Information Governance & Cyber Security

Information security is often thought of as a computer technician or network administrator protecting computers with anti-virus software and some sort of network firewall. However, there is much more to information security than just the technical staff and software. New malicious code, worms, and distributed denial of services are taking place in cyber-space at an exponentially faster level than ever before.

Senior level executives are realizing there is more to information security than just a computer technician installing anti-virus software. Companies must deal with the internal threat, the disgruntled employee; they must address fundamental security policies, and have a disaster recovery plan in place to be prepared for the worst.

An Information Security Program

All information security programs start with the CIA triad. The CIA triad is referring to Confidentiality, Integrity and Availability of data. "Confidentiality" means the assets of a computing system are accessible only by authorized parties.

"Integrity" means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.

"Availability" means that assets are accessible to authorized parties. An authorized party should not be prevented from accessing objects to which he, she, or it has legitimate access need. For example, a security system could preserve perfect confidentiality by preventing everyone from reading a particular object. However, this system does not meet the requirement of availability for proper access.

Availability is known by its opposite, "denial of service". Along with the fundamental basis of the CIA triad, a security program must start with the proper policies and must gather input from all senior leadership within an organization.

Data Classification

	Category 1	Category 2	Category 3
Need for Confidentiality	High	Medium	Low
and/or			
Need for Integrity	High	Medium	Low
and/or			
Need for Availability	High	Medium	Low

Placement of the Information Security Officer

The mistake many organizations make is the placement of the Information Security Officer (ISO) under the Chief Information Technology Officer or Information Technology Director.

Due to the technical nature of ISO, many times security has already started within the Information Technology (IT) area/division and an impromptu ISO starts up within this area. The challenge then starts when IT itself is investigated for risk, malicious intent, incident and/or any other ISO investigation.

Where should the ISO report any improper conduct by IT employees? What if the senior leadership in IT knew of a critical vulnerability in an IT system but did not share this with senior management due to risk of embarrassment or job security?

The placement of the organization's ISO under IT tends to limit the scope of the department unnecessarily and it often becomes difficult for the ISO to work effectively across the organization.

Placing the ISO under the internal audit division is also a mistake many organizations make. Internal Audit is supposed to determine compliance and the ISO is supposed to create policy and assurance; creating policy should not be in the same division with compliance.

Thus, the Information Security Officer is best positioned directly under the President/CEO. The second most ideal position would be directly under General Counsel/Legal Affairs.

Y&L Consulting

Corporate HQ
7550 IH 10 West
Suite 940
San Antonio, TX 78229
(210) 340-0098
www.ylconsulting.com

Components of an IT Data Risk Assessment/Audit

There are four overarching components to performing a successful IT Data Risk Assessment/Audit. The first is data classification. The second is management controls, concentrating on controls that management is directly responsible for. The third is operational controls, which are the day-to-day operations of systems and those that a human is most likely to do or act on. The fourth is technical controls, which are usually automated computers applying the controls.

1. Data Classification

- CIA Triad: Confidentiality, Integrity, Availability

2. Management Controls

- Risk Management
- Review of Security Controls
- Life Cycle Enforcement
- Disaster Recovery/Business Continuity Planning

3. Operational Controls

- Personnel Security
- Physical Security
- Documentation
- Security Awareness/Training
- Incident Management

4. Technical Controls

- Identification and Authentication
- Logical Access Control
- Audit Trails, Monitoring and Logging

Each of the subsets beneath the four overarching components above can be further extrapolated in terms of what a Y&L Cyber Security Analyst will be auditing. For example, here are the different elements that would be reviewed under "Operational Controls":

Operational Controls

Sub-components	Elements to Audit
Personnel Security	Training & Awareness
	"Need to Know"/least privilege
	Review of Logs
	Policy & Procedures
	Background Checks Performed
Physical Security	Layered Access/Physical Protection
	Keypads/Badge Access/Other
	Access Control Log/ Log Audits
	Training/Awareness
	Video Surveillance
Documentation	Complete/Thorough
	Living Document/Updated
	Easily Available
	Understandable
	Training
Security Awareness	Mandatory & Enforceable
	Reoccurring/Current
	Creative (multimedia)
	Information Access
	Policy Driven
Incident Management	Documented Policy & Procedures
	Incident Team in Place
	Identification of Incident Process
	Incident Documentation
	Incident Team has Authority to Respond

Y&L Cyber Security Certifications

Members of the Y&L Cyber Security practice and our Chief Security Officer (CSO) hold certificates in the following and have experience managing cyber security initiatives for a variety of Texas State Government Agencies:

- Certified Information System Security Professional (CISSP)
- GIAC Security Leadership (GSLC)
- GIAC Security Essentials (GSEC)

About Y&L

Y&L Consulting, Inc. is a global provider of IT enterprise solutions and professional services. Headquartered in San Antonio, Texas, Y&L has assisted many of the region's largest companies with their IT architecture, programming, integration, business intelligence, cyber security and help desk needs. Since Y&L's inception, our goal has been to enhance both the processes and profitability of our clients. We understand that our success depends on their success.

Y&L Consulting

Corporate HQ
7550 IH 10 West
Suite 940
San Antonio, TX 78229
(210) 340-0098
www.ylconsulting.com