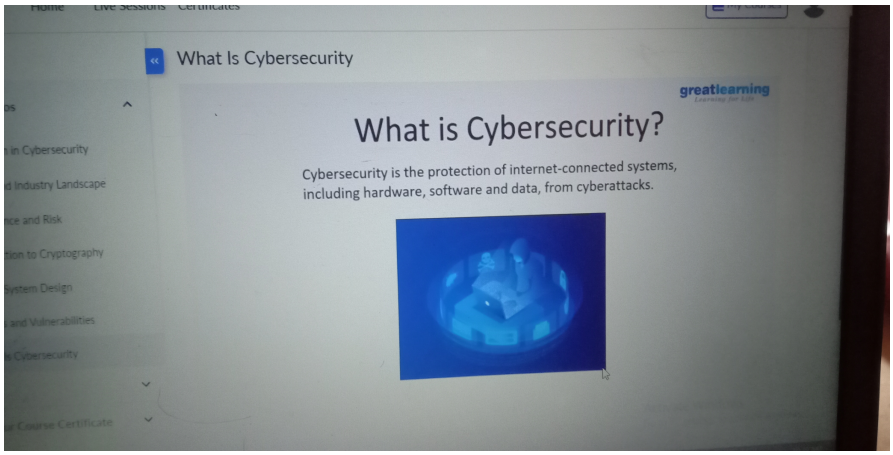
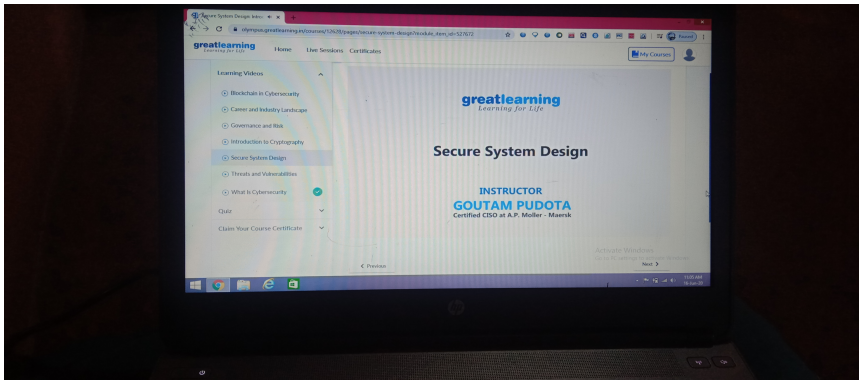
JUNE 16 REPORT

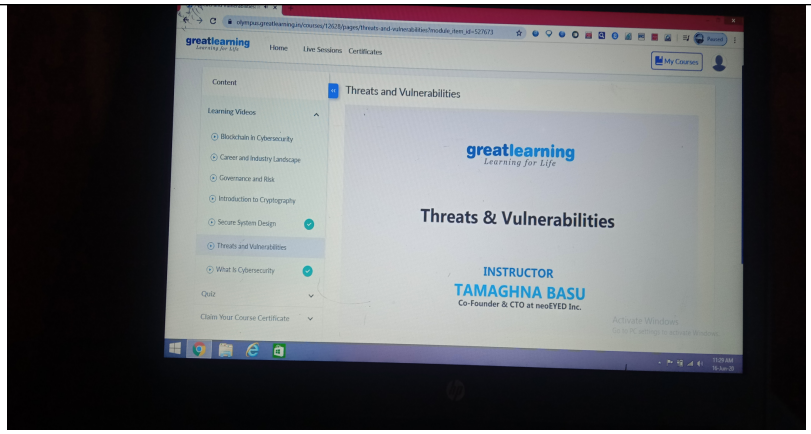
Date:	16/06/20	Name:	ANKITHA C C
Course:	Cyber security	USN:	4AL16EC004
Topic:	1. About cyber security and its motivation 2. Secure system design & security goals 3. Threats	Semester & Section:	8TH & A
Github Repository:	ankitha-course		

FORENOON SESSION DETAILS

Image of session





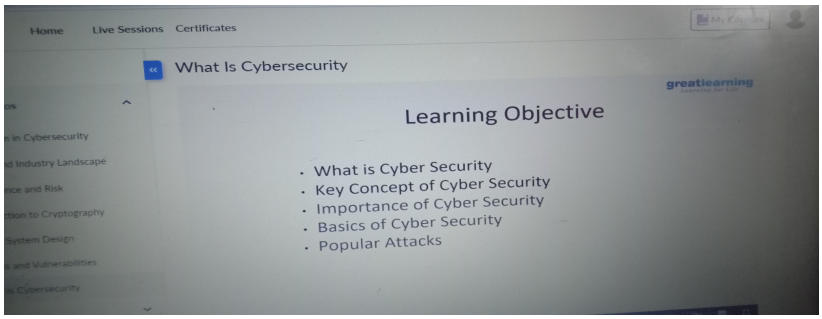


Report – Report can be typed or hand written for up to two pages.

1. What is cyber security and what is the motivation behind it

coming up with new and determined methods of threat that are increasingly difficult to detect, making attacks more dangerous than ever before.

Statistics show that cybercrime is on the rise around the world. It's estimated that by 2021 the annual cost of damages from cybercrime will cost the world $6 trillion. That's a significant jump from $3 trillion in 2015, with cyber-attacks now one of the most serious threats to any business.



No matter the size of your organization, whether you're a start-up business or have scaled to a million-dollar company, you need to be aware of the risk of a cyber-attack.

What's the motivation behind all this cybercrime? The results of studies done on cyberhacking show that the motivation behind 90% of attacks is about financial gain and espionage. Here's a closer look at the most-breached industries, who is doing the hacking, and what type of data is being hacked.

What data is hacked?

The data being hacked from businesses and organizations is specific and of value to cybercriminals. Hackers look for this data so they can make money, steal personal identities, and for blackmail. Still, other information is sold to external parties for malicious intent.

Most hacked assets

Hacking assets can be taken from information that can be directly stolen from computing devices and networks. This information can be directly used by hackers and includes both personal and financial information. The top data assets

involved in security breaches include:

Databases: Network databases are involved in 18% of security breaches. One reason for this is that businesses typically use a database to store all their company and customer information. The infrastructure security of databases is constantly at risk. Making them vulnerable to the sophisticated software that hackers are continually creating.

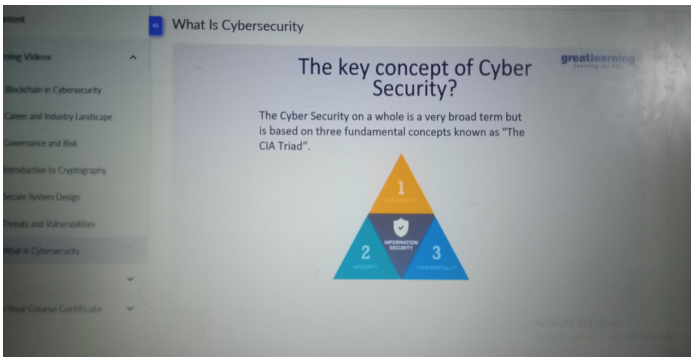
POS terminals: Making up 16% of breaches, POS terminals are at risk. Especially from malware that can easily be installed, accessing the system and stealing data such as credit card information.

POS controllers: Another 16% security risk is POS controllers which are just as vulnerable to cyberhacking and malware attacks. The POS system is linked to business and customer information and the business payment process.

Most hacked data type

The most common types of data targeted by cybercriminals include personal, payment information, and medical records.

Key concepts



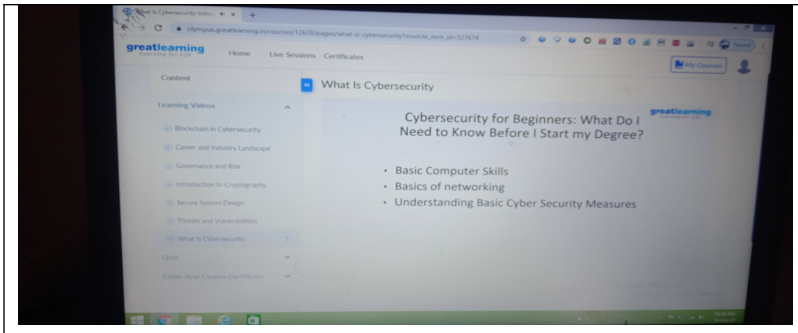
Personal: 36% of compromised data is personal information. Including name and address, social security number, and contact information such as email and phone. This data is often used in identity theft and can be used to apply for loans and open new credit cards.

Payment: Payment information compromises 27% of the data stolen in cyber-attacks and can include credit card numbers and other financial information. Once hackers have credit card information, they can make immediate online purchases.

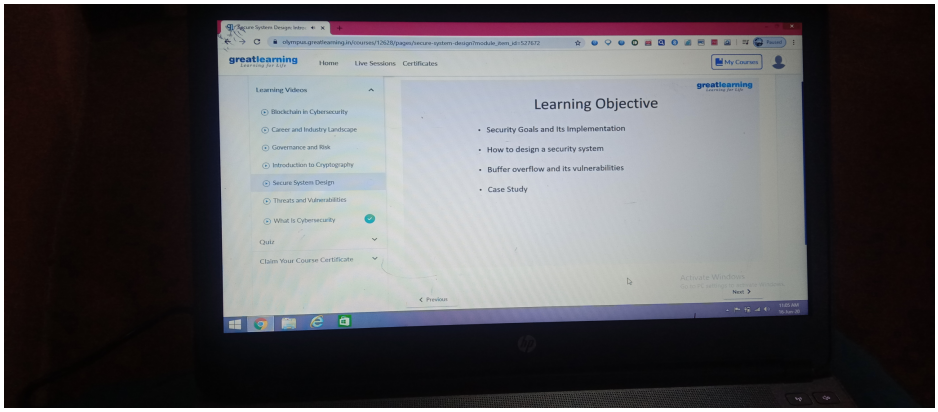
Medical: Personal medical information can be used by hackers to buy medications or receive medical treatment. Medical data makes up 25% of security breaches.

Hackers are continually finding new ways to steal your data. Is your business at risk? It's important that you know what types of businesses are most vulnerable and why. No matter how large or small your company, hackers are looking for a sensitive date to use to their advantage. By understanding the motivation of these cybercriminals, you can stay ahead by using preventive measures to keep your business data secure.

Learn more about how to protect your business and customers or clients by reading the full Hacker Motives: Red Flags and Prevention infographic by Varonis. You'll find out what motivates hackers and what you can do to keep your confidential information safe



2.Secure system design & security goals



Security Principles

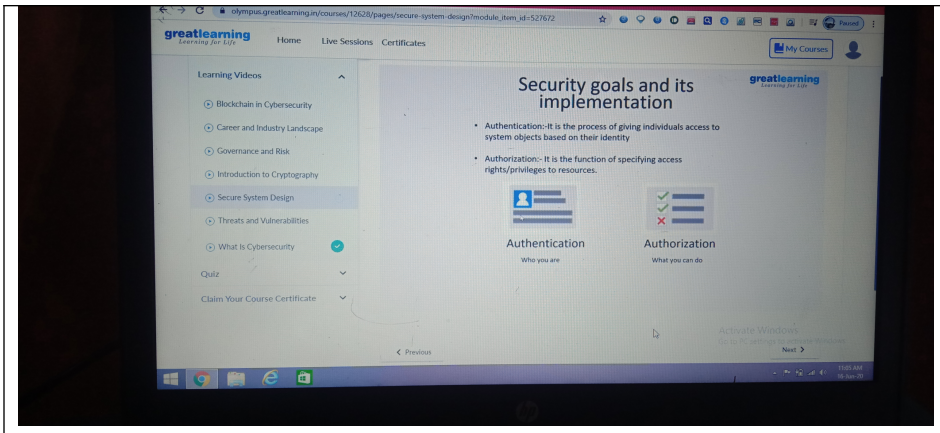
Address Privacy & Security

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

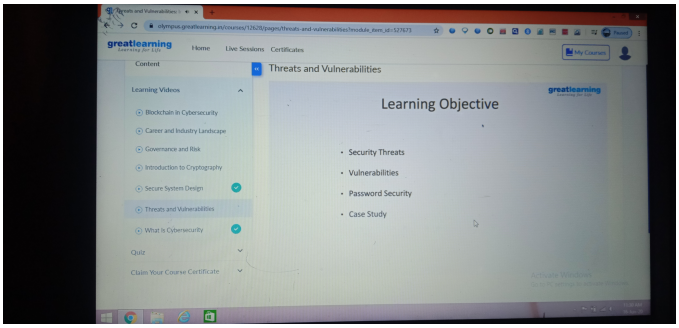


Statement: Always consider the users

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.

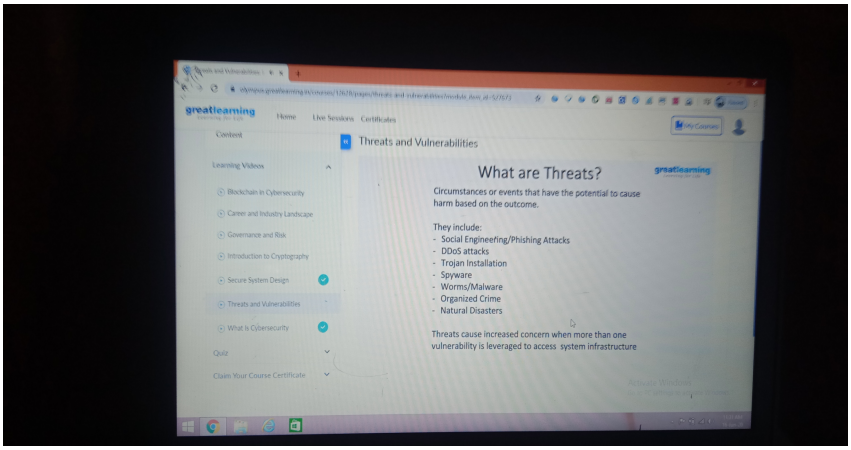
3. Threats



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.