NEWBRIDGE
CYBER & RISK, LLC

Stephen E. Lipka, Ph.D., CRISC, CISSP

Consulting CISO – Building Effective Information Security Programs

EXECUTIVE SUMMARY

With over 15 years of information security experience and decades of IT leadership and consulting experience, Dr. Stephen Lipka has a track record of creating and rebuilding information security and risk management programs appropriate for each unique client, considering each unique client's business strategy, culture, information assets and risks, security posture, and compliance requirements. Keeping in mind that security must not be an obstruction to business operations, he works to deliver risk reduction, security, and compliance results beneficial to company profitability, operating capability, and shareholder value.

KEY ACCOMPLISHMENTS & CURRENT ACTIVITY – INFORMATION SECURITY

AS CONSULTING CISO

- As virtual CISO for cloud-first clinical stage bio-tech, launch and guide information security program aligned with NIST Cyber Security Framework (CSF) and CIS Critical Security Controls (CSC), focusing on protection of intellectual property and continuity of operations; established governance program, lightweight risk management, access management, vulnerability management, patch management, incident detection with Managed Detection & Response (MDR) and Endpoint Detection & Response (EDR), user security and phishing training, and lightweight governance, risk, and compliance (GRC) system; motivated use of next-gen firewalls, transition to zero-trust network.
- As virtual CISO for private equity firm with fragmented security activities, develop coherent security program focused on meeting SEC requirements with intent on transitioning to permanent CISO; established security governance integrated with executive risk committee; guided IT to more focused and mature information security program with full rewrite of policies and standards, replacement of MDR and anti-malware services, development and ongoing operation of third party risk management program, security awareness and phishing training, and compliance management with lightweight GRC; as consultant to permanent CISO, continue above work and lead response to mock SEC IT audit.
- As virtual CISO, lead program of assessing private equity firm's portfolio companies, guiding them to security practices more resistant to ransomware, breach, and business email compromise; outcome was reduced risk of degrading portfolio companies' value to the firm.
- As virtual CISO for major affordable real estate management firm with no security program, guide buildout of security program designed to reducing risks to personally identifiable information of tenants; established enterprise risk management body, established risk management program, motivated hiring of new security director, guided new policies and practices; continuing with creation and development of incident response program, selection of outside counsel and forensic firms, and mentoring heads of IT and security on strategy, program direction, and executive communications.
- Conduct security assessments of early clinical bio-tech and young marine robotics firm, based in CIS Critical Security Controls (CSC) to guide them to more mature security programs with an eye towards future regulatory compliance.

NEWBRIDGE CYBER & RISK. LLC
HOLLISTON, MA 01746

slipka@nbcyber.com
(857) 998-0300

NEWBRIDGE
CYBER & RISK, LLC

AS CHIEF INFORMATION SECURITY OFFICER

Create, build, and direct global enterprise-wide greenfield security function for $5Bn commercial real estate services firm that operates in 60 countries, focusing on protecting company's revenue, brand image, and client relationships.

- Aligned security program with company business objectives by establishing governance structure that incorporated Service Lines, Legal, Finance, HR, Corporate Communications, and IT.
- Created policies and standards to recognize current threat environment and align with relevant privacy and security standards (ISO 27001, SOC 2, SOX, Safe Harbor/GDPR); deployed SaaS governance, risk, and compliance (GRC) system.
- Established information risk management program, including vendor information risk.
- Established vulnerability management program. Drove IT's patch management and, in conjunction with IT's consolidation program, reduced vulnerabilities by 56%.
- To reduce cost while improving capability, collaborated with CTO to simplify IT architecture and strengthen and harmonize security architecture.
- Standardized firewalls, web filtering, anti-malware, and data loss prevention
- Established global security incident response process integrating Managed Security Services Provider.
- Established application security testing (a cloud service) for cloud and internal web applications.
- Established security policy and internet threat/social engineering awareness program for employees.
- Achieved first IT SOX compliance and first EU privacy compliance (Safe Harbor)

PRIOR EMPLOYMENT

- IT leadership, individual contributor, and consulting roles in defense and commercial industries
- Product development management – DBMS and personal computer software products

PROFESSIONAL ACTIVITIES & EDUCATION

- CISSP, Certified Information Systems Security Professional
- CRISC, Certified in Risk and Information Systems Control
- Professional Society Memberships: ISC^2, ISACA
- Professional Organizations: CISO Executive Network, InfraGuard
- FAIR Analysis Fundamentals, and Advanced FAIR Analyst Training
- ITIL Foundation

EDUCATION

- PhD (Computer Science), State University of New York at Stony Brook
- MS (Electrical Engineering) and BS (Physics), Polytechnic Institute of New York (now NYU Tandon School of Engineering)

NEWBRIDGE CYBER & RISK. LLC
HOLLISTON, MA 01746

slipka@nbcyber.com
(857) 998-0300