TRUSEC CONSULTING

Information Risk Management Services

INFORMATION RISK MANAGEMENT

THE CHALLENGE

In today's risk environment, the fundamental assumption that information assets are under active attack by determined adversaries must be built into the cybersecurity strategy. The long term loss of shareholder value from public and market perception of poor cybersecurity practices can last for years after a major incident. Strong information governance and forensic readiness, and a host of compliance items dealing with data protection and corporate governance, mean that information risk management practices should be appropriate to the threat and consistent with industry and peer practices. Trends in globalization, new regulations, shorter response times and increased business complexity have brought the importance of risk to the forefront, placing an additional burden on the already busy Information Risk Managers. In this light, proper implementation and governance of an Information Risk Management strategy is key to meeting the challenge of an openconnected world.

INNOVATIVE RISK MANAGEMENT

TruSec Consulting has extensive management leadership experience developing, auditing, and implementing effective information risk governance and cybersecurity programs for organizations at all stages of maturity. TruSec considers all facets of the information defense paradigm when establishing policies, controls and practices which manage the information lifecycle across the extended enterprise by addressing organizational risk from a Data Asset Value perspective. Our team includes credentialed information security experts, former and current CISO's, cyber forensics analysts, and experts in business resiliency and crisis management. Working collaboratively with clients, we provide solutions to the most difficult information risk challenges modern organizations are confronted with by offering expert analysis, information risk road-mapping, strategic vision development, and framework audits as functional tools that ultimately bridge strategy to execution in ways that build continuous improvement and success.

Operational Security Testing

Information Risk Assessment & IT Audit Services

Information Security Educational Seminars

Virtual Chief Information Security Officer

info@truesecconsulting.com | www.truesecconsulting.com | 855 TRUSEC 1

SOCIAL RISK MANAGEMENT ASSESSMENT

Modern cyber-attacks focus on the human component by exploiting gaps in defenses against socially-focused attacks. Social Information Risk Management is the other half of the Cyber-security equation, as it's much easier to get data out of unprepared employees than to break into technically well-defended and monitored systems. Addressing Social Risk within your existing Information Risk Management program is a critical piece of your information security strategy, starting with a posture assessment of your current Social Risk Management program.

vCISO (VIRTUAL CISO)

Most organizations require a CISO-type role well before they grow large enough to afford a full time leadership resource. The vCISO service is designed to provide an organization in the early-to-mid stages of information risk maturity a dedicated part-time executive that can assist in whichever way the organization requires. Make no mistake: this is not a glorified IT Security role, but a savvy and forward-looking information risk leader who can work at the level of the organization. Whether you require a hands-on leader to control IT, a strategic leader to position the organization for the long term, a tactical leader that can develop and implement complex risk management initiatives, or a combination of all three, the vCISO service is there to support the mission.

CLOUD COMPUTING RISK ASSESSMENT

Cloud computing has unique attributes that require a holistic approach to assessing risk to data as it moves through a cloud ecosystem. A move to the cloud is incomplete without the ability to provide assurance on data integrity, recovery, privacy, ediscovery and regulatory compliance. All areas of cloud security are assessed during this service, including privacy by design, shared security model analysis, operational security management, security controls implementation, cyber liability analysis, due diligence policies and procedures, and third party risk management process analysis.

CYBERSECURITY FRAMEWORK & REGULATORY ASSESSMENTS AND AUDITS

Due diligence audits are a fact of life for all organizations, as information assets are increasingly shared between partner, clients, and 3rd party information processors. TruSec can assist with the veritable alphabet soup of cybersecurity and regulatory framework audits and assessments that modern organizations are measured against, including: ISO2700x, COBIT 5, NIST, OCTAVE, OWASP, SOX, GLBA, HIPAA, CSA2K15, FFIEC/OCC/OTS-related audits, PCI-DSS, SANS, AICPA SOC2, DFARS, and many other industryand location-specific security and privacy frameworks and regulations.

STRATEGIC INFORMATION RISK ASSESSMENT

The only way to effectively control IT Security spend is to ensure that controls are being prioritized and deployed to protect organizational assets by value. This means that leaders should approach information risk management according to the operational, tactical, and strategic value an asset provides the organization (or would not provide, if it became unavailable). By utilizing and focusing on asset value as an organizational risk prioritization metric, a strategic assessment of the overall information risk management program can be measured for alignment and used to evaluate the efficacy of the ongoing risk management effort.