Satori CONSULTING

CYBER SECURITY SERVICES

Effective information security requires organizations to quickly progress from basic controls that provide good security, to great security that understands expected behavior and thwarts potential attacks to digital assets. This level of security can only be sustained when the right culture is established.

A CULTURE OF SECURITY

Create a culture that builds security into all phases of IT planning and delivery

4 Effective governance is implemented and security is focused on protecting sensitive digital assets. Security is continually adjusted in response to changing threat environment.

3 Security controls are aligned with business risk tolerance. Continual monitoring is performed to detect and respond to security threats.

2 Minimum set of security controls implemented to meet compliance requirements. Delivery of effective security services is inconsistent.

1 The basic security controls in place to protect the environment. Monitoring and response processes are ad-hoc.

THREATS

Understanding the changing threat landscape and planning countermeasures

WHY SATORI?

- Seek to understand customers' business and desired outcomes
- Proven success transforming IT security
- Proven experience in compliance management
- Technology-agnostic partner

Satori CONSULTING

INFORMATION SECURITY FRAMEWORK

Satori's Information Security Framework identifies the security focus needed to effectively manage risk. A high level of maturity is needed in each discipline to build security into all solutions, understand threats and adjust security controls to protect digital business assets

GOVERNANCE

Provide the right guidance and oversight to ensure the right controls are in place to protect digital assets

FOCUS:

- Risk Management
- Regulatory and Industry Mandate Compliance Guidance
- Data Classification
- Employee Training and Awareness
- Security Policy Development
- Supplier Security Governance
- Security Architecture Development and Oversight
- Security Standards, Principles and Guidelines

INVENTORY & BASELINE

- Technology and Data Inventory
- Data Flow Definitions
- Solution Architecture
- Baseline of Behaviors

PROTECT/PREVENT

Implement processes and technologies to maintain the confidentiality, integrity and availabilty of data

FOCUS:

- Access Management
- Data Protection
- Network Access Control
- Application Protection Services
- End Point Protection Services
- Secure Messaging
- Patch Management
- Physical Security

MONITOR/DETECT

Monitor information systems to detect unauthorized activity or breach

FOCUS:

- Intrusion Detection Service (IDS)
- System Logging & Auditing
- Security Information & Event Management (SIEM)
- Threat Monitoring
- Vulnerability Monitoring & Management

RESPOND/RECOVER

Provide effective and efficient response to security incidents and mitigate risk

FOCUS:

- Security Investigations
- Security Incident Response
- Security Forensics
- Business Continuity
- Disaster Recovery