Global Information

○ Preempt Threats

○ Detect Vulnerabilities

○ Prevent Loss

○ Respond Effectively

Data Protection

Sensitive information must always be protected – whether it is being transmitted, stored, processed, or handled in any other way. Data Protection helps prevent data leakage by assessing, improving, and implementing security controls that protect sensitive information.

Global ID Administration

Staffs require different kinds of access to conduct day-to-day business. A Global Identification Administration program manages identification administration – including ID creation, modification, and deletion, as well as password resets – to help mitigate access management risks.

Privileged User Managed Access

A Privileged User Managed Access program implements controls around persistent and temporary privileged access to production environments of the systems, networks, and applications that allow employees to perform their jobs and provide your customers with service. A robust program also manages controls for sensitive data in non-production environments.

Security Incident Management

While protecting data is key to Information Security, knowing what to do in the event of an actual or potential compromise is also critical. Security Incident Management deals with a range of Information Security events, from malicious activities by external parties to internal incidents impacting critical information.

Information Security Risk Assessments and Issue Management

Determining and managing the risks associated with business practices and systems, as well as managing non-compliance issues as they are identified, is an important part of Information Security. An Information Security Risk Assessment program identifies Information Security risks associated with processes and systems, allowing the business to assess and react. An Issue Management program then helps businesses correct issues or accept the risk through an exception.

Vulnerability Assessment

Vulnerability Assessments are tests performed on a subset of applications and all infrastructure assets to proactively identify and remediate potential weaknesses. Vulnerability Assessments are critical for addressing weaknesses proactively.

Third Party Information Security Assessments

By working with supplier relationship managers and key Information Security staff, a Third Party Information Security Assessment program is able to help ensure third party vendors have the appropriate security controls in place when handling sensitive data.

Secure System Development Lifecycle

To reduce the number of vulnerabilities in multiple systems, a Secure System Development Lifecycle incorporates application testing earlier in software development in order to find vulnerabilities sooner and fix them earlier when it is less expensive to do so.

Cyber Intelligence Collection

The developing cyber-threat landscape poses incalculable risks to information, reputation and operations. Cyber Intelligence Collection proactively collects and analyzes intelligence to monitor and respond to these threats; ensuring security infrastructure provides end-to-end defenses.

Liaison Networks

Developing solid industry relationships, networks, and consortiums is critical for situational awareness and successful protection. Information sharing and proactive measures, along with enhanced responses to potential and real crises, are benefits of collaborating within your industry.