Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 01

Introduction to the Course: Practical Cybersecurity for Cyber Practitioners

So those of you who are here learning practical cybersecurity for cyber practitioners, many of you have probably not taken a cybersecurity course before and therefore I do not know how much you will get from this course so as we go you still have time for dropping so there is some time so today I would like to clarify what is it in this course and after that you can make your decisions but the course is quite a lot of work. So you have to accordingly decide. So cybersecurity is a very big buzzword today. Every day if you read the technology news, you will see somebody or the other is getting ransomware attacks. or somebody's data breach is happening.

We had a large-scale data breach from ICMR on the data that was collected during the COVID vaccination. Very large scale data leakage had happened. Some years ago, around 2020, 21, There was data leakage from dominos, data leakage from big basket. So data leakage, ransomware attacks are very common. We also get attacked continuously in thousands per minute, even IIT Kanpur systems, right? So many of the attacks are not very effective, so we do not see a whole lot of problems.

But you might have received an email from the Dean of Digital Infrastructure(IIT Kanpur) to change your password for Pingala, your password for your(students) CC login. because we found a data leak that was two years old. The data that was leaked was two years old. But we found that many of your passwords were the same for the last two years. And therefore, from the leaked password, anybody could log into your account.

So that's why we ask that everybody changes their passwords immediately. And we are working towards instituting two-factor authentication for all logins in the institute, but that might take some time. But in any case, cybersecurity is a big problem today. Now the question is what is it that we need to learn? So we have courses that teach you how to find vulnerabilities in web applications with standalone applications in operating systems, in networks, DNS routing protocols and so on. That course is CS 628.

In that you learn how to find vulnerabilities and how to exploit vulnerabilities. And that's the hacking 101 type of course. We also have courses on malware analysis. where you actually take malware and analyze them with various tools. Then you actually build your own malware detection tools using machine learning.

You also learn how to detect from the network activities inside your own network, maybe home network or organizational network, how to find intrusion. that some unwanted activities are happening inside your network. And that course is CS658, that's a malware analysis and intrusion detection course. We have a course on how to protect cyber from cyber attacks in critical infrastructure such as power plants, water treatment plants, oil and gas pipelines and so on. So that's CS631.

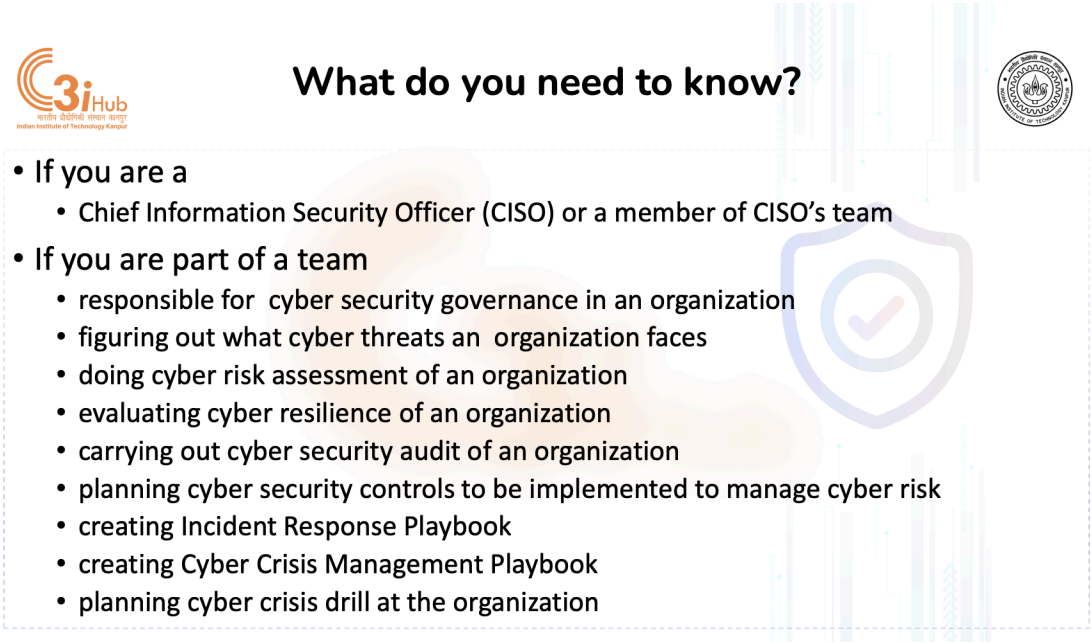
And then we have courses related to cryptography, CS641. There is a new course, CS670, that is about privacy and cryptography. And then there are courses on hardware security.I believe it's hardware security for IoT devices. So there are plenty of courses which teach you the technology behind cybersecurity, how different tools are developed, both for attacking the applications, the networks, the organizational IT systems, the OT systems, the operational technology systems in plants, manufacturing plants or power systems and so on. We also have courses where you learn how to develop tools for doing detection, how to detect that your system is under attack or our system has been attacked. So that's the malware analysis, intrusion detection, side channel analysis, those kinds of courses.

We also have courses where you actually learn about a very specific domain in cybersecurity, which is critical infrastructure security. So power grid security and manufacturing system security and so on. We also have courses where you learn nitty gritty of cryptography, like what are the algorithms used in, for example, HTTPS, SSL, TLS, right? What are the algorithms that are used for encryption inside your disk for file encryption? And what are the weaknesses that can be exploited by attackers? And how better algorithms are being developed? So that's in the modern cryptology course. And there are implementations of cryptography which may be problematic. And this implementation of cryptography problems manifest as side channels.

So side channel analysis courses are there. Post quantum cryptography. As quantum computing is becoming more likely by 2030 there should be, It is expected that quantum computing would be somewhat practical. In fact, probably in countries like China, then some of our cryptography like RSA, Diffie-Hellman, etc.

will break. And then there are efforts, pretty advanced efforts for developing cryptography that is not breakable by quantum computing. And there is a course for post-quantum cryptography. So there are lots of courses. So that's about technology. But cybersecurity actually is not only technology.

It has three components, people, process, and technology. So therefore, it is very important that we understand how the other components of cybersecurity works, people and processes. Technology is one part of it, but it's not enough. So we'll try to explain throughout this course that there are things in organizational cybersecurity that are not necessarily doable by buying expensive tools or developing tools or using AI ML tools. And that's where this course comes in.



So what do you need to know that we do not teach in the other courses? So suppose you are a chief information security officer or you are a member of his team. So the chief information security officer is in charge of organizing cyber security of any organization, right? And larger organizations, in today's world, All organizations, it may be a news media organization, it could be a manufacturing organization, it could be a power systems operator, it could be an oil and gas refinery, or it could be a food product manufacturer. Everybody has computing, network, data, everything. So every organization has a CISO. Some organizations have multiple CISOs for multiple verticals of their business.

This CISO usually has a team through which the cybersecurity activities will be organized and taken. So obviously, right out of college, nobody is going to give you a CISO job that comes after many years of working in cybersecurity. However, you can be hired as a team member of a CISO. So if you are a team member of a CISO, you are

going to be responsible for many things.

So cybersecurity governance. So for example, if you have a cybersecurity team, can they do whatever they like? Can they reset your password whenever they like? Or can they overnight tell you that you cannot do this or you can do this? Or can they actually tomorrow create such a strong firewall with strong rules that many important websites are no longer accessible or can they actually put an agent on each of the employees computer so that, that agent collects data about what's happening on your computer and see that centrally, right? These are some of the things that a CISO would like to do. He wants to know what is happening if somebody has downloaded malware by mistake or somebody has tried to enter a database that he's not supposed to and things like that. So there are a lot of things that the CISO or his team can do but can they do it just like that? There has to be some policy, there has to be some processes by which that policy has to be developed, stakeholders has to be consulted and those policies have to be actually approved by the highest authority like the board of the company and so on and only then that in the policy the processes should be well defined and then these processes have to be followed. So you cannot overnight say I am going to do this or do that and that's the main governance activity. So you cannot do arbitrary things just because you are in charge of security because you have to consult stakeholders, get approval and so on.

So that's the governance. Second thing that you may have to figure out, every organization has a unique threat perception. So an educational institute has a different set of threat actors. attacking it compared to let's say a power grid or compared to let's say a government website or compared to say railway transportation control system. So the organizational threat model, threat perception has to be developed based on much information including the organization's role in the entire scheme of things. in the national economy, also the organization's business goals, also the geopolitics, what is happening right now in terms of geopolitics, like last 15th August, The Indonesian army of cyber hackers they had pledged that they will attack all Indian government websites and they did quite a bit during the G20 summit there was similar threats.

So, therefore, The threats also change based on events, based on various other perspectives. So you have to know how to model the threats, how to understand the threats. Also there are threat feeds that can be obtained from commercial intelligence organizations. You have to also bring those in to do this. Suppose you want to do a risk assessment, right? So not everything inside your organization is at risk.

So a database containing the student grades is certainly at a higher risk than a database where you have the let's say menus of the halls, canteens, right? So certainly they will have different risks. Similarly, if you have an employee salary processing database and

servers, they are probably at a higher risk than departmental procurement databases, right? So you have to do a risk assessment based on what the role of the asset is, what are the vulnerabilities of that asset, and what kind of threat actors might be interested in getting a hand on that particular asset. Similarly, organizations have to be cyber resilient. That is, in case an attack succeeds, how do you actually bring back the system to life? For example, if this week Pingala gets attacked and none of you can register or drop your courses, what is the mechanism by which you can be enabled to do your dropping and adding courses, right? So that is what resilience is. Resilience is about withstanding an attack and recovering from the attack in the least amount of time.

That's the idea of resilience. So how do you design the resilience of an organization and how do you measure the resilience of an organization? Suppose you have to do an audit. You are working for consultants and you are sent to do an audit of a bank for cybersecurity. So how do you go about, what do you look for? What is it that you are going to benchmark that particular organization's cybersecurity against? So, also when you actually have done the risk assessments and you figured out that the risks are higher on these assets and risks are lower on these assets and so on. How do you go about designing the controls? So do you segment the network? Do you actually put firewalls between network segments? Do you do virtual networking or actual real physically segmented network? Are you going to put what we call endpoint agents on every device that is critical? How do you actually monitor the network on which the critical assets are there? How do you actually decide whether to have two factor authentication? And if you do, what kind of two factor authentication should be suitable? So all these things are about designing cybersecurity controls. So that is something that you have to also decide.

Then if there is an incident, cyber incident, How do you respond? What is the process? Do you panic and do things, shut down things randomly and keep calling, for example, the computer emergency response team in Delhi? What do you do? What is the playbook for your incident response? What happens if the incident actually gives rise to a crisis? Your entire data gets ransomware encrypted. and your function has to stop, nothing is working in the organization. How do you manage at that time and how do you recover? And also to be prepared for this kind of incident and this kind of crisis, you have to also do cyber drills like fire drills. So how do you go about doing cyber drill or tabletop exercises and so on? So these kinds of things are what this course is about, right? So this course will not teach you hacking or malware analysis or how to design cybersecurity tools, that kind of stuff. So for those who are not very familiar with cybersecurity,

cybersecurity is, has, there are many ways to define cybersecurity.

So one thing that I have put in here is based on the standard, National Institute of Standards and Technology, NIST, NIST standard called CSF, Cybersecurity Framework. And in Cybersecurity Framework, in the recent version, they had an earlier version until like 23, end of 23, and then now they have a recent version. In this version, they say that the cybersecurity of an organization should have six essential functions. And here I have listed the six essential functions. I will not explain these six essential functions right now because I have a lecture on the NIST framework later.

But just to tell you that identification of your assets, what are the cyber assets do you have, what kind of servers you have, how many servers, what operating system it is running, what applications are running on those servers, what desktops, laptops, mobiles are connected to your network, all this information has to be in an asset inventory, what kind of data you are possessing and what is the state of that data, is it encrypted and all that stuff. You also have to identify the vulnerabilities. What are the bugs in the systems that you are actually currently having in your organization? You have to also do risk assessment. You have to identify what are your critically risky assets.

and how to, you know, how to identify them. So all these things come in the identity. Then once you have identified the risks of all the assets, you know which ones are your most risky assets and which ones are your least risky assets and whatever middle risk and so on. Then you have to decide what security level you are going to put, not everything has to be secured in the same way because security is expensive. So most critical assets have to be secured with very strong security controls. The least risky assets may be given some leeway.

So you have to do that. Firewalls, antiviruses, endpoint security, All this stuff are part of the protect mechanism, authentication, authorization mechanisms, two factor authentication, etc. Also, cryptography, like encrypting data that is critical data all the time, even when it is at rest, that is, it is in store, as well as when it is moving through the network. Then, after identifying and protecting, many times we think that, okay, I have a firewall, I have two-factor authentication, I have encrypted data, I have the latest operating systems, and there are no old, you know, unlicensed applications or operating systems. All the operating systems are the latest ones like Windows 11 and Ubuntu 22.

04 or something but attacks will happen. So one thing that we have to all recognize even with all the best security, Attackers will find ways. And even attackers can fool the people in the organization. For example, they can send phishing emails or emails or messages, malware-laced pictures and stuff in messages, and if you download them, your computer will get infected by some malware and that malware may be a worm type of malware which can move from one machine to the other using weaknesses in various protocols like SMB protocol. You cannot assume that since you have the best protection, you cannot be attacked.

Attack will happen. All you have done by doing very good risk-driven protection is actually to reduce the possibility of the attack, but you haven't made it zero. So there will be attacks. So then the next few things are based on the assumption that attacks may happen. Detection is very important. You have to continuously have monitoring of all the endpoints and all the network traffic.

That is where the security operation center and security incident event management tools come in, right. So you have to have a full 24 by 7 visibility of your network and endpoints and when you have the visibility then you can actually spot various things and you can have AI ML to help you to determine that what you are seeing because you will see a lot of data you cannot manually figure out what is happening so there are rule based systems as well as there are AI ML driven systems that will tell you that what currently is happening looks suspicious. So they will generate alerts and you have to be able to respond to the alerts 24/7. So response is part of, when you spot something is wrong, what do you do, right? So that's the response part. Recover is when you actually have been through a crisis or been through an incident which may have encrypted your disks or which may have wiped out your data or which might have exfiltrated your data or which might have damaged your systems.

What do you do for recovery? Do you have standby systems? Do you have backup data? and make sure that the data, like people think that if I have my file system backed up in OneDrive or Google Drive, I am fine. But if you're logged into OneDrive or Google

Drive all the time, then when the ransomware hits, it will also find its way to the Google Drive or OneDrive and encrypt them. So you have to figure out a better way to do your recovery. And then governance, as I have discussed before, governing is a very important part of cybersecurity, especially organizational cybersecurity.

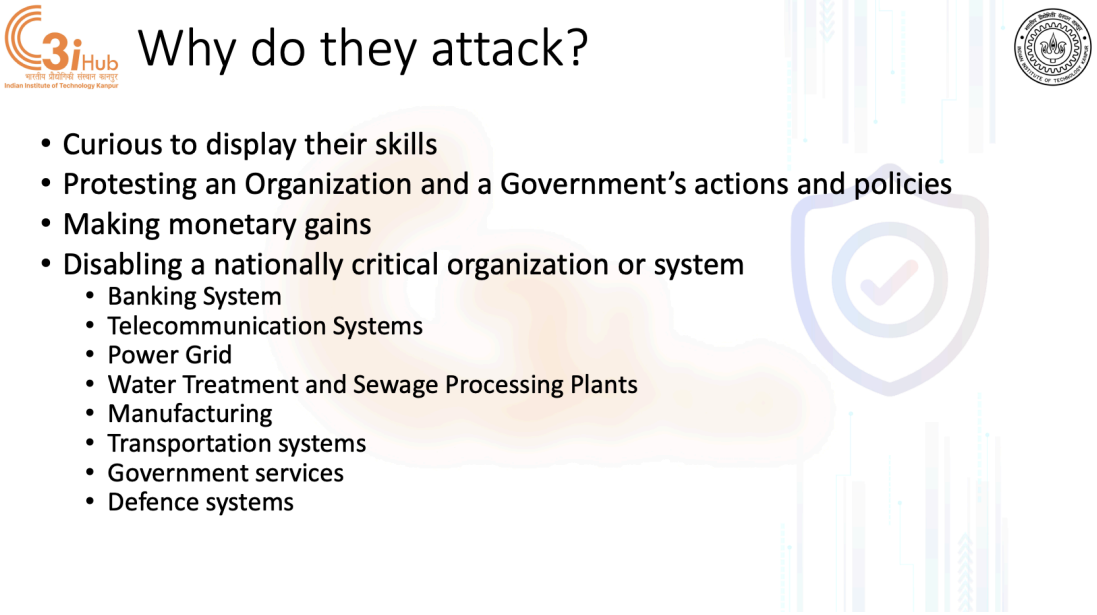
Now you might ask, who are the attackers? So if I don't know the attackers and what they want, I cannot really do a very good job in securing them. So usually we look at attackers in multiple ways. So script kiddies are the curious kids, and when I say kids, you guys are also falling in that category. So you might know how to exploit, for example, a web application, say SQL injection, command injection, and then you start trying in various places. And so that can be an attack, but that attack can be usually not very long-lasting, not very persistent, and usually they cannot do too much harm, although there have been cases, there were kids, school kids who actually breached NVIDIA.

last year and exfiltrated IP. So it is not like we should discount script kiddies but they are not as resourceful necessarily as for example nation state attackers. So there are hacktivists who would attack for example: the various organizations, governments whose policies you do not like. For example: anonymous group. Hacktivists actually also take positions like there are pro-Russian hacktivists and there are pro-Ukrainian hacktivists and they do their things.

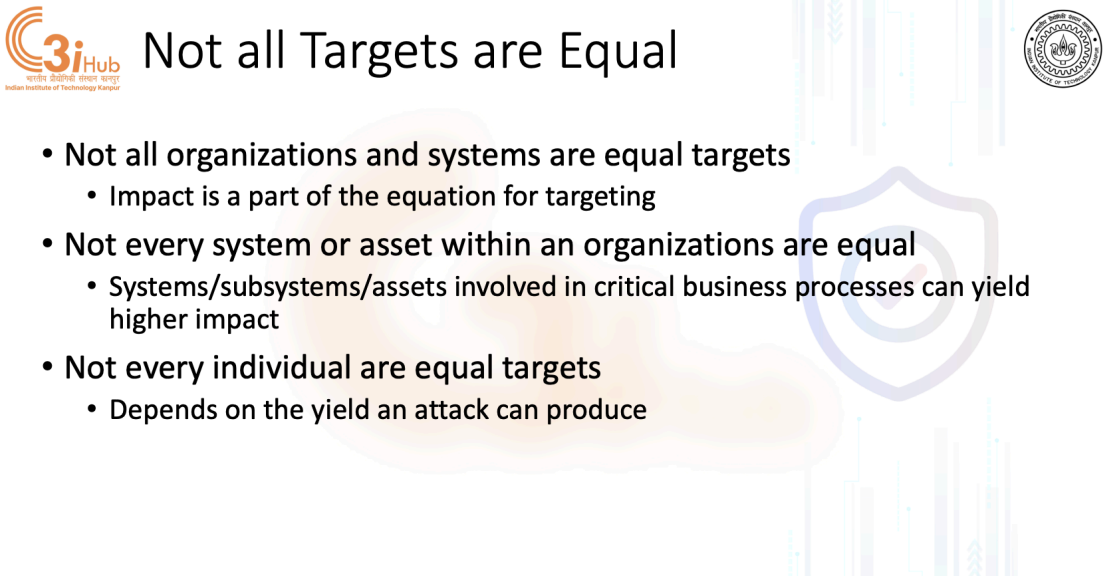
And they could be actually pretty effective. Many of them actually did very problematic things for organizations like the National Security Agency in the US. For example, they leaked a lot of vulnerabilities and their exploits in 2016 which led to the first spate of

ransomware attacks "wanna cry" because there was a bug called eternal blue in the SMB protocol in Windows and it seems NSA was using that for a long time to spy on, other countries, but that whole tool set was made public by hacktivists and then cyber criminals started creating this ransomware that basically encrypted a lot of important things including ports and so on. Cyber criminals, they actually do it for money. They try to extort you by attacking you and ransoming your, encrypting your disks and say that, you know, unless you give us cryptocurrency to this wallet address, we are not going to decrypt your data and things like that. And once people started becoming clever and took good backups, then nobody was paying the ransomware so they started double extortion, that is they also steal the data and encrypt the data and they say that if you don't pay fine we are going to leak your data in the dark web so that's a double extortion so those kind of things so cyber criminals also there are organized criminal gangs mostly Currently known criminal gangs into cybersecurity are mostly out of places like North Korea, Russia, and few other countries that is common.

But the biggest threat that we have is the nation state attackers, countries that are involved in geopolitics. And accordingly, for example, Chinese threat groups, they attack India quite a bit, Pakistani threat groups. There are Russian threat groups who attack mostly US and other US allies. So there are advanced threat groups, but we'll talk a lot more about this in the coming lectures so we can move on. I already explained to you why they attack when I was discussing the various types of attackers.



So I'm not going to go through this slide. We already discussed what happens here. Now one thing that we have to remember is that not all targets are equal. So for example, not all organizations are under the crosshair of attackers equally. Some organizations are more attacked and some are less attacked.



And it has got to do with many things. Geopolitics is one of them. Business rivalry could be another and various other reasons that some organizations are in a much more problematic situation with respect to cyber attackers than the others. So similarly, within an organization, I already discussed that risk, we have to do risk assessment because not every asset inside an organization is being used for critical functions. Some, let's say in the reception, the person sitting in the reception also has a computer connected to the network, but her computer only sees room numbers and telephone numbers of employees when a guest comes. Her laptop is not as critical an asset, for example, compared to the computer which is involved in payments or involved in keeping student registration data or grade data, right? So all assets are not equal and that's where the risk assessment comes in, that without risk assessment you cannot really formally tell what are the different assets, what their risks are.

And similarly not all individuals are equally targets. So some individuals, for example, high net worth individuals have more possibility of being a target of a cybercrime than some person who doesn't have a whole lot of things. Similarly, politicians and stuff, they might be in the crosshairs more than common people. So as I said that we have to also understand how to understand whether my organization, the organization I am protecting, what its threats are. I have to understand the threat in order to figure out the risks. When threats are high, Then we say that, for example, the US Department of Homeland Security, they use what is called a traffic light protocol. So they have like, right now the threat perception is amber, or right now the threat perception is red, Or the red means it's the highest level of threat perception.

Understanding the Geopolitics

- For large scale or high impact attacks on organizations or systems
  - Geopolitics plays a major role
- Attack on
  - Iranian Nuclear Uranium enrichment plant in 2009 - Stuxnet
  - Ukrainian Power Distribution Systems – 2015 and 2016
  - US Government Departments – Solarwind 2020
  - Indian Power Systems Operators and Ports in 2020-21
  - Indian government websites -- 2023

So right after 9-11, well, many of you were probably not born at the time, but after 9-11, the threat perception everywhere, like at the airports and everything, was red. For a long time, during the Iraq war and everything, it was amber. Now probably it is orange or probably it's green. I'm not sure. Green probably that nobody will say because green means things are very good.

So similarly, you know, you have to have a threat perception for your organization. So that, and geopolitics is important there. We have seen lots of attacks based on geopolitical considerations to various countries and their critical infrastructure, like the Iranian nuclear plant by Stuxnet, Ukrainian power system in 2015, 16, as well as more recently during the current war.

2020 solar wind attack. We'll talk about these attacks later a lot more. Indian power system operators and ports in 2021 and as well as 22. In 23, a lot of these Indonesian activists, they actually did a lot of defacing of Indian websites or DDoS attacks on airline companies and so on. Based on some geopolitical consideration, for example, whether India is supporting Israel or Hamas or India is supporting Ukraine or Russia, whether India is continuing to buy Iranian oil and all this kind of consideration. So if you are in charge of an organization like an important organization in the country, then you have to also be aware of the geopolitical considerations of cyber attack.

What not to expect from this class?

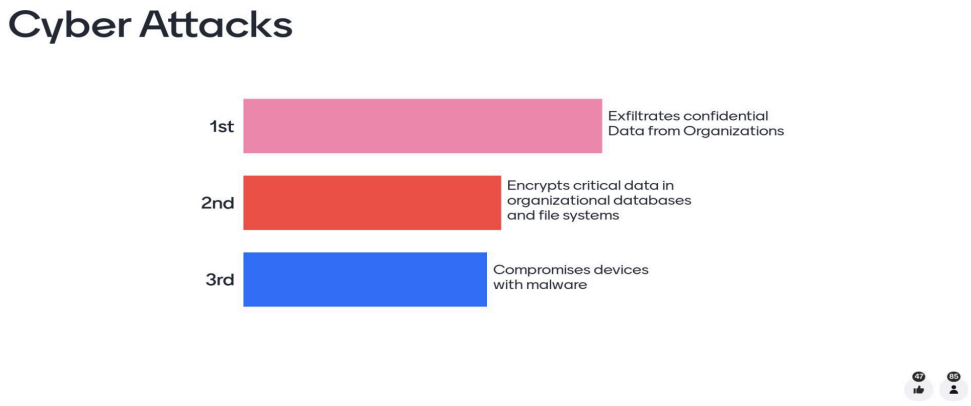
- How to hack or do VAPT? (CS 628 – Computer Systems Security)
- How to analyse malware? (CS 658 – Malware Analysis and Intrusion Detection)
- How to protect critical infrastructure from cyber-attacks?(CS631 – Cyber Security of Critical Infrastructure)
- How to analyse cryptographic protocols and algorithms? (CS 641 – Modern Cryptology)
- How to check for side channels in cryptography implementation? (CS666 – Hardware Security for IoT)
- Cryptography after Quantum Computing (CS 674 – Post Quantum Cryptography)
- Privacy and Cryptography (CS 670 – Crypto techniques for privacy preservation)

So I have already described this. I'll not dwell on this slide, but what to not expect from this class. So I said, if you want to know basic hacking, you have to take 628. If you want to know how to analyze malware, you have to take 658 or do intrusion detection. How to protect critical infrastructure, that would be 631.

How to analyze cryptographic protocols and algorithms, 641. how to check for a side channel in cryptography implementation, that will be 666. 674 is post-quantum cryptography, and a recent new course, privacy and cryptography, 670. So do not expect to learn any of these things in this class, right? So if you want this, to learn these things, then you go to those classes. Now what I want, I have about, I think 13 minutes or so.

NOTE: RESPONSES GIVEN BELOW ARE THE STUDENTS FROM IIT KANPUR WHO ENROLLED FOR THE COURSE. DON'T TAKE THE RESPONSES IN THE COMING SLIDES AS CORRECT. READ THE NOTES BELOW THE FIGURES TO GET BETTER UNDERSTANDING OF THE RESPONSES

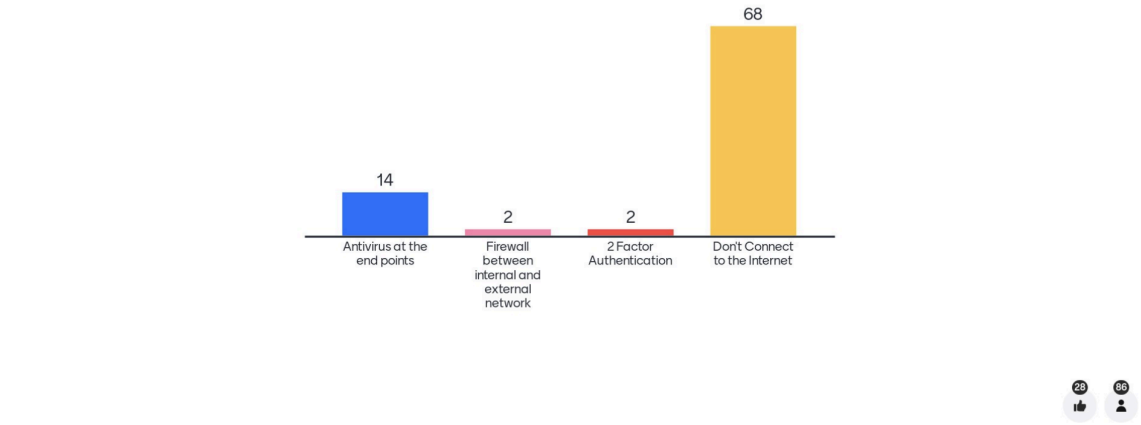
So I want to play a game. So in this one, what you think is the most critical and then which is the second most critical and which is the least critical.



Okay, so rightly so, the exfiltration of confidential data from the organization obviously is the biggest problem among these three because we have the new Digital Data Protection Act. by the government which got passed in the parliament last year and it may actually lead to 250 crores fine on an organization if they lose customer data, confidential privacy, private data about customers, the personally identifiable information. The reason why ransomware encryption is second is because it depends whether you have backups or not. See, data exfiltration, once it is out and it is being sold on the dark web, you have no control, right? So that's why nowadays ransomware attacks also come with data exfiltration.

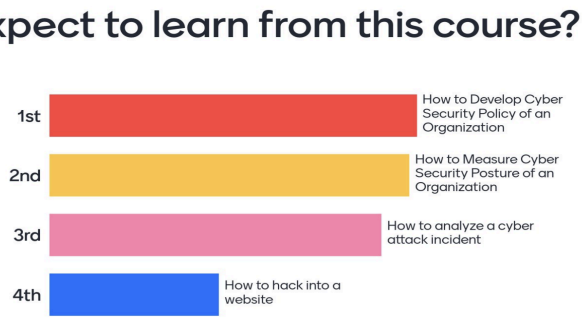
They do both. But as such, data exfiltration, the organization is in big, big trouble. Ransomware attacks, if it is just encryption, they probably have the backup to recover from, so they might actually be in a slightly better position. And then compromising a device with malware is bad, but it depends whether the device can be quickly isolated or shut down and things like that. So there are ways you have some control to respond to that incident. But if you get data exfiltrated, then you are at the mercy of the ones who have the control on the data.

Okay, so which of the following is not a cyber defense tactic? Antivirus at the endpoints, endpoints means the devices, and then firewall between internal and external network, second two-factor authentication, and don't connect to the internet.



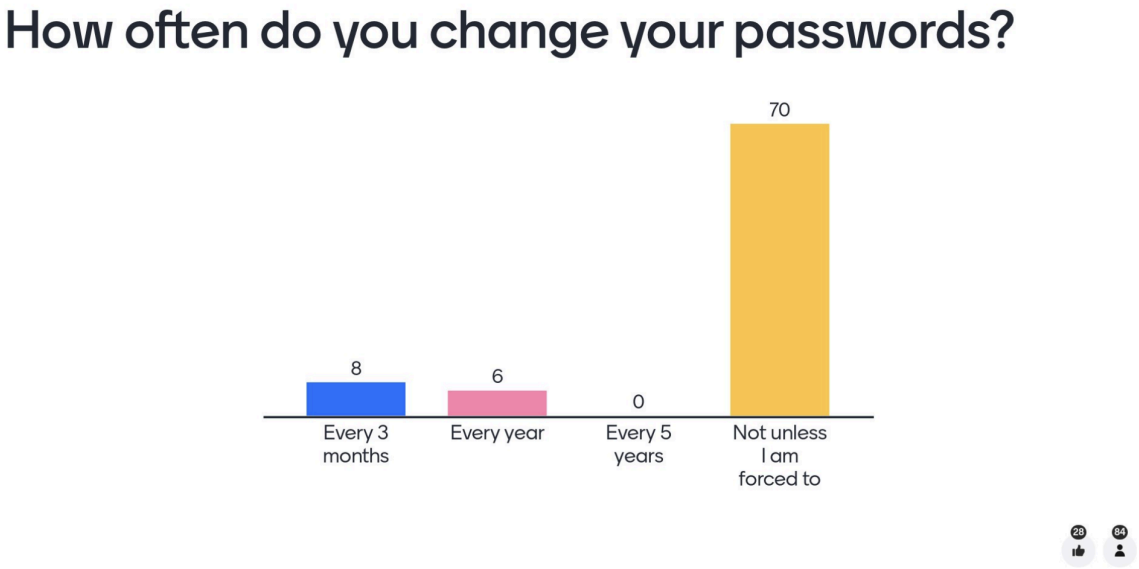
Yeah, so not connecting to the internet is not a choice anymore, right? So you cannot say that I will not connect to the internet, so I am fine. You can still get attacked, right? So the Iranian nuclear enrichment plant was not connected to the internet. So the attackers basically gave free USB to the engineers who took that USB and connected to the machines in the internal network which was not connected to the internet and still got attacked. Okay, so let's see what's, okay, here again you have to rank them by pushing with your finger.

What do you want to learn from this course? Okay, so far so good. So the top three things are what we learned. The last thing we'll not learn in this course. So good that you don't want to learn from this course because you won't learn. Okay, now something about you. How often do you change your password? Every three months? Every year? Every five years? And I'm talking about the passwords of important accounts, like not some random accounts, like your social media account or Google account or your net banking account or your CC account and so on.



So at least eight of you actually are pretty conscientious. You change your password every three months. So you have to use a password vault program application to remember your password because if you change that frequently, you won't remember your passwords, right? I think that what is concerning is that 69 of you don't change your password unless forced to, right? So that's not good. So we have to do something about that. And Soumitri here from CC, he will make you, force you to change password more often, right? I use the same password in net banking and social media.

Oh my God. We have 23 of you who are using the same password in social media and net banking. That's pretty scary. You need to think about it. So let's go and see. How many of you use antivirus on your devices? And by devices, I mean your laptop or your mobile.



This is also pretty scary. Neither laptop or mobile, 40, like half, 50% of the students. Okay. Okay, that's pretty scary. We'll have to convince you better. I update and patch my OS and applications.

Automatic updates are pretty common, I see. Now there are 10 who have no idea. That could be pretty scary also.