

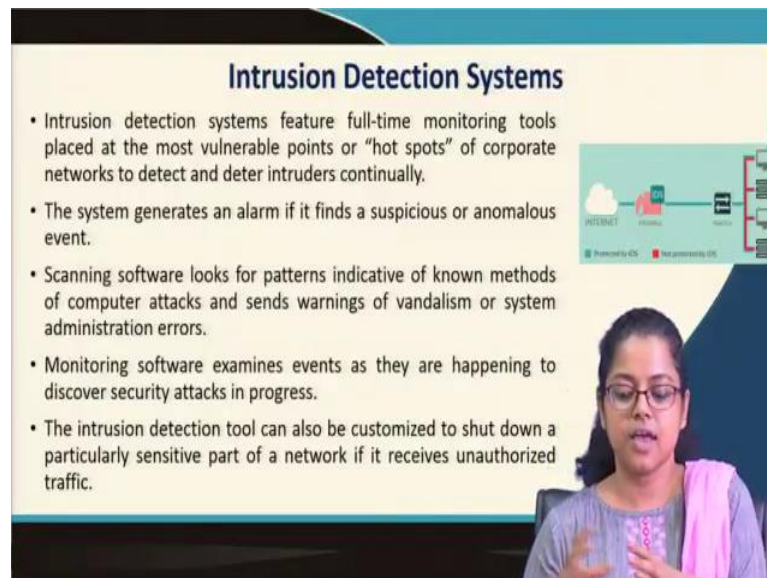
Management Information System
Prof. Saini Das
Vinod Gupta School of Management
Indian Institute of Technology, Kharagpur

Module – 11
Ethical, Social and Security Issues in MIS
Lecture – 55
Security Issues in MIS – III

Hello and welcome back to this lecture on 'Ethical, Social and Security Issues in MIS'! So, we are in the 3rd lecture wherein we are going to discuss about Security Issues in MIS. Of course, this is the last lecture in this particular module but with respect to security issues, this is the 3rd lecture. So, in the previous lecture, we had spoken about different categories of security threats in organizations and we had also discussed about some countermeasures, in terms of technical countermeasures, to these security breaches.

So, today, we will move ahead with the other some other technical countermeasures and then, we will be discussing more of organizational and legal measures which can be used to defend organizations against security breaches.

(Refer Slide Time: 01:10)



Intrusion Detection Systems

- Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable points or "hot spots" of corporate networks to detect and deter intruders continually.
- The system generates an alarm if it finds a suspicious or anomalous event.
- Scanning software looks for patterns indicative of known methods of computer attacks and sends warnings of vandalism or system administration errors.
- Monitoring software examines events as they are happening to discover security attacks in progress.
- The intrusion detection tool can also be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

The slide includes a network diagram showing a cloud labeled 'INTERNET' connected to a server labeled 'Firewall', which is connected to a server labeled 'Intrusion Detection System'. Below the diagram, there are two small icons: a green one labeled 'Promoted to IDS' and a red one labeled 'Not promoted to IDS'. A woman is visible in the bottom right corner of the slide, speaking.

So, the next information security technological countermeasure pertains to intrusion detection systems. So, intrusion detection systems are often coupled with firewalls, wherein they are used to monitor and scan intrusions in networks. Intrusion detection

systems feature full-time monitoring tools placed at the most vulnerable points or hot spots of corporate networks to detect and deter intruders continuously.

So, they do not work you know for a certain period of time and then they stop. They constantly monitor and keep on deterring. So, the system generates an alarm if it finds a suspicious or an anomalous event. Scanning software looks for patterns indicative of known methods of computer attacks and sends warnings of vandalism or system administration errors.

And, the next is the monitoring software. So, monitoring software examines events as they are progressing to discover security attacks in the progress. And, once you know if any malicious attack or a security breach is detected, this the intrusion detection tool can be customized to shut down a particularly sensitive part of a network if it receives unauthorized traffic.

So, for example, you know if your organization has a very critical or a sensitive part of the network and if malicious you know attack is detected by the intrusion detection system, the IDS can automatically switch off that particular part sensitive part of the network so that part of the network is actually protected from the cyber breach. So, this is the role of the intrusion detection system.

Now, moving on, antivirus and antispymware software. So, I am sure even if you have not heard of the other technological measures, all of you must be having an antivirus in your computers. So, an antivirus software is designed to check computer systems and drives for the presence of computer viruses, obviously. So, often the software eliminates the virus from the infected area it itself.

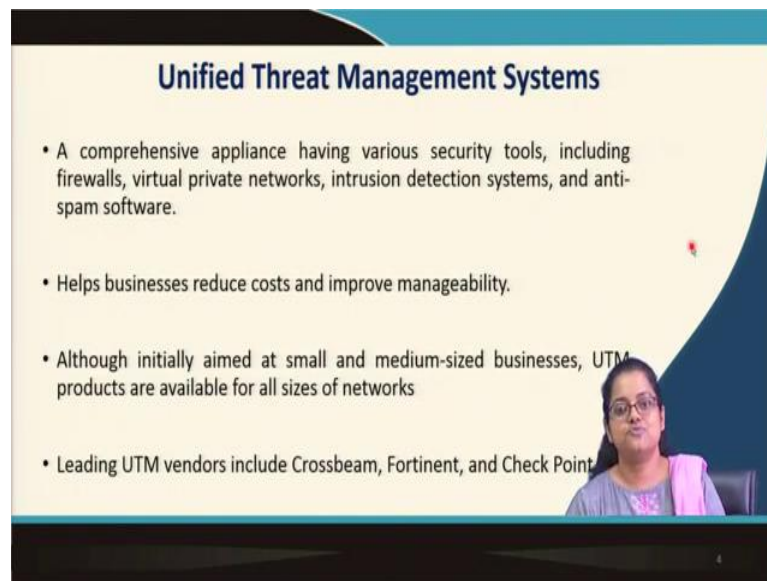
However, most antivirus software is effective only against viruses already known when the software was written. Again as in the case of phishing anti-phishing filters, anti-viruses are also created you know in through trial and error over a period of time based on past data. So, anti-viruses would also be able to protect against old virus, but if there is a virus that is unknown and unique and absolutely new, antiviruses might actually fail.

So, in order to remain effective antivirus software must be continuously updated. Therefore, it is very important to have dynamic anti-viruses which are constantly updated with new viruses that keep coming. Now, leading antivirus software such as MacAfee,

we have Trend Micro, we have Norton, we have Symantec. So, these popular antivirus software also come up also have enhanced their products to include protection against spyware.

So, antivirus software also you know have recent in recent times they have also come up with antispyware software, right.

(Refer Slide Time: 04:52)



Unified Threat Management Systems

- A comprehensive appliance having various security tools, including firewalls, virtual private networks, intrusion detection systems, and anti-spam software.
- Helps businesses reduce costs and improve manageability.
- Although initially aimed at small and medium-sized businesses, UTM products are available for all sizes of networks
- Leading UTM vendors include Crossbeam, Fortinet, and Check Point

The slide features a light yellow background with a dark blue curved border on the right side. A small red cursor is visible on the slide. In the bottom right corner, there is a video inset showing a woman with glasses and a pink top speaking.

So, moving on, unified threat management system this is another very very interesting you know network defense you know security tool you can say or a management system you can say. This is a comprehensive appliance having various security tools in amalgamation. So, you may not have a separate firewall a separate VPN or separate intrusion detection system, but you can have all of them together.

So, it gives you a more holistic and comprehensive security counter measure in your organization. So, you can have only one system that will have all of these together in one place. Now, it is beneficial in two ways. Firstly, it improves manageability because instead of having all of these in isolation, maintenance might be very difficult – all of them are amalgamated into one product.

So, maintenance becomes much easier and at the same time cost is also reduced. So, although initially these were UTM systems were targeted at small MSMEs or small and medium sized businesses, over time they were available for all sorts of networks. So,

everybody all organizations understood the benefits of UTM's and tried to engage UTM's into their systems. Now, leading UTM vendors include Crossbeam, Fortinet and Check Point. Check Point is a very popular UTM vendor right.

(Refer Slide Time: 06:26)



So, we have discussed quite a few security technologies in these two lectures and we have seen how technology can be used as the first layer of defense against information security breaches. But, if we have to move on to the next layer of course, we have to focus on organizational policies and procedures.

(Refer Slide Time: 06:51)

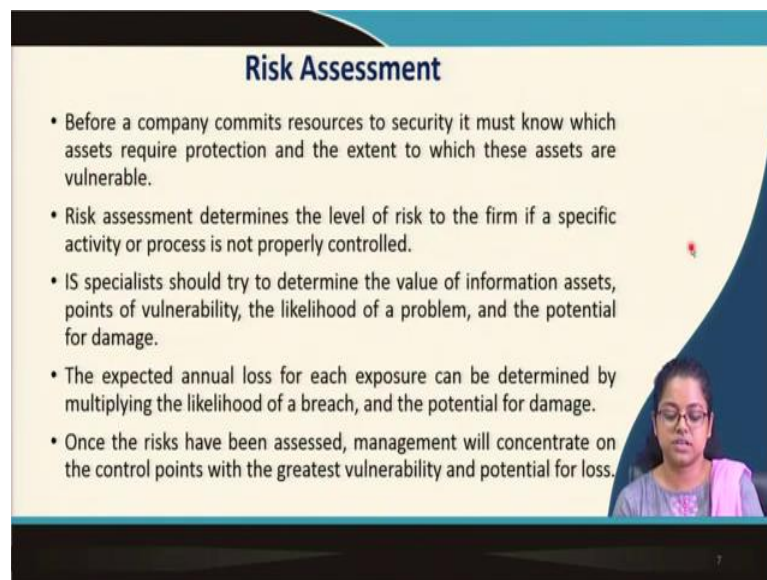


So, let us see what these are; so, organization security plan, very-very important. In order to protect organizations against security breaches technological measures are always not sufficient, they are not enough because they are necessary, but they not they may not be a sufficient condition because if even you know despite having n number of security technologies if there is a small loop hole the perpetrator or the hacker can easily find that out and can exploit it.

That is why it is said that any you know information system is as secure as the security of the weakest link. So, if there is even one weak link it can be exploited by a hacker and that can wreak havoc in the entire system. So, it is very important to have a comprehensive organizational approach to see to manage the security. So, with respect to a security plan there are 5 steps.

Firstly, perform a risk management develop a security policy develop an implementation plan, create a security organization and finally, perform a security audit. So, all of these are very critical and let us see what these are.

(Refer Slide Time: 08:13)



Risk Assessment

- Before a company commits resources to security it must know which assets require protection and the extent to which these assets are vulnerable.
- Risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled.
- IS specialists should try to determine the value of information assets, points of vulnerability, the likelihood of a problem, and the potential for damage.
- The expected annual loss for each exposure can be determined by multiplying the likelihood of a breach, and the potential for damage.
- Once the risks have been assessed, management will concentrate on the control points with the greatest vulnerability and potential for loss.

Risk assessment; that is the first step. So, before a company commits resources to security, it must know which assets require protection and the extent to which these assets are vulnerable; right.

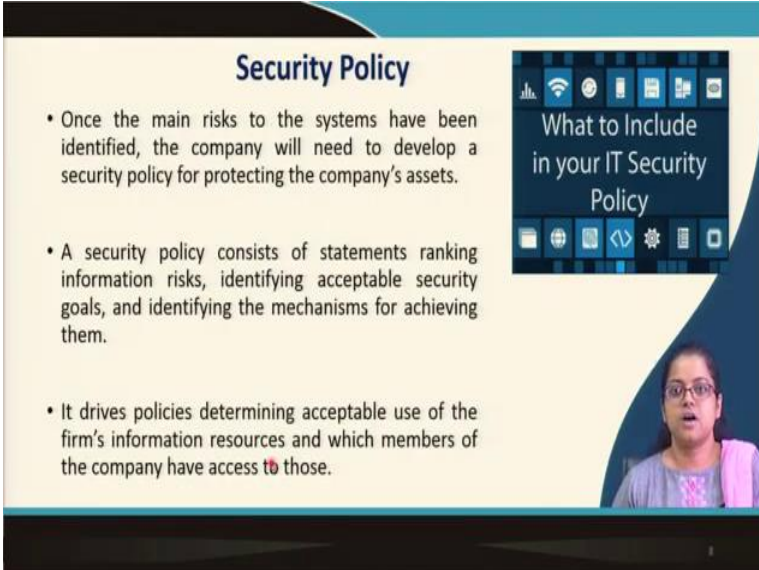
So, you need to identify those assets which are vulnerable and those that require protection. Risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Now, information security specialist should try to determine the value of information assets, points of vulnerability, the likelihood of a problem and the potential of damage. It is not very easy to identify any of these.

However, specialists, information system specialists should be aware of all of these and they should because they are experts in this particular job. So, they should be able to find out the value of each of them though it is difficult the. The expected annual loss for each exposure can then be determined by multiplying the likelihood of a problem by the potential for damage. So, in this case likelihood of a breach by the potential for damage, but these are all based on the perceptions of the information system specialist.

Risk assessment is of course, you know always based on the perception of a team of people or you know specialist you cannot exactly point out the risk, but you can always calculate an expected risk. Once the risks have been assessed management will concentrate on the control points with the greatest vulnerability and potential for loss.

So, once potential for loss is found out and you know the vulnerabilities of each of the information assets, the management will have to concentrate on those assets which have the greatest vulnerability and the highest potential for loss.

(Refer Slide Time: 10:22)



Security Policy

- Once the main risks to the systems have been identified, the company will need to develop a security policy for protecting the company's assets.
- A security policy consists of statements ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving them.
- It drives policies determining acceptable use of the firm's information resources and which members of the company have access to those.

What to Include in your IT Security Policy

The slide features a video inset in the bottom right corner showing a woman with glasses speaking. The background of the slide is light blue with a dark blue header and footer. The text is in a dark blue font.

Now, coming to the next step, it is now very important to come up with a security policy. So, once the main risks to the system have been identified, the company will need to develop a security policy for protecting the company's assets. So, here you see several assets have been identified. So, you have to put in rules or policy measures pertaining to those very critical vulnerable assets.

So, for example, here is a wireless technology, we can see hard drives, we can see biometric system. So, we can see multiple you know information assets within organizations and the security policy will actually talk about how these information assets should be you know what is the acceptable level of security risk and how those risks can be handled.

So, a security policy consists of statements ranking information risks, identifying acceptable security goals and identifying the mechanisms for achieving those goals or in brief it drives policies for determining the acceptable use of the firm's information resources and which members of the company have access to those. So, you identify which are what is what are the acceptable uses of these vulnerable information resources within your organizations and which members of your company have access to those resources. So, this is what is mentioned.

For example, it in your if you identify your e-mail server as extremely vulnerable point in your information system and also if you identify that there is a huge potential for loss if the email server is breached, then you can say that you can actually say or you can actually craft in your security policy who are the members of your company who would have access to that particular e-mail server.

You can also set up some password related policies to protect the user IDs of people of members of your organization using the e-mail server and to prevent them from getting hacked, right. So, this is what the security policy of an organization looks like.

(Refer Slide Time: 12:43)

DRP/BCP

- Disaster recovery plan (DRP) devises strategies for the restoration of computing and communications services after they have been disrupted.
- DRP focuses primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services.
- Business continuity plan (BCP) focuses on how the company can restore business operations after a disaster strikes.
- The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.

BCP

- Business Management Procedures
- Business Continuity Strategy
- Risk Assessment

DRP

- Emergency Management Procedures

Next we come to very important part of information security organization that is the disaster recovery plan or the business continuity plan. So, these 2 plans are extremely important and as the name suggests disaster recovery plans have to do with emergency response to a security breach or a which is a disaster and business continuity plan have play a very important role in ensuring that the business continues despite the disruption.

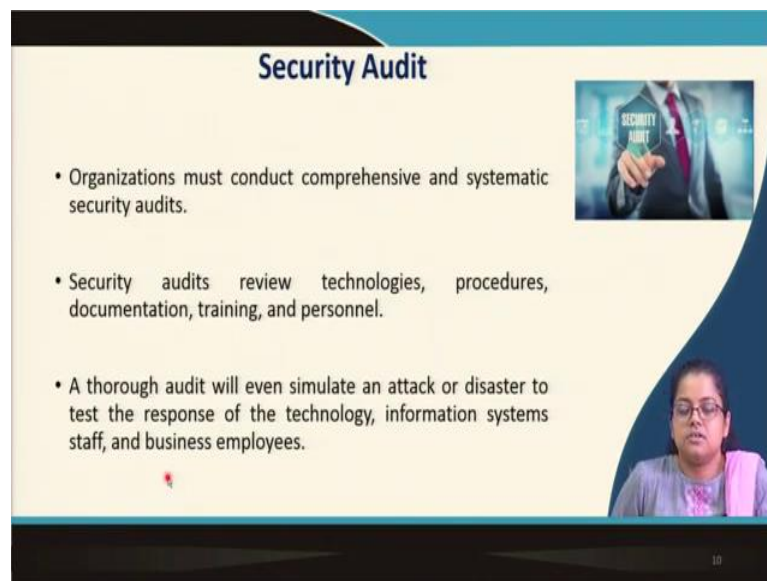
So, disaster recovery plan both of these plans let me mention at the very beginning it itself have to be in place if you have to have a information security environment, a strong information security environment within your organization. These two plans are a must. So, a DRP devices strategies for restoration of computing and communication services after they have been disrupted so, all the emergency procedures.

DRP focuses primarily on technical issues involved in keeping systems up and running, such as which files to backup and the maintenance of backup computer systems or disaster recovery systems. So, again to reiterate DRP has to do with you know very with has to do with emergency responses to the disruption.

On the other hand, business continuity plan or BCP focuses on how the company can restore business operations after a disaster strikes or in other words the BCP identifies critical business processes and determines action plans for handling mission critical functions if systems go down.

So, if systems go down due to a security breach there are certain mission critical functions without which the system will not be able to continue it is business. So, in order to ensure that those mission critical functions are you know up and running despite the entire system going down because of the disruption in this context the security breach, the BCP plan needs to be crafted in advance and it needs to be followed during the disruption.

(Refer Slide Time: 15:06)



Security Audit

- Organizations must conduct comprehensive and systematic security audits.
- Security audits review technologies, procedures, documentation, training, and personnel.
- A thorough audit will even simulate an attack or disaster to test the response of the technology, information systems staff, and business employees.

So, now moving on the final step in creating this organizational security environment has to do with security audit, very-very critical. So, no matter how much you know you might have invested a lot in technology and you might have kept a lot of plans and procedures in place, but you have to perform some of these mock security audits or drills to ensure that everything works you know as per the plan in case disaster strikes all of a sudden.

So, organizations must conduct comprehensive and systematic security audits. Security audits review technologies, procedures, documentation, training, and personnel. A thorough audit will even simulate an attack or disaster to test the response of the technology information system staff, and business employees.

So, very important if there is a thorough audit, the thorough audit will actually simulate a cyber security breach or an information security breach to see how the technology or the information system staff, technology personal and business employees, how all of them

react at the time of the crisis or the breach. So, this is what a security breach is and audit is.

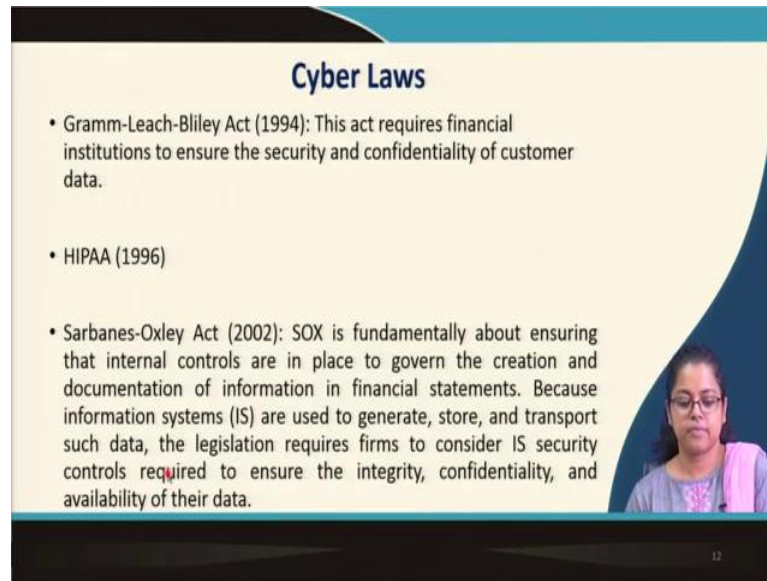
And in case you know the security audit reports that some of the, you know, there are certain problems; those problems would be reported to the management so that the management can take appropriate action in order to fix them before the actual disaster strikes; alright.

(Refer Slide Time: 16:48)



So, these are some of the you know organization policies and procedures that we wanted to focus on in case of a security breach. Now, coming to the third and final layer of defense against information security breaches. Now, we will talk about legal and regulatory requirements.

(Refer Slide Time: 17:13)



Cyber Laws

- Gramm-Leach-Bliley Act (1994): This act requires financial institutions to ensure the security and confidentiality of customer data.
- HIPAA (1996)
- Sarbanes-Oxley Act (2002): SOX is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements. Because information systems (IS) are used to generate, store, and transport such data, the legislation requires firms to consider IS security controls required to ensure the integrity, confidentiality, and availability of their data.

Cyber laws. So, there are some cyber laws: most of them are drafted in the context of the United States, but some of them are very relevant in other geographies as well. So, we begin with Gramm-Leach-Bliley Act which was drafted in 1994. This act requires financial institutions to ensure the security and confidentiality of customer data. So, GLB Act pertains to the financial; to the financial services industry financial institutions, so that they ensure the security and confidentiality of customer data.

The next law pertains to HIPAA. HIPAA we had discussed thoroughly when we had spoken about privacy laws, we were talking about privacy laws. So, HIPAA is was drafted in 1996 and it talks about the Health Insurance Portability and Accountability Act. And, it says how you know whenever there is a patient how the electronic medical records of the patients should be shared among the different entities in the health care value chain, but at the same time it should be ensured that his privacy is maintained.

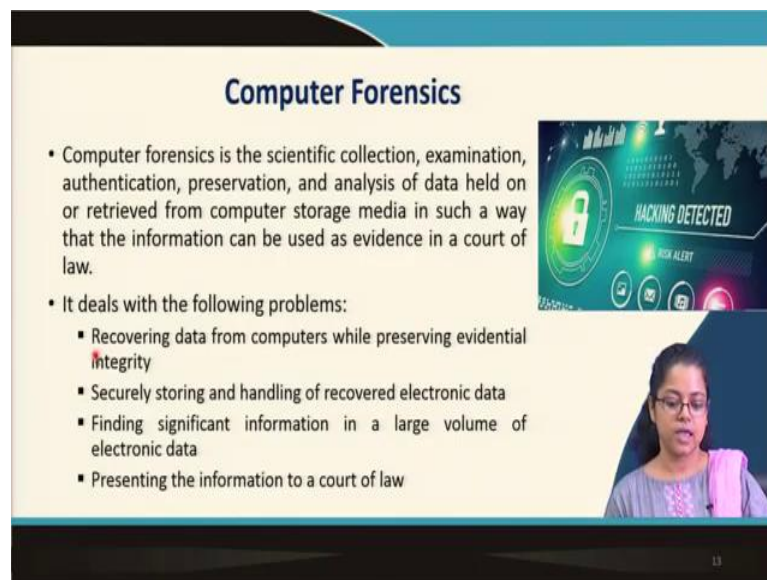
So, there should be a balance between the quality of health care that the customer that the patient receives and the privacy of his or her confidential electronic medical records. The next law is the SOX; so, the Sarbanes-Oxley Act in 2002. SOX is fundamentally about ensuring that internal controls are in place to govern the creation and documentation of information in financial statements. Again, SOX pertains to the financial institutions.

So, because information systems are used to generate, store and transport such data, the legislation requires firms to consider information system security controls required to

ensure the integrity confidentiality availability or CIA of their data. So, here again it is mentioned that in order to you know protect financial institutions from security breaches SOX act plays a very important role here.

This goes without saying that different other geographies around the world all of them have some or the other law with respect to cyber security, but these are some of the most prominent laws across the world. Of course, drafted in the United States, but other countries, other nations, other geographies do have their own laws with respect to protecting customer information in case of security breaches.

(Refer Slide Time: 20:13)



Computer Forensics

- Computer forensics is the scientific collection, examination, authentication, preservation, and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law.
- It deals with the following problems:
 - Recovering data from computers while preserving evidential integrity
 - Securely storing and handling of recovered electronic data
 - Finding significant information in a large volume of electronic data
 - Presenting the information to a court of law

The slide features a graphic on the right with a padlock icon, a world map, and the text 'HACKING DETECTED' and 'RISK ALERT'. A video inset in the bottom right corner shows a woman with glasses speaking.

Now, moving on, computer forensics. So, very important, forensics the name it itself the term it itself suggests that you know post any incident you try to dig into the problem and see what has happened and try to find out what had happened. So, forensics play a very important role in case of murders or crimes. You go to the crime scene or the murder spot and you try to figure out what happened.

So, if you were to draw an analogy with computer systems, we do have computer forensics. Computer forensics is the scientific collection; examination, authentication, preservation and analysis of data held on or retrieved from computer storage media in such a way that the information can be used as evidence in a court of law.

So, here you collect information from computer storage media after a breach has been after there has been a breach or a hacking to find out what exactly happened, so that this can be actually served as an evidence in a court of law.

Forensics computer forensics deals with the following problems recovering data from computers while preserving evidential integrity, very important. Securely storing and handling of recovered electronic data. Finding significant information in large volume of electronic data is very-very critical because if you have a huge volume of data and computer systems do generate huge volumes of data. So, finding significant information there might be very challenging.

And, finally presenting the information in a court of law; so, you collect the data through forensics which is actually post an event, post a cyber breach you collect data through forensics in order to be able to present it as an evidence in a court of law. So, you have to be when you collect the data you have to be very specific that all the details are carefully preserved and maintained, so that they are in a suitable condition to be in an appropriate condition to be presented in a court of law.

So, this is of course, you know if you consider prevention, detection and recovery measures computer forensics is a recovery measure; whereas, prevention you may have firewall, you may have the network security solutions as preventive measures and as detective measures you can have intrusion detection, intrusion prevention systems.

And, recovery measures you can have a computer forensics, you can have a different laws, you can have certain organizational policies and procedures that we have discussed which could be recovery as well as preventive measures also or detective measures.

So, what how you can handle a crisis or how you can handle disruption by using the BCP plan, the disaster recovery plan. So, all of those lie in the, you know, detection zone; so, prevention zone, detection zone and of course, recovery zone or during an information security breach; fine.

(Refer Slide Time: 23:32)



Organizations that Promote Computer Security

- **CERT**
 - Responds to thousands of security incidents each year
 - Helps Internet users and companies become more knowledgeable about security risks
 - Posts alerts to inform the Internet community about security events
- **Microsoft Security Research Group**
 - Privately sponsored site that offers free information about computer security issues

So, let us move on and spend some time on organizations that promote computer security. So, we do have certain organizations that promote computer security across the world. These organizations you know they are a repository which wherein information about different security breaches that are happening across the world are stored and preserved, and of course, they also disseminate a lot of information, a lot of best practices, good procedures with respect to protecting organizations against security breaches.

So, the first one that we want to discuss is CERT. CERT stands for Computer Emergency Response and Training. So, CERT responds to thousands of security incidents each year. It helps internet users and companies become more knowledgeable about security breaches. So, if there are certain security breaches for example, in 2017 ransom ware breaches became the talk of the town.

So, these organizations would actually contain details about ransom ware breaches and how organizations could defend themselves against these breaches, how they could prepare themselves a priori, how they could what legal actions they could take in case you know they were victims of for ransom ware breach. So, all such details were available in such platforms at the same time they also post alerts to inform the internet community about security events.

So, in so, they not only you know talk about security breaches that are happening around the world, they would talk about counter measures to those and they would have a they are a repository of all the cyber breaches that happen around the world. So, CERT is one very popular example. Another example is Microsoft Security Research Group which private it is a privately sponsored site that offers free information about computer security issues which is again very similar to what CERT does.

Similarly, there are several other bodies there is some there is another body called the SANS Institute which again provides similar information about security breaches around the world. So, to summarize these organizations promote computer security across the world and they are very useful for protecting in organizations against the losses that they might incur due to security breaches.

So, with this we come to the end of this particular session and I would like to quickly you know spend some time summarizing what we had discussed in this module. So, initially we had spoken about ethical and social issues. So, we had discussed about privacy which is a very critical issue today in the digital world and we had spoken about the counter measures to privacy in terms of technological countermeasures and legal counter measures.

Then we had discussed about copyright infringement which is another very important problem in the digital world. And, we had also tried to understand how organizations could protect themselves against these problems. Finally, we had also discussed about workplace monitoring and how the information panoptic can plays a very important role in digital monitoring in workplaces.

Then, we had then we moved on to security issues and we had discussed about the pillars of information security and how organizations could undergo you know financial losses due to security breaches. Then, we moved on to technological counter measures to prior to that we had spoken about different categories of security breaches ranging from phishing attacks to man in the middle attack to denial of service attacks and so on.

And, then we had spent time on technology solutions or counter measures to these security breaches. Post which we had we have spent some time on organizational procedures and policies against security breaches and finally, we wrapped up with legal countermeasures to security breaches. So, overall this session spoke about various

challenges that information systems face. Of course, you know as information system evolves newer and more unique challenges keep coming up.

So, they would require attention in future but as of now these are some of the challenges very critical, you know. challenges that information system faces in today's world.

Thank you!