential breach. Data breaches are considered the number one risk to enterprises in recent security assessment polls.

We treat cyber threat mitigation with a holistic and top-level planning approach through our comprehensive threat, risk and vulnerability management services to protect against a full spectrum of cyber and physical security issues. These innovative capabilities are specifically designed to improve cyber defense capabilities and prevent or remediate any incidents when they occur.

With our extensive experience and unique approach, we lead organizations through the planning, design, and implementation of their virtual systems. Our experts can identify and evaluate gaps in network security that may be causing unnecessary risk exposure and suggest the most effective solutions. Once the weak points have been identified, we can help design a cyber security plan for implementing services and processes into the digital environment to make it more predictive and secure.

WE APPLY AN APPROACH TO CYBER THREAT MITIGATION THAT WILL:

- Help determine adequate mitigation controls needed to protect critical assets and business processes
- Evaluate the mitigation and defense posture of current processes and systems, using applicable major security standards, including PCI, as a benchmark
- Determine what; if any, legacy systems need to be updated and enhanced
- Assess network vulnerability and provide countermeasures and penetration testing assurance
- Build an adaptive cyber security model that can evolve with the changing virtual landscape

Application Security Threat Evaluations

In this technology-driven and competitive business era, a single data breach can have a far-reaching negative impact on an organization's reputation and bottom line. The risks associated with regulatory violations, security breaches and data leaks are very real, and it's essential to understand the systems and standards external technology providers operate within to control and mitigate exposure. Each company's third-party IT and software developers need to operate within standards that meet the regulatory guidelines of industry and security requirements. For a modern

company that outsources even a fraction of their application services, managing various independent developers and service providers can seem like an overwhelming and impossible task.

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

Our application security and threat mitigation services include:

- Third-party reviews to make sure software code meets industry and compliance requirements;
- Evaluations 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; and
- Insight on the most cost-effective solutions for ensuring external providers meet or exceed internal standards and all industry regulations.

Cyber Assessments

The success of security policies and systems depends, in part, on their proper implementation and use. A continuous improvement process is required to sustain a security program on a day-to-day basis. The program must meet the business needs and appropriately mitigate security risks.

Guidepost Solutions 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's perfectly tailored and designed to grow as business needs change.

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; and
- A gap analysis to help identify and measure risk exposure with metrics management.

Cyber Investigations

At Guidepost Solutions, our computer forensics solutions help clients strengthen cases, avoid pitfalls, identify opportunities and make key decisions. The team includes investigators with backgrounds 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, the Federal Bureau of Investigation, the Internal Revenue Service, the U.S. Secret Service, and the U.S. Marshal Service who have extensive experience testifying as experts in federal and state courts.

Our unique capabilities, relationships and tools, coupled with professionals who convert "tech-speak" into valuable

information for attorneys and in-house counsel, enhance both responsiveness and investigative efficiency to respond to the increasingly complex cyber challenges clients face – nationwide and on a moment's notice.

Services

Our professionals are expert in the forensic analysis of data from all 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. Specific expertise includes:

- Theft of trade secrets
- Employment disputes
- Regulatory investigations
- Threat, vulnerability, management & identification
- Real-time support and administration
- Computer / network forensics
- Data breach analysis
- Cyber security assessments
- Client-specific "Watch Lists"
- Overt penetration testing
- Data privacy analysis
- Third-party security analysis
- Technical surveillance counter measures

Our team understands that computer forensics may be used for a variety of tasks, such as finding the "smoking gun" e-mail, proving deliberate spoliation by an opposing party, or trying to make sense of suspicious computer activity on the day a key employee departed. We specialize in focused, aggressive computer investigations into intrusions, internal misconduct, phishing scams, malicious software and other digital attacks.

Our cyber investigators routinely synchronize their work with our firm's more traditional investigative resources, such as surveillance, research and interviews. This provides our clients with a formidable synergy of investigative skills that sets us apart from other agencies that operate only without or within the digital arena.

We regularly advise attorneys and corporate clients on preserving, analyzing and utilizing computer evidence in litigation, regulatory proceedings, presentations to law enforcement and governmental investigations. We perform all forensic investigations under the assumption that court testimony will be required and adhere to law enforcement standards of chain of custody and evidence storage. Our investigators have experience as court-appointed experts and in giving testimony under cross-examination.

Cyber Security Governance

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

Guidepost Solutions cyber security governance remediation services provide peace of mind. We've built our process around the 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.

Data Protection

As reliance on technology in business becomes greater, the need for data protection and information security grows more important. A data breach or leak can devastate even the most well-regarded company and compromise its reputation, costing potential customers, investors, and partners for years to come.

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

Our data protection and information services can help:

- 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; and
- Ensure third-party suppliers are adhering to data protection standards.

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 required to sustain a security program on a day-to-day basis. The program must meet the business needs and appropriately mitigate security risks.

Guidepost Solutions 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's perfectly tailored and designed to grow as business needs change.

Program assessment and maturation 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; and
- A gap analysis to help identify and measure risk exposure with metrics management.

Operations Security Design + Project Management

One of the most important aspects of cyber threat mitigation is the day-to-day operations and system management activities that 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.

Guidepost Solutions operational security services 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 operations security design and project management services include:

- Threat prevention tactics and recommendations;
- Solutions to help protect against credible threats and fill risk gaps; and
- Suggestions for improving 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 provide make us uniquely qualified to work with a client and assist in the transition from short term reaction and response to long term security strengthening of human and digital operations.