

An aerial night view of a city skyline, likely New York City, showing numerous skyscrapers and buildings illuminated with lights. The perspective is from a high angle, looking down on the city. The lights from the buildings and streets create a dense pattern of yellow and white against the dark night sky.

Cybersecurity

A Compliance Professional's Perspective

Cybersecurity?

- Body of technologies, processes, and practices
- Designed to protect networks, devices, programs and data
- Attack, damage, or unauthorized access
- Corresponds to but is also distinct from information security.
- Costs¹:
 - Average annualized cost of cyber crime - \$ 11.7 Million
 - Average cost of a malware attack - \$ 2.4 Million
 - Increase in cybersecurity costs (2017 Vs 2016) – 23%

Cybercrime Landscape



Target	Asset	Actor	Motivation
Individual	Information	Organized Crime	Money
		Script Kiddies	Recognition
Organization	Application	Insider	Revenge
		Hacktivists	Morality
			Competition
State	Network	Nation State	Nationalism

Insiders – An Ominous Threat

90%

Organizations which feel vulnerable to insider attacks

53%

Confirmed insider attacks reported by organizations

64%

Organizations shifting focus to insider threats

86%

Organizations which have or are building an insider threat program

Source : Insider Threat 2018 Report by CA Technologies

Cybersecurity Landscape

Network

Database
and
Infrastructure

Disaster
recovery /
Business
continuity
planning

Data
security

Identity
managemen
t

Cloud
security

Mobile
security

Endpoint
security

End-user
education

Frameworks

Standards to develop Infrastructure Security Management Systems (ISMS). ISMS consists of:

- Roles and Responsibilities
- Policies/Standards/Procedures/Guidelines
- SLA's Service Level Agreements/Outsourcing
- Data Classification/Security
- Auditing

BS7799 / ISO 27002

*Code for ISMS
Guideline to implement ISO
27001*

NIST SP-800-30

*Risk Management guide for
Technology Systems*

OCTAVE

- 3 Step Risk Assessment*
1. ID Staff knowledge, assets & threats
 2. ID vulnerabilities and evaluate safeguards
 3. Conduct risk analysis, develop risk mitigation strategy

CoBIT

- IT Management Controls*
1. Plan and Organize
 2. Acquire & Implement
 3. Deliver & Support
 4. Monitor & Evaluate

COSO

- Fraudulent Financial
Activities and Reporting.*
1. Control environment
 2. Risk Assessment
 3. Control activities
 4. Information
 5. Communication
 6. Monitoring

ITIL

*IT Services Management
Framework.*

CMMI

*Software Development
Framework*

Illustrative Org Structure

Protect

Application Security
Access Control

Detect

Vulnerability Testing
Monitoring Logs

Recover

Disaster Recovery
Investigations

Govern

Policies
Training



Legal Remedies - India

- Information Technology Act, 2000 – Primary Act.
- Covers offenses where a computer resource:
 - Is the target of an offense (Hacking)
 - Is used for committing an offense (Cheating, IP Theft)
- Operational Issues:
 - Relevance and admissibility of evidence
 - Gathering evidence – Internal & External
 - Jurisdiction
 - Expertise of investigating officers

Role of Compliance Professionals

Investigations

- Awareness & knowledge of fundamentals
- Act as an interpreter
- Evidentiary rules
- Legal Expertise
- Red Flags

Awareness

- Embed in training & awareness programs
- Reinforcement
- Consistent messaging
- Discipline bad behavior

Collaborate

- Evangelize
- Awareness of risks
- Pitch in with your skills & competencies
- Assess and drive tone & culture

