**DAILY ASSESSMENT REPORT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **16/06/2020** | **Name:** | **Gaganashree P** |
| **Course:** | **Cyber Security** | **USN:** | **4al15EC024** |
| **Topic:** | **1. About cyber security and its motivation**  **2. Secure system design & security goals**  **3. Threats** | **Semester & Section:** | **8th &"A" section** |
| **Github Repository:** | **Gaganashree-P** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| **Report–**  **What is Cyber Security?**  Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.  **THE IMPORTANCE OF CYBER SECURITY**  [Cyber security](http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm) is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the [volume and sophistication of cyber attacks grow](https://digitalguardian.com/blog/biggest-incidents-cybersecurity-past-10-years-infographic), companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation’s top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.  **CHALLENGES OF CYBER SECURITY**  For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. [Elements of cyber](http://whatis.techtarget.com/definition/cybersecurity) encompass all of the following:   * **Network security:**The process of protecting the network from unwanted users, attacks and intrusions. * **Application security:** Apps require constant updates and testing to ensure these programs are secure from attacks. * **Endpoint security:** Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company’s network. * **Data security:**Inside of networks and applications is data. Protecting company and customer information is a separate layer of security. * **Identity management:** Essentially, this is a process of understanding the access every individual has in an organization. * **Database and infrastructure security:** Everything in a network involves databases and physical equipment. Protecting these devices is equally important. * **Cloud security:** Many files are in digital environments or “the cloud”. Protecting data in a 100% online environment presents a large amount of challenges. * **Mobile security:**Cell phones and tablets involve virtually every type of security challenge in and of themselves. * **Disaster recovery/business continuity planning:** In the event of a breach, natural disaster or other event data must be protected and business must go on. For this, you’ll need a plan.End-user education: Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes, 2-factor authentication, etc.) is an important part of cybersecurity.   The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology ([NIST](http://www.nist.gov/)) issued guidelines in its risk assessment [framework](https://www.nist.gov/cyberframework) that recommend a shift toward [continuous monitoring](https://digitalguardian.com/blog/what-continuous-security-monitoring) and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.  **MANAGING CYBER SECURITY**  The National Cyber Security Alliance, through [SafeOnline.org](https://staysafeonline.org/), recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing [cyber security management](https://staysafeonline.org/cybersecure-business/) across all business practices. NCSA advises that companies must be prepared to “respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company’s reputation are protected.” NCSA’s guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization’s “crown jewels,” or your most valuable information requiring protection; identifying the threats and risks facing that information; and outlining the damage your organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way your company collects, stores, and secures data, such as [PCI-DSS](https://digitalguardian.com/blog/what-pci-compliance), [HIPAA](https://digitalguardian.com/blog/what-hipaa-compliance), [SOX](https://digitalguardian.com/blog/what-sox-compliance), [FISMA](https://digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more), and others. Following a cyber risk assessment, develop and implement a plan to mitigate cyber risk, protect the “crown jewels” outlined in your assessment, and effectively detect and respond to [security incidents](https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/types-of-security-incidents). This plan should encompass both the processes and technologies required to build a mature cyber security program. An ever-evolving field, cyber security best practices must evolve to accommodate the increasingly sophisticated attacks carried out by attackers. Combining sound cyber security measures with an educated and security-minded employee base provides the best defense against cyber criminals attempting to gain access to your company’s sensitive data. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures.  **2.Secure system design & security goals**    Security Principles  Address Privacy & Security  Statement: Address Privacy & Security  Rationale: Information is power and this is certainly true in the context of technology-enabled global development interventions. How information is collected, stored, analysed, shared, and used has serious implications for both the populations about whom data are being transmitted, and the organizations transmitting the data.  Implications: Assess and mitigate risks to the security of users and their data. Consider the context and needs for privacy of personally identifiable information when designing solutions and mitigate accordingly. Ensure equity and fairness in co-creation, and protect the best interests of the end end-users.  Always consider the users  Statement: Always consider the users  Rationale: The security of a software system is linked to what its users do with it. It is therefore important that all security-related mechanisms are designed in a manner that makes it easy for users to deploy, configure, use, and update the system securely. Security is not a feature that can simply be added to a software system, but rather a property emerging from how the system was built and is operated. The way each user interacts with software is dictated not only by the design and implementation decisions of its creators but also by the cognitive abilities and cultural background of its users.  Implications: Failing to address this design principle can lead to a various problems, e.g.: When designers don’t “remember the user” in their software design, inadvertent disclosures by the user may take place. If it is difficult to understand the authorization model, or difficult to understand the configuration for visibility of data, then the user’s data are likely to be unintentionally disclosed. Designers sometimes fail to account for the fact that authenticated and properly authorized users can also be attackers! This design error is a failure to distrust the user, resulting in authorized users having opportunities to misuse the system. When security is too hard to set up for a large population of the system’s users, it will never be configured, or it will not be configured properly.  **3. Threats**    The term itself originates from the military, where a red team would play the role of an adversary and act as attackers, and a blue team would act as defence. In cybersecurity, red teaming has come to refer to a team of ‘ethical hackers’ who simulate a cyber attack. It is already widely used in financial services and defence, and its usage is expanding across a wider range of industry sectors as more organisations seek ways of addressing the risks associated with their data.  RT is able to provide insights that cannot be achieved with a traditional PT approach. This is because their objective and scope is far wider. PT is usually limited to testing a particular network, system or application, with the objective of identifying as many vulnerabilities as possible, within the scope of the test, and trying to exploit them. RT goes beyond system-specific tests and instead focuses on your organisation’s broader information assets; analysing, for example, whether intellectual property can be stolen; whether customer contact lists, personally identifiable information and payment details are adequately secured. Although RT conducts some similar exercises to PT, they are not aiming to uncover every single vulnerability, just those that will enable them to access the critical information.  Choosing the right strategy  RT therefore plays a key role in providing insight into a company’s capabilities to withstand a potential cyber attack and to identify the steps they need to take to mitigate risk effectively. But is the approach right for every business?  The right testing strategy for your organisation will depend on your objectives, risk level, security maturity and budget:  Objectives: If your objective is to understand if your most critical assets are secure then a real-world approach to testing is essential. A RT approach will identify the threats to which you are vulnerable and highlight blind spots that are unlikely to be identified through traditional PT techniques.  Risk level: What information assets do you hold? What are the threats, vulnerabilities, likelihood and impact of these assets being compromised? For instance, if personal or sensitive data is stolen what will be the financial and reputational consequences? If these are significant, you need a proactive approach to managing them. RT testing delivers insight that will help to improve risk management strategies and processes, ultimately designed to mitigate your risk.  Security maturity: How sophisticated is your security program? Have you conducted extensive PT and patched vulnerabilities? An RT approach is most likely to benefit an organisation with a more mature security program but there are exceptions. RT can also be useful if you have not yet embarked on your security journey; it can provide visibility of your weaknesses and risks, and help shape the requirements of your ongoing security program. Equally, significant changes to your organisational structure may require another evaluation of testing strategy to ensure it meets your evolving business needs. |