CultureLink

Overview - Cybersecurity
CSX Fundamentals Program

Welcome

Thank you…

Our goal is to assist you on your journey…

Program

- Cybersecurity Nexus (CSX) - ISACA

CSX CERTIFICATIONS

CSX training and certifications offered for skill levels and specialties throughout a professional's career.

Specialization Level…

Specialization Level…

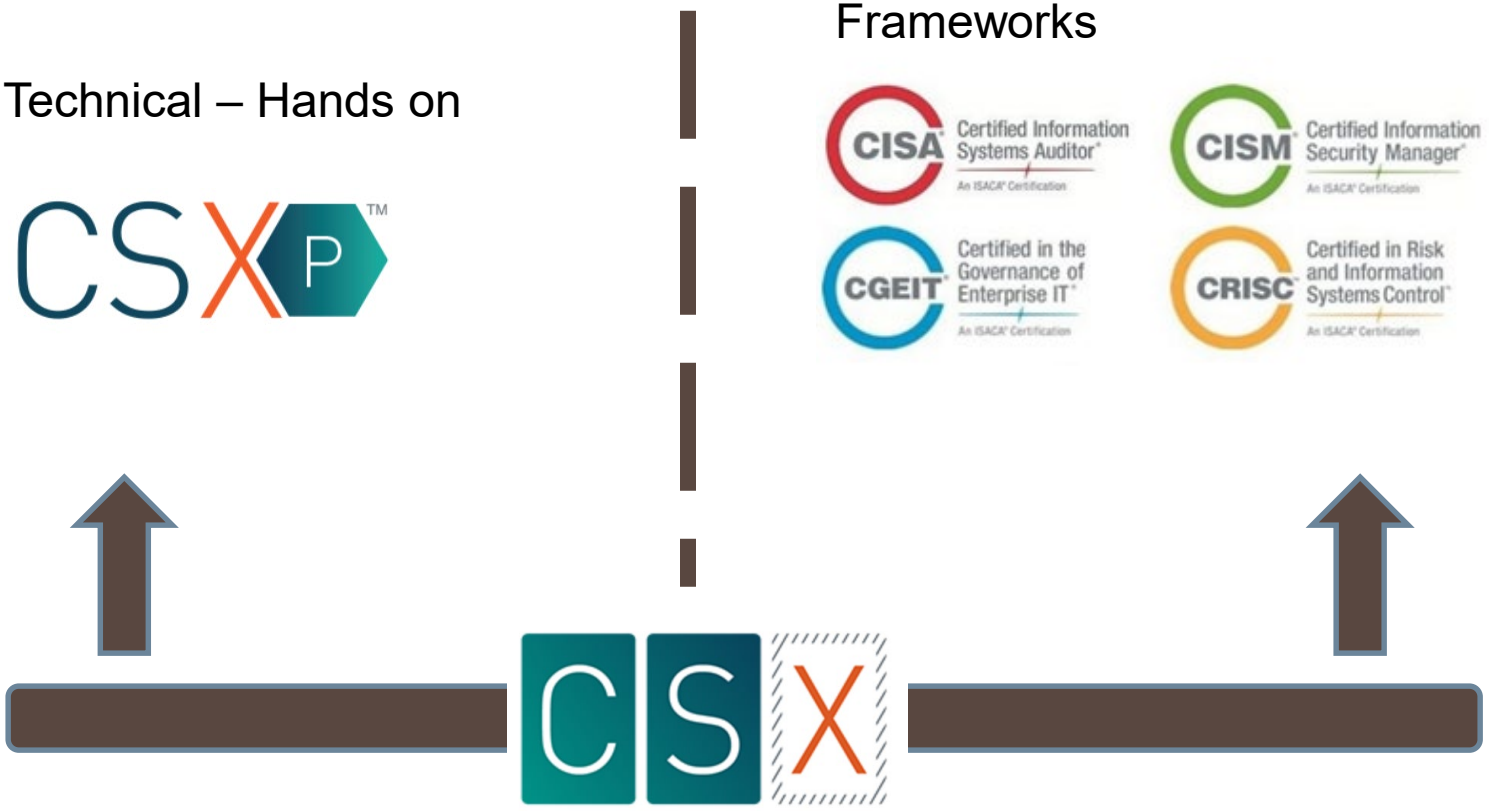
CSX ISACA Program

- Established 1969
- Authority in the security industry
- ISACA has a presence in more than **180 countries**, including more than **217 chapters** and offices in both the United States and China
- ISACA offers the **Cybersecurity Nexus™**, a comprehensive set of resources for cybersecurity professionals
- **COBIT 2019** – Business Framework that helps with Governance
- CEGIT, CISM, CISA, CRISC (Governance, Security, Audit, Risk)

The Journey

Management side – less technical
Business Models, Processes, Frameworks

Technical – Hands on



CSX EXAM

- The Cybersecurity Fundamentals Certificate **exam is an online**
- Closed-book, **remotely proctored** exam.
- Covers five domains and includes a total of **75 questions**
- Each **multiple-choice question** has four options with only one correct answer. You will be given **2 hours (120 minutes) to complete** the exam. The **passing score is 65%**
- No work pre-requisite experience*

CSX Domains

The **Cybersecurity Fundamentals exam** tests for foundational knowledge **across five key areas** of cybersecurity:

- Cybersecurity concepts
- Cybersecurity architecture principles
- Cybersecurity of networks, systems, applications and data
- The security implications of the adoption of emerging technologies
- Incident response

CultureLink

Meet your Tutors:

Tutor Introduction

CultureLink

Administration Logistics

Administration & Logistics

Class Format

- Weekly sessions

Workload

- 2-3 hours – read assigned readings as shown in course outline

Resources / Tools

- Internet search, framework manuals, videos

Text / Readings

- Handouts, links

Course Material

- CSX Study Guide

Grading and Evaluation

- No official grading
- Quizzes in each section
- Final practice exam

- Encourage all students to have active participation & contribute to class discussion

Student Responsibilities

- Review all material for classes
- Prepare for quizzes
- Self-study, research topic
- Participate in the discussion
- Relate personal experiences
- Ask questions

Current Event Guidelines

- **Objective:** to share recent updates in the field of Cyber Security, Privacy, IT Risk Management, IT Governance and closely related topics.
- **Opportunity:** to further develop communication skills when talking about these topics in real life
- Each person is expected to present on the dates assigned. The presentation length will be **5 minutes**
- **Format:** casual but being aware of your professional audience, standing in front of the class, and making use of material.
- If you are using Power Point slides then send them to tutors via eMail
- Presentations are expected to deliver a good understanding of the article(s) and/or news: why they were chosen, their interesting facts/findings, main conclusions, and source for reference.

Group Discussion

- Work in pairs
- Introduce yourself to your partner:
  - Name
  - Work Experience, ambitions
  - IT experience or any tech experience

- Switch roles
- Introduce your partner to the class

CultureLink

Any questions?

CultureLink

CSX – Cybersecurity Fundamentals

Section 1 : Cybersecurity Introduction and Overview

Course Plan

Module Titles
Section 1 – Cybersecurity Introduction and Overview
Section 2 – Domain 1: Cybersecurity Concepts
Section 3 – Domain 2: Security Architecture Principles
Section 4 – Domain 3: Security of Networks, Systems, Applications and Data
Section 5 – Domain 4: Incident Response
Section 6 – Domain 5: Security Implications and Adoption of Evolving Technology
Section 7 – Course Review
Section 8 – Practice Exam

Learning Outcomes for this Module

- Understand the evolution of cybersecurity
- Understand the general landscape in the industry
- Understand cybersecurity principles (CIA)
- Understand the skill gap
- Understand the governance – roles and responsibilities with the business

Topics for this Module

- **1.1** Introduction to cybersecurity
- **1.2** Difference between information security and cybersecurity
- **1.3** Cybersecurity objectives
- **1.4** Cybersecurity governance
- **1.5** Cybersecurity domains

CultureLink

Section 1.1

Introduction to Cybersecurity

Question

What is cybersecurity?

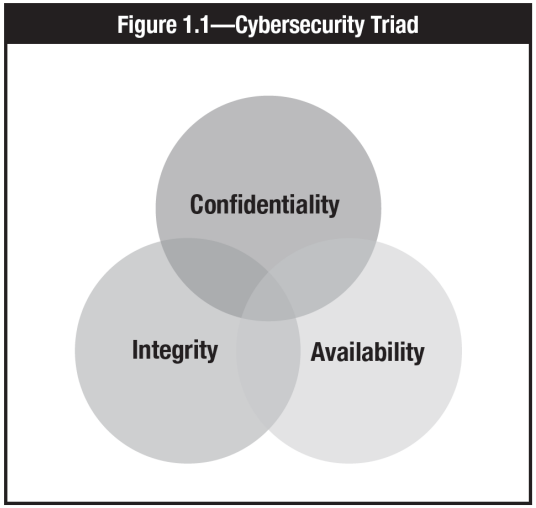
Cybersecurity Introduction

- Safeguarding information has been a priority
- Simple encryption techniques such as ciphers were created
- Today the objective is three fold cord

CIPHER ALPHABET

A	=	B	H	=	A	O	=	O	V	=	L
B	=	V	I	=	D	P	=	Y	W	=	P
C	=	G	J	=	Z	Q	=	F	X	=	U
D	=	Q	K	=	C	R	=	J	Y	=	I
E	=	K	L	=	W	S	=	X	Z	=	R
F	=	M	M	=	S	T	=	H			
G	=	N	N	=	E	U	=	T			

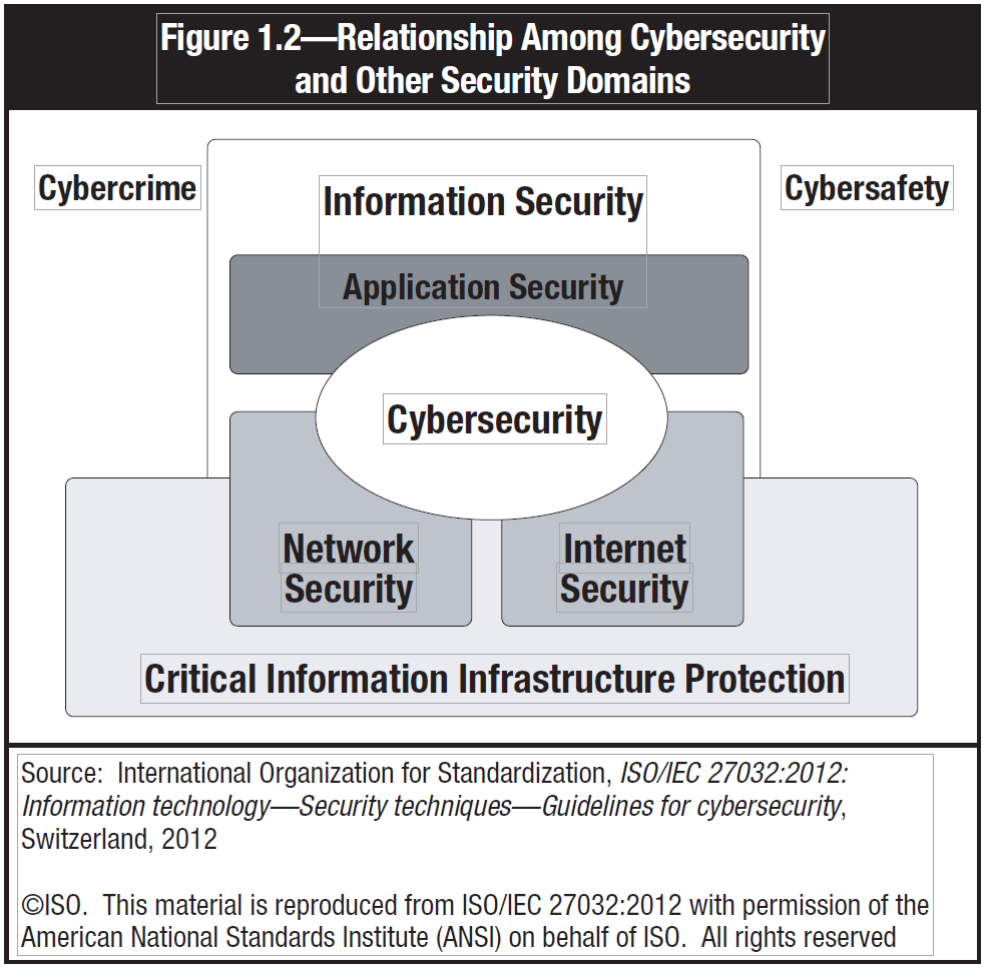
Figure 1



Source: CSX Fundamentals Guide - ISACA

Cybersecurity Introduction

- Cybersecurity is complex



Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

Cybersecurity and situational awareness

Many factors can impact security:

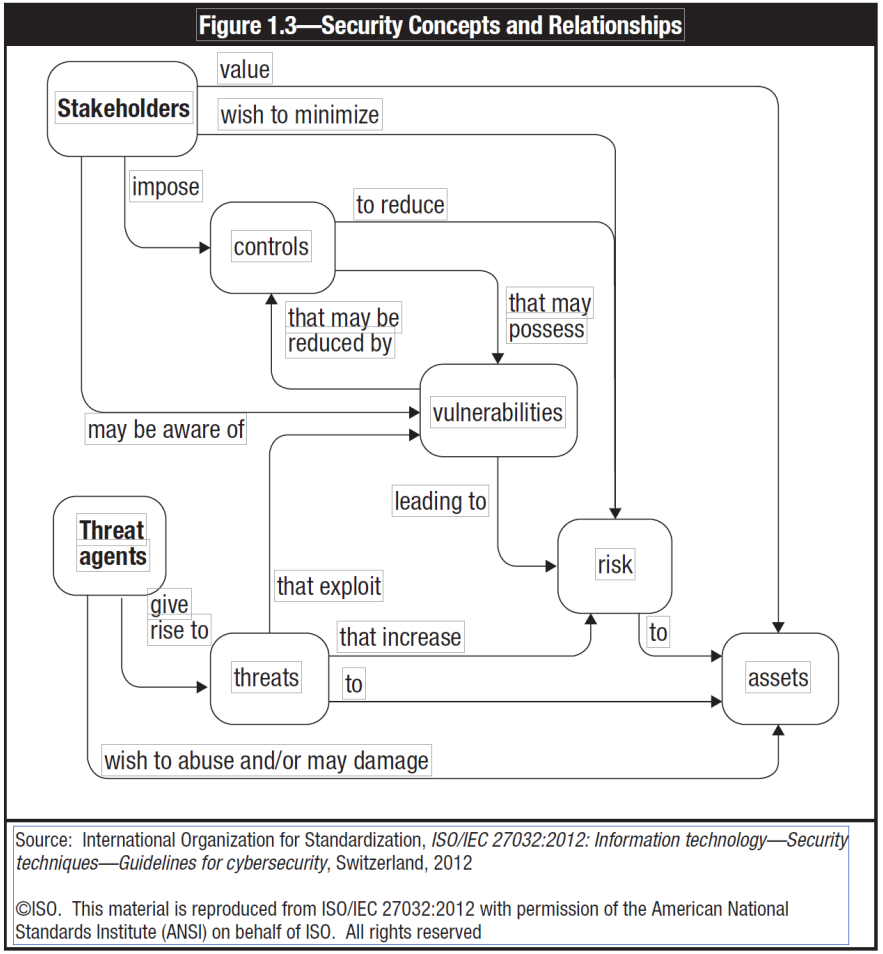
- Level of IT complexity
- Network connectivity (i.e. Internal, third party, public)
- On prem. vs Hybrid
- New tools, Platform applications and tools

When evaluating business plans and the general business environment:

- Risk Tolerance, Risk Appetite, Mergers & Acquisitions (M&A)
- Business vision
- Regional regulatory compliance

Cybersecurity and situational awareness

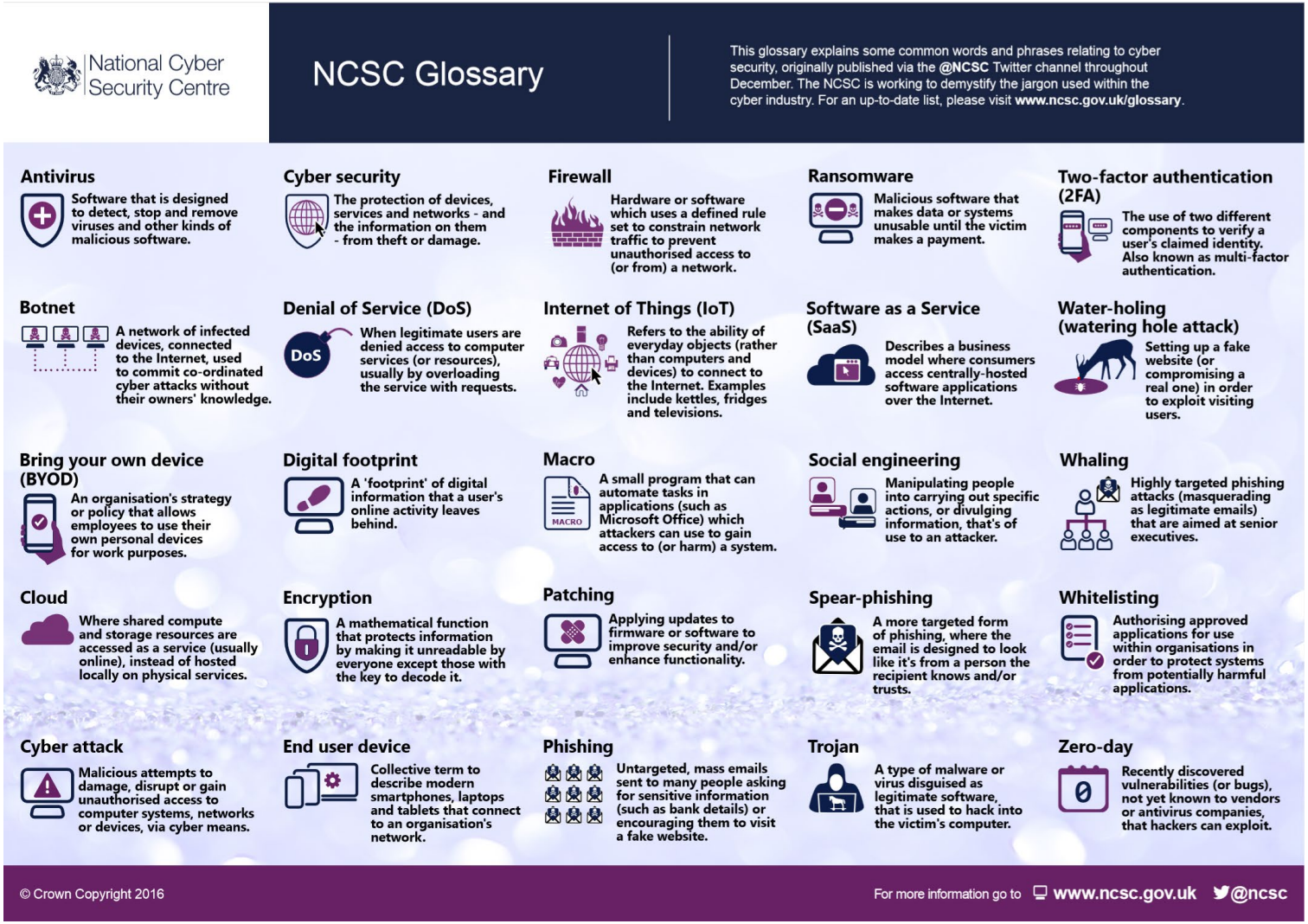
- Cybersecurity (CS) plays a significant role
- CS professionals must stay on top
- Deal with Advanced Persistent Threats (APT)



Source: CSX Fundamentals Guide - ISACA

Cybersecurity and situational awareness

LANDSCAPE



The Cybersecurity skills gap

The Cybersecurity Skills Gap from ISACA Podcast

https://itunes.apple.com/ca/podcast/isaca-podcast/id1209164381?mt=2&i=1000431166781

CultureLink

Any questions?

CultureLink

Section 1.2

Difference between information security and cybersecurity

Information Security vs. Cybersecurity

- **Information security** deals with **information,** regardless of its format—it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications.

- **Cybersecurity**, on the other hand, is concerned with **protecting digital asset**s—everything encompassed within network hardware, software and information that is processed, stored within isolated systems or transported by internetworked information environments.

- CSX refers cybersecurity as protection of information assets

Protecting Digital Assets

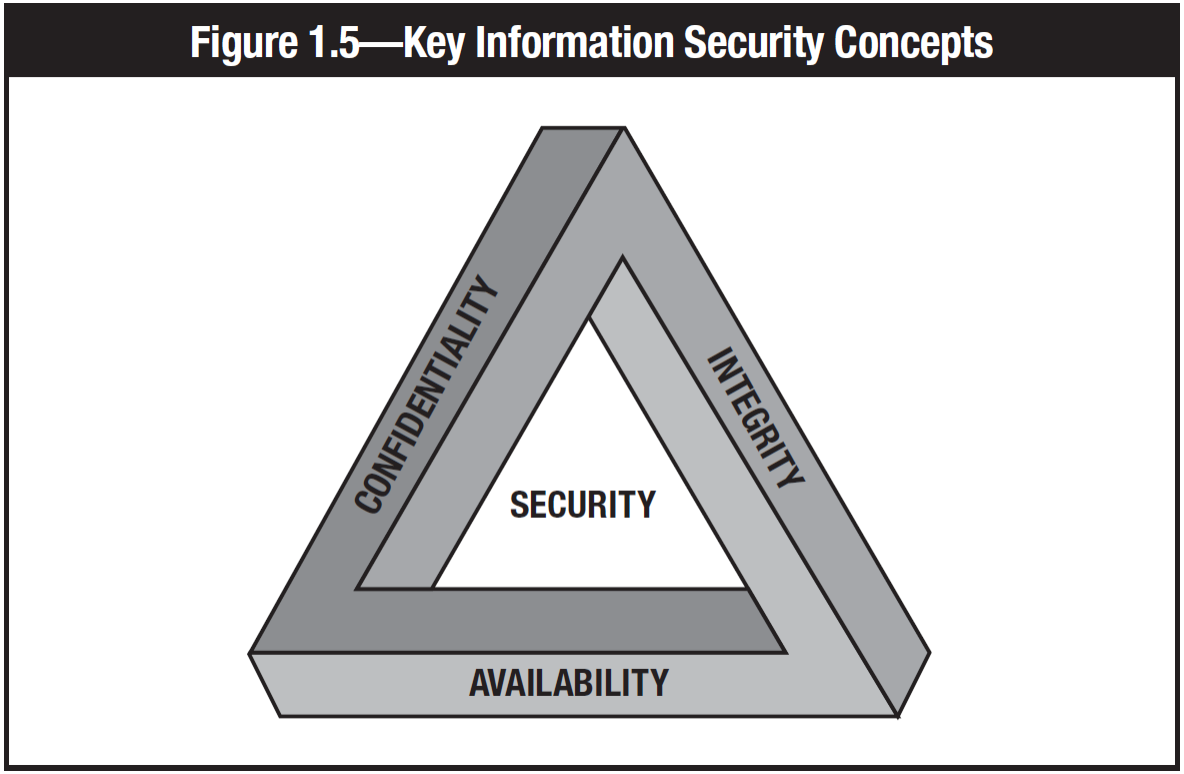
Source: National Institute of Standards and Technology (NIST)

CultureLink

Section 1.3

Cybersecurity Objectives

Confidentiality, Integrity and Availability



Also known as the "CIA Triad Triangle"

CIA Control

Figure 1.6—Confidentiality, Integrity and Availability Model and Related Impacts		
Requirement	**Impact and Potential Consequences**	**Methods of Control**
Confidentiality: The protection of information from unauthorized disclosure	Loss of confidentiality can result in the following consequences: • Disclosure of information protected by privacy laws • Loss of public confidence • Loss of competitive advantage • Legal action against the enterprise • Interference with national security • Loss of compliance	Confidentiality can be preserved using the following methods: • Access controls • File permissions • Encryption
Integrity: The accuracy and completeness of information in accordance with business values and expectations	Loss of integrity can result in the following consequences: • Inaccuracy • Erroneous decisions • Fraud • Failure of hardware • Loss of compliance	Integrity can be preserved using the following methods: • Access controls • Logging • Digital signatures • Hashes • Backups • Encryption
Availability: The ability to access information and resources required by the business process	Loss of availability can result in the following consequences: • Loss of functionality and operational effectiveness • Loss of productive time • Fines from regulators or a lawsuit • Interference with enterprise's objectives • Loss of compliance	Availability can be preserved using the following methods: • Redundancy of network, system, data • Highly available system architectures • Data replication • Backups • Access controls • A well-designed disaster recovery plan or business continuity plan

Examples

Can you think of challenging examples CIA faces?

- **Big data** poses extra challenges to the CIA paradigm because of the **sheer volume of information** that needs to be safeguarded, the **multiplicity of sources** it comes from and the variety of formats in which it exists. Duplicate data sets and disaster recovery plans can multiply the already high costs. Furthermore, because the main concern of big data is collecting and making some kind of useful interpretation of all this information, responsible data oversight is often lacking.

Examples

Other things come to mind of challenging examples CIA faces?

- Internet of Things privacy is the special considerations required to protect the information of individuals from exposure in the IoT environment, in which almost any physical or logical entity or object can be given a unique identifier and the ability to communicate autonomously over the Internet or a similar network. The data transmitted by a given endpoint might not cause any privacy issues on its own. However, ***when even fragmented data from multiple endpoints is gathered, collated and analyzed, it can yield sensitive information.***

Summary of Terms

- **Confidentiality** is the protection of information from unauthorized access or disclosure
- **Integrity** is the protection of information from unauthorized modification
- **Availability** ensures the timely and reliable access to and use of information and systems
- **Nonrepudiation** refers to the concept of ensuring that a message or other piece of information is genuine.

CultureLink

Section 1.4

Cybersecurity Governance

Governance Risk Management and Compliance

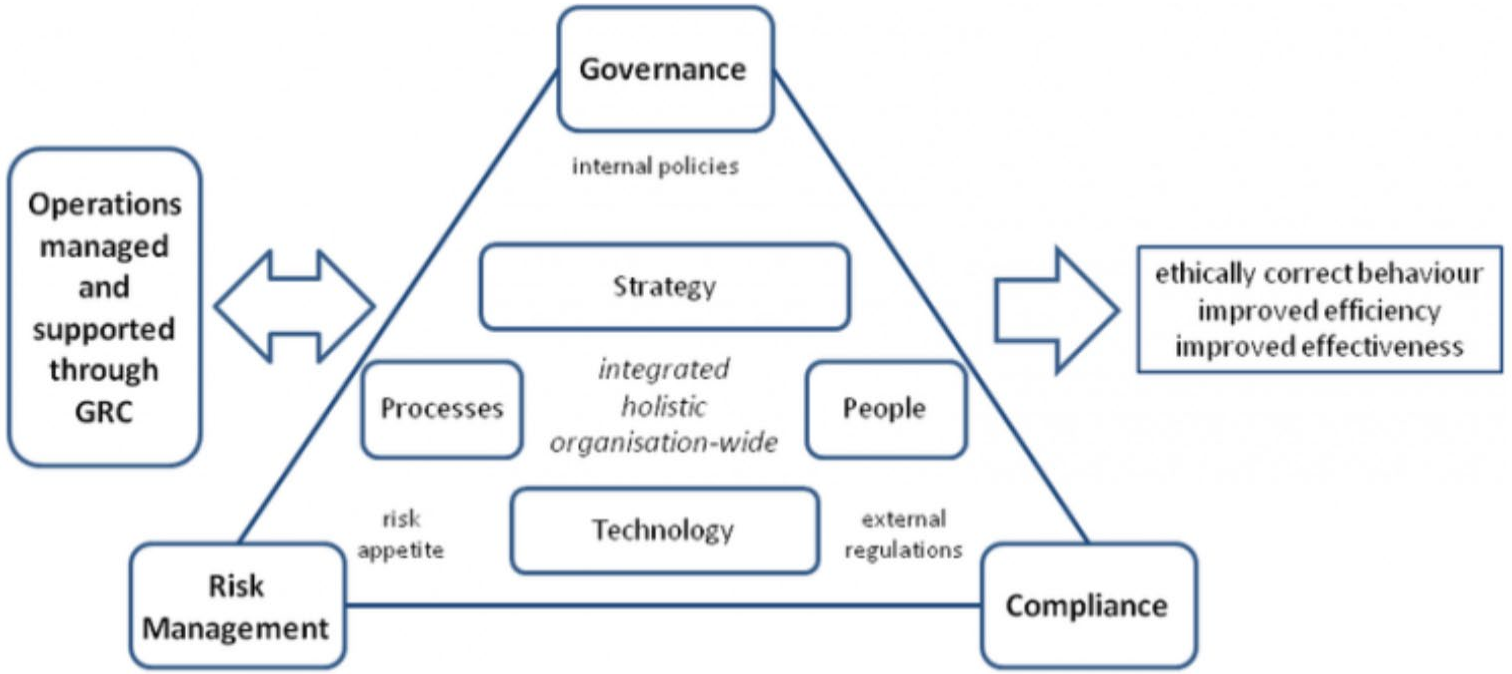
- **What is governance?**
  - *"the action or manner of governing"*

- Governance is the reasonability of the board of directors and senior management of the organization

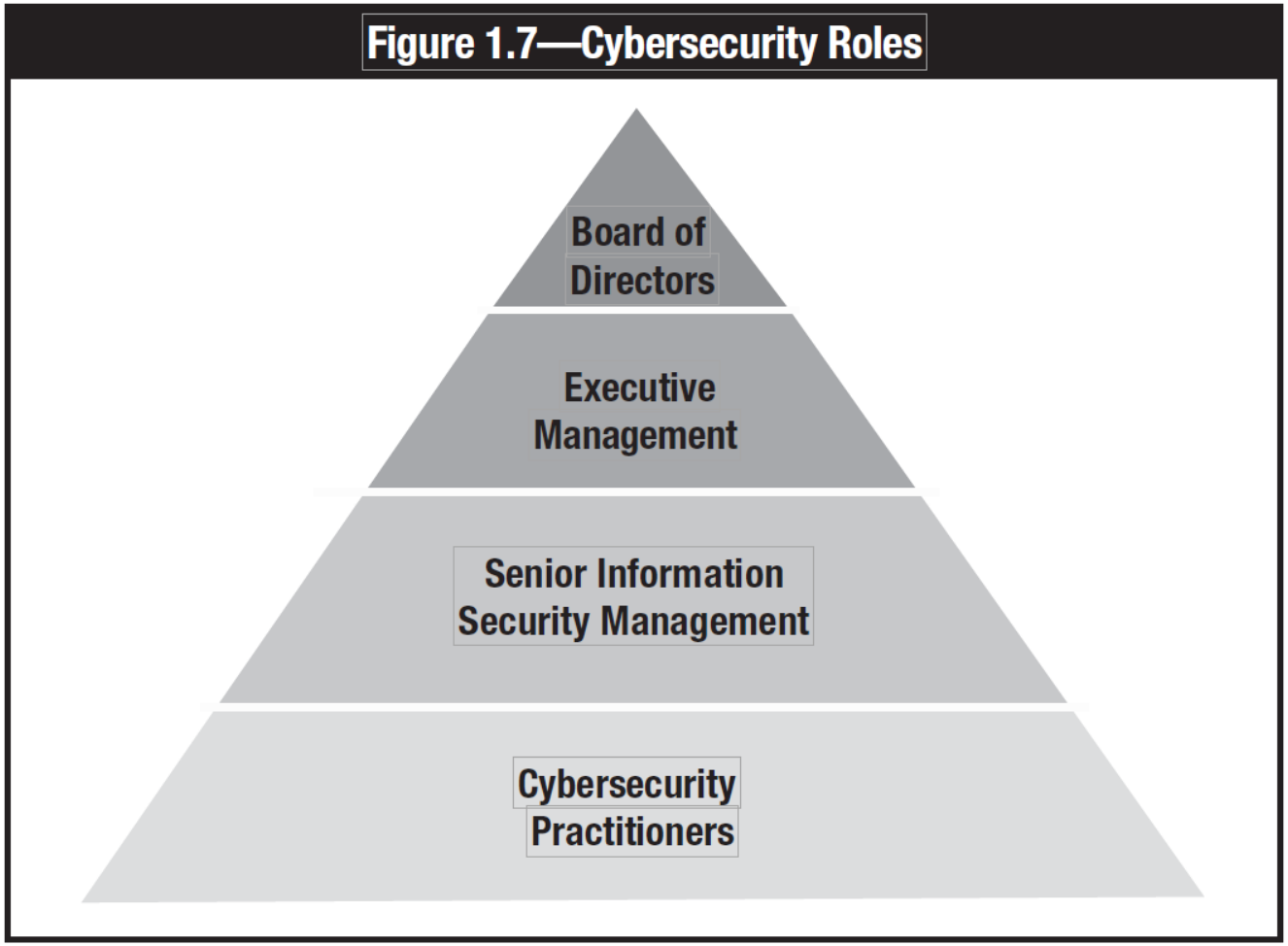
- Their duty to protect their assets and operations, including IT infrastructure and information

Governance Risk Management and Compliance

- At the highest level this is referred to GRC.



Information security roles



CultureLink

Any questions?

CultureLink

Thank You