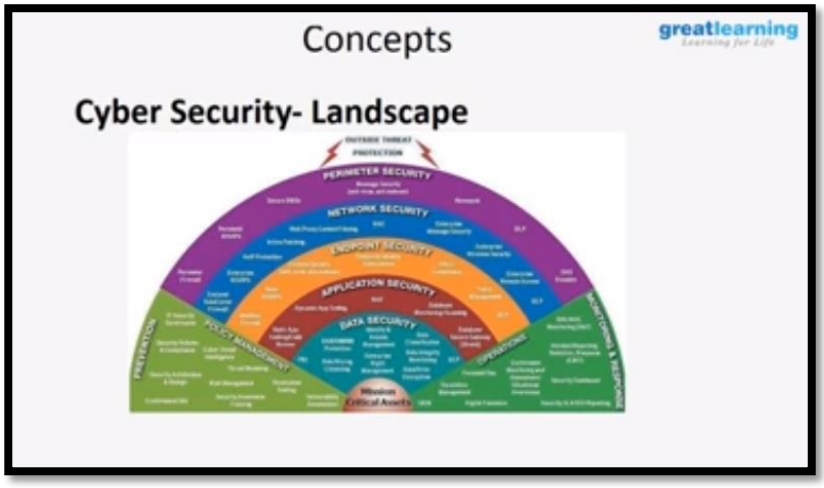
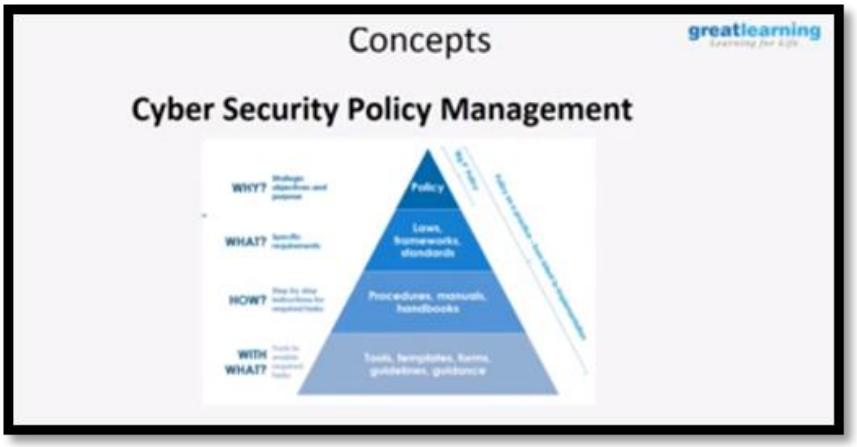
DAILY ASSESSMENT

Date:	**17/06/2020**	**Name:**	**Davis S. Patel**
Course:	**Cyber Security**	**USN:**	**4AL16EC045**
Topic:	**Governance and Risk Introduction to Cryptography**	**Semester & Section:**	**8th - A**
GitHub Repository:	**Davis**		

FORENOON SESSION DETAILS

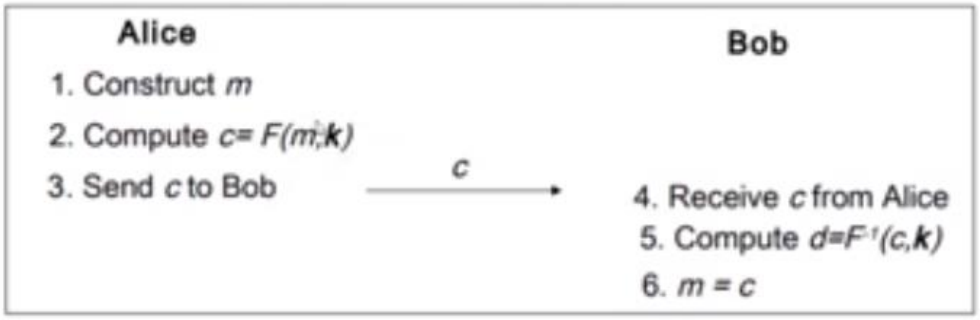
Image of session





Symmetric Key Cryptography

Alice encrypts a message with the same key that Bob uses to decrypt.



Eve can see c, but cannot compute m because k is only known to Alice and Bob.

```
Cipher Text - 176e1o87e67832tei372t923y8eyxeh9oy8do7y

(Internet)

4 bit
4 bit

18 bit
18 bit

6 bit
18 bit (first 6 bits)

Bob
--------
Cipher Text - 176e1o87e67832tei372t923y8eyxeh9oy8do7y

Symmetric Key - "We are still working under quarantine"
Hex Key - 38n26eo32o23y7o7yeoh7yeoyo3e39
```

REPORT –

When it comes to cybersecurity, governance, risk and compliance (GRC) is often a second thought and seen as the bureaucracy getting in the way of threat prevention. However, their importance shouldn't be underestimated. A focused GRC program establishes the foundation to allow organizations to meet their security and compliance objectives. If done well, this proactive approach to cybersecurity can minimize reactive incident response for businesses.

Cybersecurity as a whole is made up of three component parts - people, processes and technology. Out of the three, technology is often focused on most, as it's arguably the simplest element to enact. However, for a businesses to successfully reach their security goals, all three elements need to be considered with a programmatic, flexible and scalable approach. To achieve this, an effective GRC program is crucial, as it ensures a holistic view has been taken, whilst tackling the daunting mission of cybersecurity. After all, automating a poorly thought out process with cutting edge technology doesn't improve the process itself or the resultant outcome. Take, for instance, a security operations employee who is faced with four events to monitor and mitigate. Without a GRC program, they would have no context on the business risk or compliance impact of the events, meaning they would need to rely solely on technology and stove-pipe processes. As a consequence, they are at risk of incorrectly prioritizing the least important issue in a way they wouldn't have with a GRC program in place.

Whilst governance, risk and compliance are often viewed as separate functions, taking a holistic view on these fundamental components demonstrates the symbiotic relationship they share. Governance ensures that organizational activities are aligned in a way that supports the organization's business goals. Risk that is associated with any organizational activities is identified and addressed in a way that supports an organization's business goals. Compliance allows all organizational activities to be operated in a way that meets

the laws and regulations impacting those systems. And all three aspects work together to create an approach which will enable security architecture, engineering, and operations to be aligned with the wider business goals, while effectively managing risk and meeting compliance objectives.

Governance

To establish base governance, it's vital to first identify compliance requirements. This means investigating and understanding contract obligations, compliance frameworks and identifying required or chosen standards that need to be implemented. Following this, you must conduct a program assessment to understand the capabilities and maturity of your current profile, determine what your target profile is, and create a plan for how you will achieve this. Your strategy should consider procurement, DevSecOps, management, security and human resource allocation, including defining and assigning functions, roles, and responsibilities.

Finally, you need to update and publish your new policies, processes, procedures to educate your employees and reassure that cybersecurity and governance is upheld. Your policies should clearly align with your business objectives. While your processes must specify how to upgrade old technologies for the adoption of modern organization and management techniques, and how your procedures integrate cloud services and other emerging technologies.

Risk

The second stage in scaling your GRC policy is looking at your risk management. Conducting a risk assessment for every aspect of your organization and each business line and asset type is paramount. Once this is done and you have full understanding over the risk within your business, you can implement a plan to mitigate, avoid, transfer, or accept risk at each tier, business line, and asset.as well

Risk management frameworks can then be used to track systems by selecting controls and risks which can be continuously monitored and adjusted as the business grows and threat landscape increases. The final stage is incorporating risk information into leadership decision making. To put it simply, it should become routine to ask “what the financial, cyber, legal is and reputation risk to our business of making this decision.” By embedding this approach into your culture, you can ensure that you have complete visibility over your risk position, when make critical business decisions and driving company growth.

Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. OpenPGP is also about the latter sort of cryptography. Cryptography can be strong or weak, as explained above. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. How difficult? Given all of today's computing power and available time — even a billion computers doing a billion checks a second — it is not possible to decipher the result of strong cryptography before the end of the universe.

One would think, then, that strong cryptography would hold up rather well against even an extremely determined cryptanalyst. Who's really to say? No one has proven that the strongest encryption obtainable today will hold up under tomorrow's computing power. However, the strong cryptography employed by OpenPGP is the best available today. Vigilance and conservatism will protect you better, however, than claims of impenetrability.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key. A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. OpenPGP is a cryptosystem