



SECURITY CENTER OF EXCELLENCE

Hanover, Maryland, USA

Annapolis Junction, Maryland
USA

Macquarie Park, Sydney
Australia

Contacts:

Jennifer Schulze
jschulz2@csc.com

Phil Justice
pjustic2@csc.com

For more information on CSC's security solutions, visit www.csc.com/security

CSC's Centers of Excellence help clients explore state-of-the-art solutions with minimum up-front investment, leveraging CSC's top talent to maximize innovation and results. Each Center has a designated facility and staff who demonstrate and deliver solutions and evaluate products, methodologies and concepts.

The Security Center of Excellence (CoE) focuses on all dimensions of security as it relates to information technology. The Center helps clients ensure business continuity, achieve regulatory compliance and reduce liability to protect enterprise objectives and stakeholder value. CSC's strength is in knowing how to quantify the value of an enterprise for security purposes, determine the value at risk, and manage that risk. The Center represents all of CSC's security capabilities and is responsible for managing and future planning around the entire portfolio and delivery of security services to government and commercial clients as well as CSC itself.

CSC has a comprehensive portfolio of security solutions to protect an enterprise's critical assets and key processes against any credible internal or external threat, whether physical, cyber or personnel-oriented in nature. Key security practices include risk governance, risk management and security operations.

As one of the largest providers of IT services to commercial and government organizations, CSC delivers end-to-end security for facilities, information systems and people. The Center's security experts explore and apply leading edge technology and practices for evaluating security and privacy, to insure alignment and compliance to government and industry standards such as SOX, HIPAA, NIST800-53, FISMA, ISO 27000, and PCI DSS in facilities and laboratories located on four continents. Security solutions are delivered through both consulting and advisory services as well as in managed service contracts.

CAPABILITIES

CSC's Security CoE offers solutions including strategy, program planning, support and operations in a number of comprehensive practices:

- **Risk Governance:** most strategic element whereby we equip executives and policymakers with the data and support they need to integrate information risk data and insight into a unified enterprise risk strategy
- **Information Risk Management:** strategic consulting engagements that strengthen and inform executives' risk governance deliberations with vital information via three risk analyses and associated workshops. Thus facilitating risk policy decisions that commit resources commensurate with enterprise value-at-risk
- **Security Operations:** Intrusion prevention, firewalls, monitoring, vulnerability assessments and intelligence, incident response, business continuity
- **Identity and Access Management:** Strategy, planning, user provisioning, authentication, meta directories, access management, biometrics

The Center's growing offerings and recent advances include the expansion of managed security services to include audit log assurance, data loss prevention, managed vulnerability assessments, technology compliance and managed encryption. In addition, a suite of strategic information risk management consulting engagements and digital investigative services have been added to the portfolio. Beyond the traditional needs to protect enterprise assets and operations, the group has introduced Digital Trust, an innovative security strategy that creates new enterprise value with security technology and services while still tending to important information risks all throughout the modern digital enterprise.

UNIQUE QUALIFICATIONS

- Trusted advisor to executives, policy makers and security experts for industry and government; significant contributors to security policy and doctrine through the NSTAC, the NSIE and other global standards committees
- Highest ability to execute, from strategy and implementation to operations
- Proven experience delivering results to U.S. federal and international agencies and Global 2000 customers on five continents
- Advanced service model extensions that respond to the new reality of national health and security being intertwined with private sector critical infrastructures
- Certified Common Criteria (ISO 15408) testing worldwide; the only company with accredited labs on three different continents

RESOURCES

CSC's more than 1200 full-time security experts serve both commercial and government clients, many having worked in the field for decades designing, deploying and operating security solutions in various roles. The Security CoE's laboratories in Europe, Australia and the United States are virtually integrated around the world. The facilities of the Center have over 6,000 square feet of space dedicated to helping define, test and integrate security solutions for global clients. In addition, our identity management technology has been integrated into our Hanover, Maryland Innovation Center. This includes a robust suite of biometric technology demonstrating ID management and authentication using any combination of fingerprints, palm prints, iris scans and facial recognition.

Case Example: Risk Management for a Global Client. CSC's enterprise-wide approach to risk management helps protect a global client with major data centers in North America, Europe and the Far East. To evaluate its existing security program, the client turned to CSC security experts, who uncovered several risk-filled circumstances.

Each one indicated a condition that, left untended, was capable of jeopardizing the security and integrity of the entire processing and data infrastructure. These conditions included lack of a global security policy, an inconsistent infrastructure, and no security compliance standards or method for assessing compliance. Compounding this, the client operated without a uniform access control method for its global IT infrastructure. Combined, these factors rendered the enterprise vulnerable to major security breaches, forcing it to respond to one critical alert after another. CSC combined static and dynamic countermeasures, enabling the client to benefit from comprehensive security in a much shorter time frame than would have been possible via a stovepipe problem-by-problem approach. Putting in place a number of CSC experts and employing proven processes and proprietary vulnerability technology, the client achieved a 90 percent reduction in vulnerability ratios, a seven percent reduction in denial-of-service vulnerabilities, and a 530 percent increase in systems with no vulnerabilities, thereby improving security overall as well as efficiencies in operations.