**ASSESSMENT 29**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | 19-06-2020 | **Name:** | Sheela Golasangi |
| **Course:** | Introduction to Cyber Security | **USN:** | 4AL16EC068 |
| **Topic:** | * Compliance * Governance * and industry standards * Career and industry landscape * Program relevance | **Semester & Section:** | VIII  ‘B’ |
| **Github Repository:** | Sheela-Course |  |  |
| **Forenoon Session Details** | | | |
| Report **Image of the session**  **C:\Users\india\Pictures\Screenshots\Screenshot (495).png** C:\Users\User\Pictures\Screenshots\Screenshot (262).pngWhat is compliance? In general, compliance is defined as following rules and meeting requirements. In cyber security, compliance means creating a program that establishes risk-based controls to protect the integrity, confidentiality, and accessibility of information stored, processed, or transferred.  However, cyber security compliance is not based in a stand-alone standard or regulation. Depending on the industry, different standards may overlap, which can create confusion and excess work for organizations using a checklist-based approach.  For example, the healthcare industry needs to meet [Health Insurance Portability and Accountability Act (HIPAA)](https://www.zeguro.com/blog/hipaa-security-risk-assessment-for-small-practices) compliance requirements, but if a provider also accepts payments through a point-of-service (POS) device, then it also needs to meet [Payment Card Industry Data Security Standard (PCI DSS)](https://www.zeguro.com/ebook/cybersafety101-thank-you)requirements.  Moreover, as compliance requirements shift from control-based to risk-based, the landscape of cyber security compliance also shifts. 5 Steps to Creating a Cyber security Compliance Program1. Create a Compliance Team Even in small to mid-sized businesses, a compliance team is necessary. Cyber security does not exist in a vacuum. As organizations continue to move their business critical operations to [the cloud](https://www.zeguro.com/blog/a-cloud-infrastructure-101), they need to create an interdepartmental workflow and communicate across business and IT departments. 2. Establish a Risk Analysis As more standards and regulations focus on taking a risk-based approach to compliance, organizations of all sizes need to engage in the risk analysis process. IDENTIFY Identify all information assets and information systems, networks, and data that they access. ASSESS RISK Review the risk level of each data type. Determine where high risk information is stored, transmitted, and collected and rate the risk of those locations accordingly. ANALYZE RISK After assessing risk, you need to analyze risk. Traditionally, organizations use the following formula:  Risk = (Liklihood of Breach x Impact)/Cost SET RISK TOLERANCE After analyzing the risk, you need to determine whether to transfer, refuse, accept, or mitigate the risk. 3. Set Controls Based on your risk tolerance, you need to determine how to mitigate or transfer risk. Controls can include:   * Firewalls * Encryption * [Password policies](https://www.zeguro.com/blog/five-tips-for-better-cyber-hygiene) * [Vendor risk management program](https://www.zeguro.com/blog/third-party-cyber-risk) * [Employee training](https://www.zeguro.com/blog/security-training-for-employees-5-steps-to-stronger-cybersecurity) * [Insurance](https://www.zeguro.com/cyberinsurance)  4. Create Policies Policies document your compliance activities and controls. These policies serve as the foundation for any internal or external audits necessary. 5. Continuously Monitor and Respond All compliance requirement focus on the way in which threats evolve. Cybercriminals continuously work to find new ways to obtain data. Rather than working to find new vulnerabilities, called Zero Day Attacks, they prefer to rework existing strategies. For example, they may combine two different types of known ransomware programs to create a new one.  C:\Users\india\Pictures\Screenshots\Screenshot (543).png  [Continuous monitoring](https://www.zeguro.com/blog/continuous-monitoring-for-stronger-cybersecurity) only detects new threats. The key to a compliance program is to respond to these threats before they lead to a data breach. Without responding to an identified threat, the monitoring leaves you open to negligence arising from lack of security.  **Cyber Security Governance**  **Introduction:** Cyber Prep is a conceptual framework, together with a practical methodology, which an organization uses to define and implement its strategy for addressing adversarial threats related to its dependence on cyberspace. In particular, Cyber Prep enables organizations to articulate their strategies for addressing the advanced persistent threat (APT). The Cyber Prep framework defines five levels of organizational preparedness, characterized in terms of The organization’s perspective on, and/or assumptions about, the threat it faces The organization’s overall strategy for addressing the cyber threat (see Table 1, below), including which adversary tactics, techniques, and procedures (TTPs) it addresses. The organization's approach to cyber security governance. This white paper presents the governance component of Cyber Prep, which is driven by the organization’s overall cyber security strategy.1 The governance component complements the part of Cyber Prep that addresses technical and operational security measures, which is driven by the organization’s assumptions and/or knowledge about adversary TTPs as well as its strategies regarding Which architectural approaches the organization takes; Which technical and operational security measures the organization selects from generally accepted standards of good practice, tailors, supplements, and uses When and how the organization adopts new architectural, technical, and/or operational approaches. Cyber Prep expects that organizations apply sound principles for information systems security governance (see Appendix B) and make effective use of standards of good practice for security management.3 The cyber security governance component of Cyber Prep focuses on what organizations must do differently from or in addition to generally accepted information security governance practices in order to address the APT. Cyber security governance determines how generally-accepted management controls (including, in particular, risk assessment controls) are tailored, supplemented, and used in the face of the APT. Cyber security governance also reflects the overall enterprise risk management strategy and enterprise risk governance framework. In Cyber Prep, the five levels of organizational preparedness entail different approaches to Strategic integration. To what extent is the cyber security strategy integrated with other organizational strategies? To what extent does the strategy extend beyond the organization? Disciplines. What disciplines are part of, or aligned with, cyber security?  **Career Growth in Cyber Security**  In a cyber security workforce study conducted by (ISC)2 on October 2018, it was projected that by 2019, the industry would be short of [3 million](https://www.isc2.org/workforce-study) cyber security professionals. Another report by Cyber security Ventures predicted a 3.5 million shortfall by 2021. Going by this trend, it would be right to infer that the demand for cyber security professionals is here to stay.  What does this mean for individuals desiring to venture into a career in cyber security?  Positive outlook, right?  However, these 5 important factors will help shape the cyber security professional.   1. **Formal Education**   While it is not cast in stone that you have a degree to pursue a career in cyber security and honestly not many started at this point, employers still have some value attached to a bachelor’s degree.  With a bachelor’s degree in cyber security or a degree in a related field like computer science or information technology, you will have started your career on a high note and with an added advantage.   1. **Experience**   The one challenge that the cyber security field faces is a wide skills gap. This has resulted in high demand for professionals and a talent pool that does not fit the skills requirements. Skills are best acquired through learning and doing.  It is possible to gain some experience through self-learning even without a formal educational background in a related field. However, you will need deep interest, passion, and a lot of patience to achieve your goals. Secondly, you must learn the basics before getting to the practical.   1. **Certifications**   In cyber security, certifications matter a great deal. Certifications are skill-specific. They are one way of achieving specific goals, especially if you want to sharpen specific skills in cyber security or curve your career path.  Certifications like the ones listed below are good and can help you boost your skills at any point in your career.   * CISSP (Certified Information Systems Security Professional) * CISM (Certified Information Security Manager) * CEH ([Certified Ethical Hacker](https://www.simplilearn.com/cyber-security/ceh-certification)) * CCSP (Certified Cloud Security Professional) | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | 19-06-2020 | **Name:** | Sheela Golasangi |
| **Course:** | Introduction to Ethical Hacking | **USN:** | 4AL16EC068 |
| **Topic:** | * Ethical hacking on mobile platforms - Demonstration * Ethical hacking in network architecture - Demonstration | **Semester & Section:** | VIII  ‘B’ |
| **Github Repository:** | Sheela-Course |  |  |

|  |
| --- |
| **Afternoon Session Details** |
| **Image of the session**  C:\Users\User\Pictures\Screenshots\Screenshot (264).png  Imagine an attack surface that is spread across your organization and in the hands of every user. It moves regularly from place to place, stores highly sensitive and critical data, and sports numerous and different wireless technologies all ripe for attack. Unfortunately, such a surface already exists today: mobile devices. These devices constitute the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.  SEC575 Now Covers Android 10 and iOS 13  SEC575: Mobile Device Security and Ethical Hacking is designed to give you the skills to understand the security strengths and weaknesses of Apple iOS and Android devices. Mobile devices are no longer a convenience technology - they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores across the world. Users rely on mobile devices more today than ever before -- we know it, and the bad guys do too. The SEC575 course examines the full gamut of these devices.  Learn How to Pen Test the Biggest Attack Surface in Your Entire Organization  With the skills you learn in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and manipulate apps to circumvent client-side security techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS, and you'll bypass lock screen to exploit lost or stolen devices.  Take a Deep Dive into Evaluating Mobile Apps and Operating Systems and Their Associated Infrastructures  Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review ways to effectively communicate threats to key stakeholders. You'll leverage tools, including Mobile App Report Cards, to characterize threats for managers and decision-makers, while also identifying sample code and libraries that developers can use to address risks for in-house applications.  To be an EC Council Certified Ethical Hacker, you have to be thorough with the EC Council course materials. You should not only master the theoretical aspect of it but also the step by step implementation of all the processes.  Here’s a webinar video hosted 21st of November 2017 by Mr. Joe Davis, Business Manager, Americas and presented by Mr. Syama Prasad a Certified Ethical Instructor by EC Council.  Mr. Syama gives you a feel of working on iLabs. The access to this is provided along with the Training and Certification course provided by GreyCampus.  In the video Mr. Syama covers:   * Collecting information from target websites ( eg. session id, platform, technologies, organization details like email, phone number and fax) using firebug & web data extractor which demonstrate steps of Reconnaissance. * UDP & TCP packet crafting techniques using hping3. * Gaining windows 8 machine access using Metasploit exploitation toolkit. * Maintaining access to system using spytechspyagent. |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |