PROACTIVELY MITIGATING THE CYBERSECURITY CHALLENGES IN A HYPERCONNECTED WORLD

ADEKUNLE K. OMIDIORA (MBCS, CITP)
CHIEF INFORMATION OFFICER (CIO)
HYGEIA NIGERIA LIMITED

PRESENTATION OUTLINE

- Introduction
- Collective Computing and Internet of Things (IoT)
- How Internet of Things (IoT) is changing Cybersecurity
- Major Cybersecurity breaches in 2016
- Systems Thinking approach to Cybersecurity Mitigation.
- The Cybersecurity Talent Gaps
- Cybersecurity skills in high demands in the Industry
- Conclusions
- Questions and Answers.

OUR CURRENT WORLD……

Global connectedness….

INTRODUCTION….

- Cybersecurity refers to the technologies and processes designed to protect Computers, Networks and data from unauthorized access, vulnerabilities and attacks.
- It covers the fundamental concept underlying the construction of secure systems, from the hardware to the software and to the human-computer interface.
- Mitigation, or the act of mitigating, is lessening the force or intensity of something unpleasant. The act of making a condition or consequence less severe.
- Proactivity, or the act of being proactive, is to prepare for, or control an expected occurrence, especially a negative or difficult one
- Hyperconnectedness is a term characterized by the widespread or habitual use of devices that have internet connectivity. Hyperconnectivity therefore is the increasing digital connection of people – and things, anytime and anywhere. (Term coined by Anabel Quan-Haase and Barry Wellman)
- 'CyberCrime 'refers to any crime involving the use of a computer connected to the Internet. The motives may be financial, political, anarchical or other, but the basic attack and intrusion techniques generally remain the same regardless of motive

Nigeria Cybersecurity Outlook 2016 - 2017…….

Year 2016 took the issues of cybersecurity to another dimension…..

1. Reports of cybersecurity being used to influence election outcome
2. In Nigeria, several organisations suffered cyberattacks, some had to pay ransom to get their data released.
3. The Federal Government of Nigeria estimated annual cost of cybercrime in Nigeria to be 0.08% of national GDP, representing about N127bn
4. Several financial institutions reported sophisticated phishing attacks
5. There were reports of "Cyber-harams"

What should we expect in 2017?

1. Rise and fall of Cyber Ponzi Schemes
2. Ransomware will continue to evolve
3. Regulatory interest in crypto-currencies
4. Increase in cloud base attacks
5. Rise in internet of things compromises

Generations of Interactive Computing Technologies……

- Mainframe Computing
- Personal Computing
- Ubiquitous Computing (… Mark Weiser)
- Collective Computing (Combined use of the cloud, the crowd and the shroud… Gregory Abowd)

FROM MAINFRAME TO COLLECTIVE COMPUTING……..

A framework for comparing Computing Generations

Generation	Time Frame	Human to Computer Ratio	Canonical Device	Application	
				Initial	Follow-on
1	Mid -1930s	Many - 1	Mainframe	Scientific Calculations	Data Processing
2	Late 1960s	1-1	PCs	Spreadsheet	Database Management, document Processing
3	Late 1980s	1- Many	Inch/foot/yard	Calendar and contact management, human to human communication	Location based services, social media, apps ecosystem, education
4	Mid - 2000s	Many - Many	Cloud/Crowd/Shroud	Personal navigation and entertainment	Heath advisors, educational assistants, supply chains logistics

The Rise of Internet of Things (IoT)

- IoT was first used in 1999 by British technology pioneer Kevin Ashton to describe a system in which objects in the physical world could be connected to the Internet by sensors
- The term Internet of Things (IoT) generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention
- IoT can be implemented in many different domains including transportation, agriculture, healthcare, energy production and distribution, and many other areas that require things to communicate over the Internet
- Over the next decade, IoE can help governments create value by saving money, improving effectiveness and productivity, generating new revenue and enhancing citizen benefits
- Data is ubiquitous and no longer a differentiator. IoT's ability to combine data with people, process, and things will provide competitive advantage for companies that harness its capabilities

The Internet of Things
a very short story

The Internet of Things is the network of physical devices, vehicles, buildings and so on embedded with electronics, software, sensors and network connectivity that enable these objects to collect and transmit data via the Internet.

In the year 2016, we had over **4.9 billion** connected things, so get ready, the Internet of Things is here to stay

ATMs were some of the **first** Internet of Things objects as far back as **1974**

The " Internet of Things " is a phrase that **87 %** of people haven't heard of

Back in **2008**, there were already more objects connected to the Internet than people

Companies like **Google** and **Samsung** are investing in home devices and having a connected kitchen could save the food and beverage industry as much as **15%** annually

The global wearable device market has grown **223% in 2015**

According to some estimates, the Internet of Things will add **USD 10-15 trillion** to global GDP in the next **20 years**

By 2020, 250 K vehicles will be connected to the Internet

Google's self-driving cars average about **10000 autonomous miles** per week

How Internet of Things is changing Cybersecurity

- Expansion of the scope of responsibility into new platforms, services and directions
- IoT systems are highly heterogeneous with respect to communication medium and protocols, platforms, and devices.
- IoT devices do not have well defined perimeters, are highly dynamic and continuously changing because of mobility
- IoT systems may also include "objects" not designed to be connected to the Internet.
- The Open Web Application Security Project (OWASP) Internet of Things (IoT) project has identified most common IoT vulnerabilities including:

OWASP Internet of Things Vulnerabilities Listing	
• Insufficient authentication or authorization	• Insecure cloud interface
• Insecure network services	• Insecure mobile interface
• Lack of transport encryption	• Insufficient security configuration
• Insecure software or firmware	• Poor physical security
• Insecure Web interface	• Privacy concerns

Some of the major cybersecurity Incidents in 2016

- **Dyn DDoS attack:** In October, cybercriminals launched major DDoS attacks, disrupting a host of websites, including the likes of Twitter, Netflix, PayPal, Pinterest and the PlayStation Network, amongst many others. (October, 2016)
- **Tesco Bank accounts compromise:** Customers lose real money (November, 2016)
- **DDoS against automating systems in Finland:** Cybercriminals in Finland were able to halt the heating system in two buildings in the city of Lappeenranta (classical threat to IoT device,)
- **US Department of Justice:** The attackers released data on 10,000 Department of Homeland Security employees in one day, and then released data on 20,000 FBI employees next day (February, 2016)
- **AdultFriendFinder.com:** Approximately 412 million users had personal information stolen and published in criminal marketplaces on the dark web. (November, 2016)
- **LinkedIn, Tumblr and Myspace:** More than half a billion passwords were posted in June by a hacker named 'Peace'
- **DDoS attack on Brian Krebs website :** A near successful attack in September, 2016
- **Yahoo suffers from massive data breach #1:** 500 million customer data stolen in September 2016
- **Yahoo suffers from massive data breach #2:** December 14th and 15th 2016, 1 billion customer accounts compromised
- **Attack on Philippine election voters database :** Philippine Commission on Elections (COMELEC) database involving approx. 55 million voters details were released

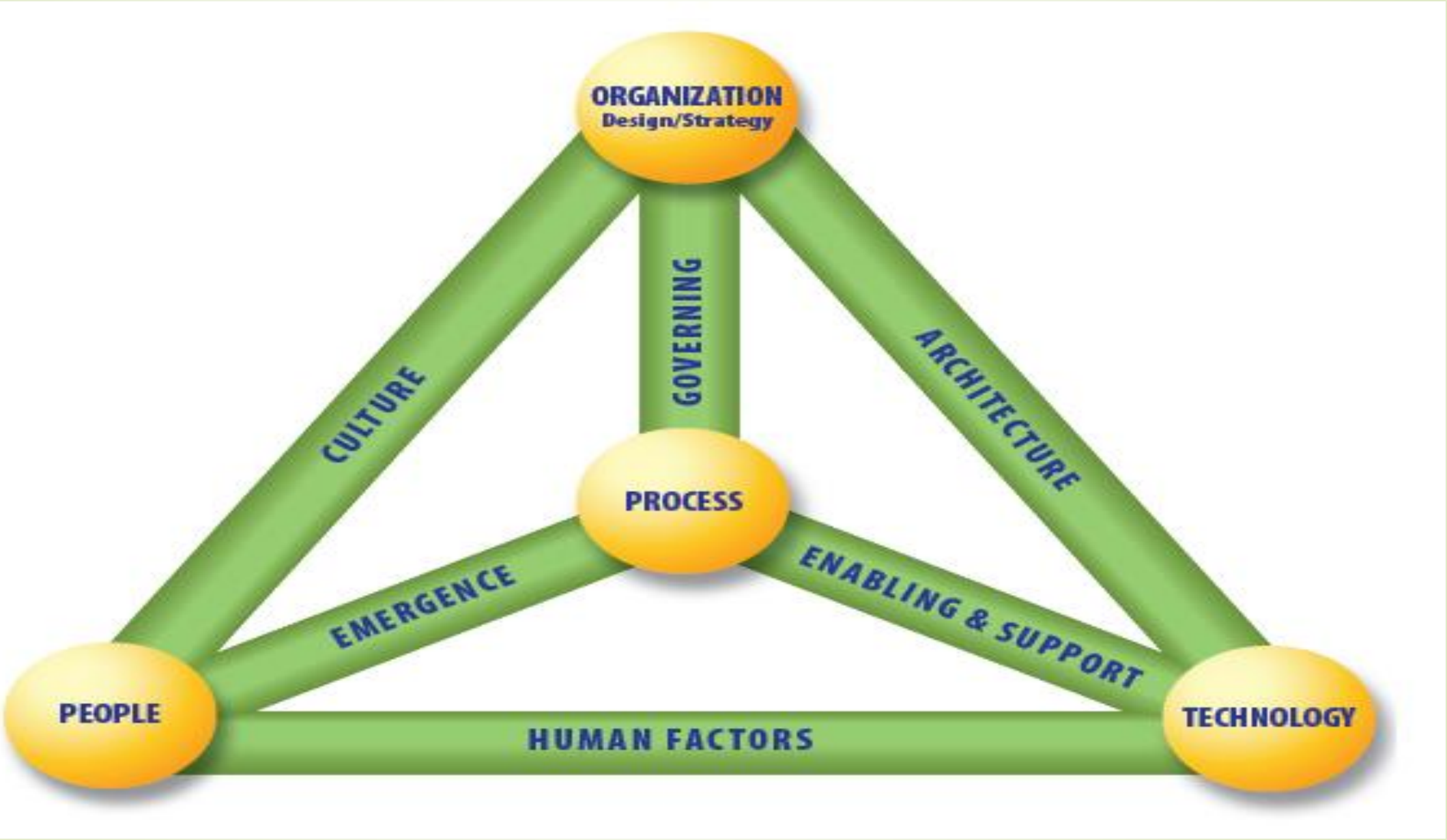
Readiness Assessment for Cybersecurity Incidents

If you know your enemies and you know yourself, you will not be imperil in a hundred battles; if you do not know your enemies but you do know yourself, you will win one and lose one; if you do not know your enemies nor yourself; you will be imperiled in every single battle….Sun Tzu

Systems Thinking approach to Cybersecurity Mitigation…..

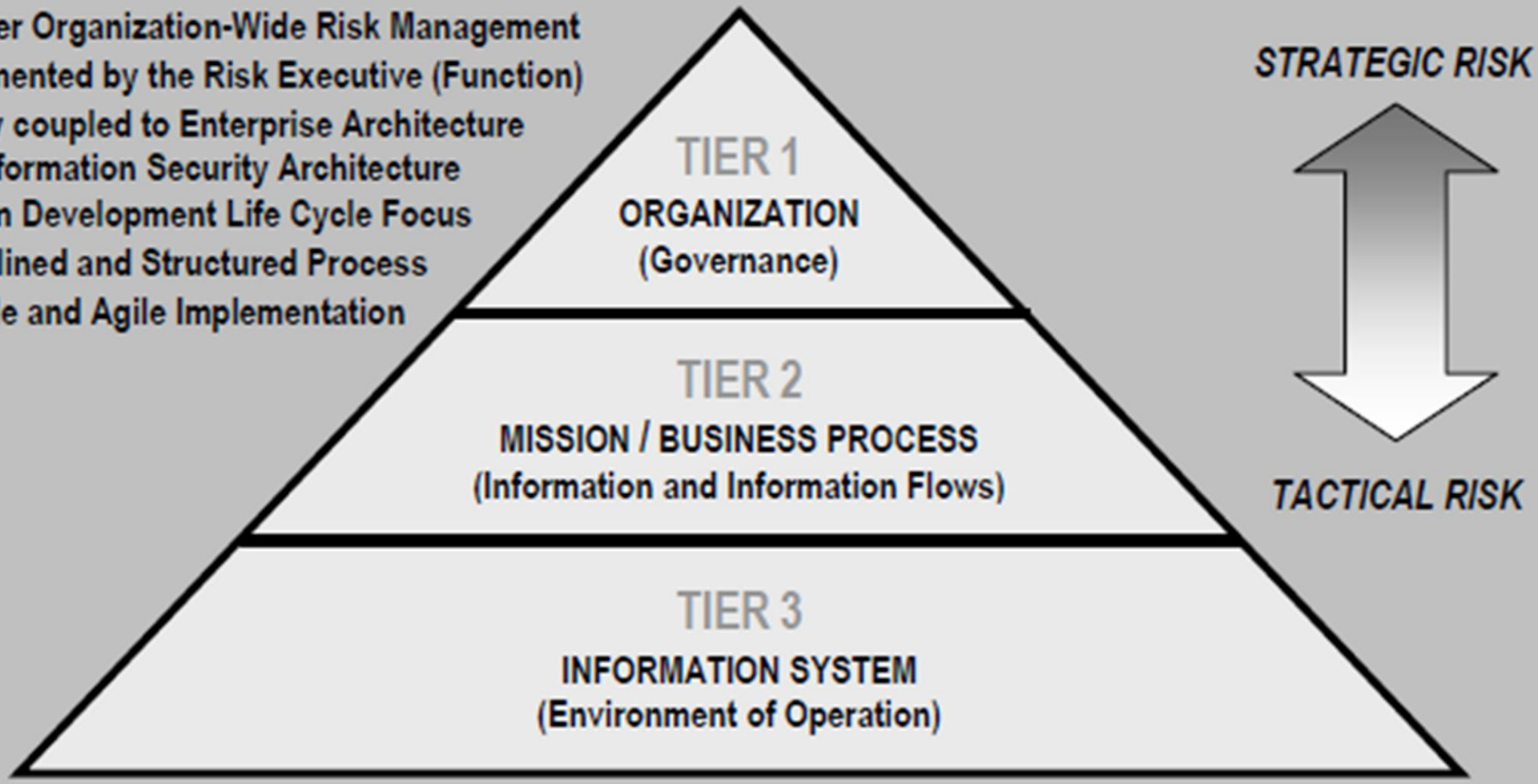
- Systems thinking refers to the examination of how systems interact, how complex systems work and why "the whole is more than the sum of its parts."
- Studying the behaviours and results of the interactions of the various units of a system assist one to better understand the entire system and the way itfunctions.
- Systems thinking is about wholeness. Looking at information security in pieces (people, process, technology) has not proven to be an effective method to manage a security program
- Utilizing a systems thinking approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors.

The structure of the System Thinking Model……



Integrated Organization-Wide Risk Management

- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation



Security Risks Assessment

Cybersecurity risks usually occur through 3 key means:

- Vulnerabilities: Design flaws in hardware, software or connectivity; reliance on unreliable or unsecured vendors
- Human error and human frailty : Hectic workplace, complex systems, serious temptations to breach privacy
- Compliance failure: Improperly secured devices or data can lead to non-compliance, followed by fines or sanctions

Asset Identification and Prioritization

- IT Networks and Infrastructure
  - Servers, routers, switches etc.
  - Databases
- Applications
  - Customer facing applications e.g websites
  - Internal Applications for processing sensitive information
- Data
  - Company trade secret
  - Financial data
  - Personally Identifiable Information
  - Protected Health Information

Threat Determination

- Malware (Ransomware, Botnets and other rogue software)
- Phishing
- DoS/DDoS
- Cyber-epsionages: Spoofing, man in the middle
- Lost and/stolen assets
- Unpatched or outdated software
- Malicious codes
- Removable media etc
- Other organised Crimes – Ping of death etc
- Privilege Account Management
- Spamming, Malvertising

Vulnerability Assessment

- Penetration Test
- Perimeter Network and Firewall review – Port Scanning etc
- Active Directory Assessment
- Web Application Assessment
- Database Audits
- Review of Policies and Procures

Conduct Impact Analysis and determine Risk Level….

- High : Exploitation of the vulnerability
  - (1) may result in the highly costly loss of major tangible assets or resources;
  - (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or
  - (3) may result in human death or serious injury.
- Medium : Exploitation of the vulnerability
  - (1) may result in the costly loss of tangible assets or resources;
  - (2) may violate, harm or impeded an organization's mission, reputation, or interest; or
  - (3) may result in human injury.
- Low : Exploitation of the vulnerability
  - (1) may result in the loss of some tangible assets or resources;
  - (2) may noticeably affect an organization's mission, reputation, or interest.

Adopt and Implement Cybersecurity Framework

- NIST Cybersecurity Framework v 1.1 (Jan 10, 2017)
- The Framework Core consists of five concurrent and continuous Functions

IDENTIFY

- Asset Management : The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
- Business Environment : The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Governance The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- Risk Assessment The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy : The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

PROTECT

- Access Control : Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Awareness and Training : The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures : Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance : Maintenance and repairs of information system components is performed consistent with policies and procedures
- Protective Technology : Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

DETECT

- Anomalies and Events : Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- Security Continuous Monitoring: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes : Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events

RESPOND

- Response Planning : Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events
- Communications: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis: Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation : Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- Improvements : Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RECOVER

- Recovery Planning : Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications : Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

The Cybersecurity Talent Gap

- Increasing digitisation of customer and business records and the proliferation of interconnected devices have resulted in greater avenues for cybercriminals, unfortunately, educational institutions have not expanded capacity quickly enough to keep pace with demand in the sector.
- More than 14% of IT spend is on Security
- Top 10 best job in United States
- There is a distinct (manpower and skills) gap in the area of Cybersecurity, and the gap is widening
- Cybersecurity talents gap is a major issue confronting CIOs, and it is assuming an emergency situation
- Presents a huge opportunity for young professional as a clear career pathway
- Young graduates need to create interests in this field, there is opportunity to become immediately relevant after graduation

Cybersecurity Skills in High Demands in the Industry

- Cloud Security Specialist
- Data Security Specialist
- Network Security Specialists
- Identity and Access Management Expert
- Intrusion Detection Experts
- Secure Software Development
- Security Analyst

Best IT Security Certifications

- CISSP – Certified Information Systems Security Professional
- CISM – Certified Information Security Manager
- CEH – Certified Ethical Hacking
- SANS GIAC Certification – Global Information Assurance Certification
- CPTE/CPTC – Certified Penetration Testing Engineer/Consultant
- OSCP – Offensive Security Certified Professional

Conclusion

- The current technology landscape is riddled with security challenges, hence Integrating cyber-resilience into enterprise-wide risk management and governance process is a must do for ALL establishment or they will soon be extinct.
- This landscape presents a unique opportunity for Computer Science and Engineering graduates to acquire relevant skills in this area so that they can become immediately relevant in the industry after graduation.