IT INFRASTRUCTURE MANAGEMENT

UNIT-4

1. What are the ethics of computer security?

In computer security, cyber-ethics is what separates security personnel from the hackers. It's **the knowledge of right and wrong, and the ability to adhere to ethical principles while on the job**.

What is Computer Security and its types?

One way to ascertain the similarities and differences among Computer Security is by asking what is being secured. For example,

- *Information security* is securing information from unauthorized access, modification & deletion
- *Application Security* is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- C*omputer Security* means securing a standalone machine by keeping it updated and patched
- *Network Security* is by securing both the software and hardware technologies
- *Cybersecurity* is defined as protecting computer systems, which communicate over the computer networks

It’s important to understand the distinction between these words, though there isn’t necessarily a clear consensus on the meanings and the degree to which they overlap or are interchangeable.

So, **Computer security** can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. Let’s elaborate the definition.

Components of computer system

The components of a computer system that needs to be protected are:

- *Hardware,* the physical part of the computer, like the system memory and disk drive
- *Firmware,* permanent software that is etched into a hardware device's nonvolatile memory and is mostly invisible to the user
- *Software,* the programming that offers services, like operating system, word processor, internet browser to the user

Computer Security Practices

Computer security threats are becoming relentlessly inventive these days. There is much need for one to arm oneself with information and resources to safeguard against these complex and growing computer security threats and stay safe online. Some preventive steps you can take include:

- Secure your computer physically by:
    - Installing reliable, reputable security and anti-virus software
    - Activating your firewall, because a firewall acts as a security guard between the internet and your local area network
- Stay up-to-date on the latest software and news surrounding your devices and perform software updates as soon as they become available
- Avoid clicking on email attachments unless you know the source
- Change passwords regularly, using a unique combination of numbers, letters and case types
- Use the internet with caution and ignore pop-ups, drive-by downloads while surfing
- Taking the time to research the basic aspects of computer security and educate yourself on evolving cyber-threats
- Perform daily full system scans and create a periodic system backup schedule to ensure your data is retrievable should something happen to your computer.

Apart from these, there are many ways you can protect your computer system. Aspects such as encryption and computer cleaners can assist in protecting your computers and its files.

Unfortunately, the number of cyber threats are increasing at a rapid pace and more sophisticated attacks are emerging. So, having a good foundation in cybersecurity concepts will allow you to protect your computer against ever-evolving cyber threats.

2. Internet security

Internet security is a term that describes **security for activities and transactions made over the internet**. It's a particular component of the larger ideas of cybersecurity and computer security, involving topics including browser security, online behavior and network security.

Internet Protocol Security (IPsec)

IPsec is designed to protect TCP/IP communication in a secure manner. It is a set of security extensions developed by the Internet Engineering Task Force (IETF). It provides security and authentication at the IP layer by transforming data using encryption. Two main types of transformation form the basis of IPsec: the Authentication Header (AH) and ESP. They provide data integrity, data origin authentication, and anti-replay services. These protocols can be used alone or in combination.

Basic components include:

- Security protocols for AH and ESP
- Security association for policy management and traffic processing
- Manual and automatic key management for the Internet key exchange (IKE)
- Algorithms for authentication and encryption

The algorithm allows these sets to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

3.physical security

What is physical security and how does it work?

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events.

The physical security framework is made up of three main components: access control, surveillance and testing. The success of an organization's physical security program can often be attributed to how well each of these components is implemented, improved and maintained.

Access control

The key to maximizing one's physical security measures is to limit and control what people have access to sites, facilities and materials. Access control encompasses the measures taken to limit exposure of certain assets to authorized personnel only. Examples of these corporate barriers often include ID badges, keypads and security guards. However, these obstacles can vary greatly in terms of method, approach and cost.

The building is often the first line of defense for most physical security systems. Items such as fences, gates, walls and doors all act as physical deterrents to criminal entry. Additional locks, barbed wire, visible security measures and signs all reduce the number of casual attempts carried out by cybercriminals.

More sophisticated access controls involve a technology-supported approach. ID card scanners and near-field communication (NFC) ID cards are methods of physical authentication that security teams can use to verify the identities of individuals entering and exiting various facilities. Some Swedish companies have recently experimented with embedding NFC microchips below the skin of their employees -- making it extremely difficult to forge or replicate their credentials. Invasive devices like this, however, are much less popular among labor unions, given the degree of physical pain and bodily concern.

Using tactically placed obstacles, organizations can make it more difficult for attackers to access valuable assets and information. Similarly, these barriers increase the time it takes for threat actors to successfully carry out acts of thievery, vandalism or terrorism. The more obstacles that are in place, the more time organizations have to respond to physical security threats and contain them.

But criminals are not the only threat that access controls can minimize. Barriers such as walls and fences can also be used to harden buildings against environmental disasters, such as earthquakes, mudslides and floods. These risks are extremely location-dependent. Organizations that divert resources toward such hardening measures should balance the cost and benefit of their implementation prior to investment.

Surveillance

This is one of the most important physical security components for both prevention and post-incident recovery. Surveillance, in this case, refers to the technology, personnel and resources that organizations use to monitor the activity of different real-world locations and facilities. These examples can include patrol guards, heat sensors and notification systems.

The most common type of surveillance is closed circuit television (CCTV) cameras that record the activity of a combination of areas. The benefit of these surveillance cameras is that they are as valuable in capturing criminal behavior as they are in preventing it. Threat actors who see a CCTV camera are less inclined to break in or vandalize a building out of fear of having their identity recorded. Similarly, if a particular asset or piece of equipment is stolen, surveillance can provide the visual evidence one needs to identify the culprit and their tactics.

Testing

Physical security is a preventative measure and incident response tool. Disaster recovery (DR) plans, for example, center on the quality of one's physical security protocols -- how well a company identifies, responds to and contains a threat. The only way to ensure that such DR policies and procedures will be effective when the time comes is to implement active testing.

Testing is increasingly important, especially when it comes to the unity of an organization. Fire drills are a necessary activity for schools and buildings because they help to coordinate large groups, as well as their method of response. These policy tests should be conducted on a regular basis to practice role assignments and responsibilities and minimize the likelihood of mistakes.

Importance of physical security

As businesses become more dependent on the internet of things (IoT), so does the need for digital and physical security. IoT demands a significant amount of physical security to safeguard data, servers and networks. The rising interconnectedness of IoT has expanded the sphere of physical security. Virtual machines (VMs) and applications that run in the cloud, for example, are only as protected as their physical servers.

Whether organizations invest in first-party or third-party cloud computing services, these data centers need to be sufficiently protected using physical security measures to avoid severe data losses.

Physical security examples

Physical security can take many shapes and forms. The strategies, barriers and techniques that organizations use to support general physical information technology (IT) security, for example, are significantly different from those used to facilitate consistent physical network security. Here are a few physical security examples used to contain and control real-world threats.

4. Identity management

What is Identity Management?

Identity management (IdM), also known as identity and access management (IAM) ensures that authorized people – and only authorized people – have access to the technology resources they need to perform their job functions. It includes polices and technologies that encompass an organization-wide process to properly identify, authenticate, and authorize people, groups of people, or software applications through attributes including user access rights and restrictions based on their identities.

An identity management system prevents unauthorized access to systems and resources, helps prevent exfiltration of enterprise or protected data, and raises alerts and alarms when access attempts are made by unauthorized personnel or programs, whether from inside or outside the enterprise perimeter.

Identity management solutions not only protect software and data access, they also protect the hardware resources in an enterprise, such as servers, networks, and storage devices from unauthorized access which could lead to a ransomware attack. Identity management has gained importance over the past decade due to the growing number of global regulatory, compliance, and governance mandates that seek to protect sensitive data from exposure of any kind.

IdM and IAM systems generally are part of IT security and IT Data management within the enterprise, and identity and access management tools are widely available for the broad range of devices that users rely on to perform business functions from phones and tablets to desktop computers running Windows, Linux, iOS or Android.

IdM and IAM are terms often used interchangeably, however identity management is more focused on a user identity (or username), and the roles, permissions, and groups that user belongs to. IdM also focuses on protecting identities through a variety of technologies such as passwords, biometrics, multi-factor authentication, and other digital identities. This is usually achieved by the adoption of identity management software applications and platforms.

The difference between Identity and Access Management

The difference between identity management and access management can be simplified like this:

IDENTITY management is all about managing the attributes related to the USER, group of users, or other identity that may require access from time to time.

ACCESS management is all about evaluating those attributes based on existing policies and making a yes or no access decision based upon those attributes.

Why do we need identity management?

A recent **(ISC)²** study found that 80% of breaches were due to identity access issues, namely weak or mismanaged credentials. If proper controls are not in place – or procedures and processes for IAM not properly followed, passwords could become compromised, phishing attacks enabled, and breaches or ransomware attacks become a reality. Fortunately, modern IAM platforms offer automation of many of the functions to help ensure controls are utilized, such as removing a user from the directory when the HR system indicated an employee has left the organization.

Since new privacy and data secrecy legislation is so frequently created, IAM can play another important role, that of helping the organization stay in compliance with the myriad of regulatory and governance mandates in effect, ensuringthat only authorized users have access to data, but that the data itself is where it should be. In the end, IT security is largely about access, so a solid IAM strategy is a critical component of overall IT security and offers a first line of protection to any threat, whether from outside or inside the firewall.

What are the business benefits of identity management?

The ability to successfully protect assets – including digital assets – can have a direct bottom-line impact on the value of the organization. IAM accelerates the time to value for anyone who needs access to enterprise resources to perform their job, often speeding the time between onboarding a new employee until when they have access to system resources from days to minutes.

Besides providing an enhanced business value as a result of improved security, there are other tangible business benefits. Automation of IAM tasks frees up IT for bottom-line focused projects, and self-service identity management tools improve the overall productivity of employees, contractors, and other users who access corporate resources.

Implementing an overall IAM framework can provide opportunities for growth, by improving scalability of those services critical to onboarding new users, and that reduction of IT manpower translates to a better ROI for the IT organization as a whole.

Identity and access management has become the foundation for all of these business benefits and continues to protect the enterprise from threats that could lead to data theft, malicious attacks, or exposing sensitive customer, patient, or legal information.

5.Acess control system

Access control systems are the electronic systems that are designed to control through a network and they should have an access to a network. Access Control System recognizes authenticates and authorizes entry of a person to enter into the premise thereby giving complete protection ensuring security with the system.

Many access control systems use network for communication purpose and information is communicated through these networks.

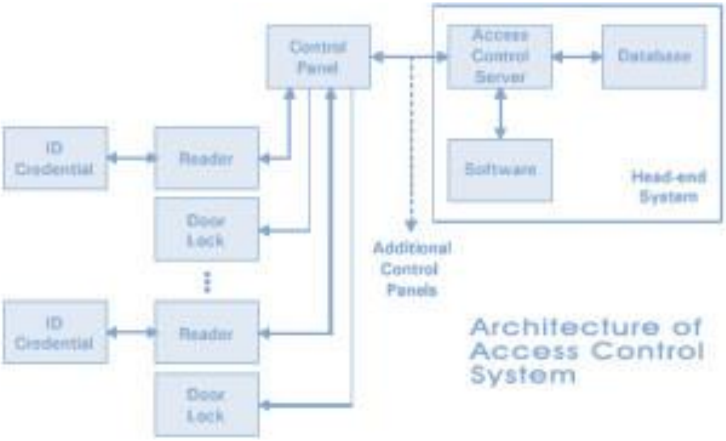
Example of an access control system : A door may be unlocked with a swipe card, an RFID system or by the technology of bio metric system.

What is access control system?

Access control system provides security by giving flexible control over who is allowed to enter your premises.

Access control system is one of the most common used system in electronic door control using a card or a magnetic stripe which can be accessed by swiping through a reader on the door. These access control systems are used for security purposes.

The areas or organizations which require high security use different types of access control systems like bio metric, RFID, door controllers and card readers etc. Each access point may be controlled individually as per the requirement of company or organizations where high security is necessary. Network security is also important, especially in a company which handles sensitive data.



metric Access Control System:

Bio metric Access Control System

The Bio metric Access Control System is a time attendance control system with fingerprint access and it tracks and records data of Visitors and Employees through its Access Software. This is widely used in confidential places for its easy installation and high security.

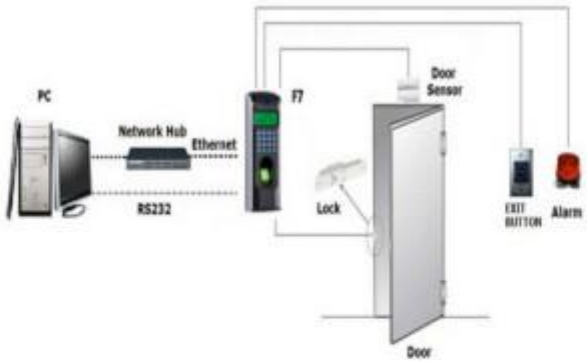
Finger Print Access

Bio metric Access Control System uses fingerprint instead of card system for access. The Access Control System not only permits entry but also gives the data regarding the entry of persons. The Attendance Software can be integrated with any existing payroll software and it gives automatic record of information generated by the Attendance System and this saves time and resources in recording. It increases productivity and profitability for any organization.

Door Access Control Systems:

Access Control Door opening/closing System is a compact, low cost, standalone. It is ready to use, easy to install device. Any electrician can install it with electromagnetic lock with simple instructions provided. It is widely used in Offices, Server rooms, Homes, Airports, Defense, Data centers etc.

Access control systems within a building may be linked or standardized based on the size of the organization and the varying levels of security. It is suitable for homes, offices and other access control applications. Access control systems were typically administered in a central location. Besides electronic door locks, there are access control panel models, magnetic door locks with uninterrupted power supplies.



6. Intrusion dectection

Intrusion detection, protection, and prevention

There are other forms of threat protection such as host”-based intrusion detection (HIDS) software that will alert you to the fact that an “attempt” to access your data was made. It operates off of a threat database that uses heuristics to look for trends in traffic that seem malicious. There are network-based forms of this protection such as network-based intrusion detection system (IDS) or intrusion prevention system (IPS), where it will attempt to prevent intrusions or detect that they have occurred.

When you think about surveillance activities, data gathering is a key to learning about your target and preparing for more advanced attacks. When attackers probe systems to gather data, data is logged in systems, firewalls, and sometimes can be flagged by IDS and IPS units. While, typically, IPS and other intrusion softwares are meant to block attacks such as IP fragmentation attacks, SYN attacks, and other types of network-based attacks, they can be referenced when scans are done to learn about a network architecture; so this may be a clue that someone is trying to gather information to learn a way to map or penetrate the network in order to obtain data.

Intrusion Detection

Intrusion detection is a funny thing. Some focus on the network layer, some on the application layer. In a XenApp environment, you are typically dealing with application-layer traffic. Web services behaviors and transactions using eXtensible Markup Language (XML), SOAP, and so on. There are two sorts of IDS in this context: *network* and *applications*. In addition, there are two layers of IDS: *network* and *host*.

Network IDS is going to work in a similar vein to Intrusion Protection System (IPS), except that the purpose is to detect situations like distributed Denial of Service (DoS) attacks, while IPS is simply permitting or denying certain traffic.

Intrusion Detection and Prevention

Intrusion detection and intrusion prevention on a nationwide scale or even across the DoD, as we discussed in the previous section, is a difficult prospect. At present, the networks that comprise the Internet are not segmented along national boundaries, for the most part. Additionally, we have a wide variety of media that can be used to carry network communications, including: copper and fiber optic cables, satellite communications, purpose build wireless networks, packet radio, and any number of other means. This lack of network segmentation along physical borders and wide variety of communications methods makes IDS/IPS a technically challenging prospect to implement.

Two main strategies exist for accomplishing intrusion detection and/or prevention on this scale; we can either structure networks to provide a limited number of connections outside of the area that we wish to protect and monitor, or we implement massively distributed IDS/IPS; either method has its inherent issues. Restructuring our networks to provide only a few choke points is most certainly the cleanest route to take, and may be workable when building new networks, but would likely be prohibitively expensive for existing networks. It will also be impacted by the move to the cloud and mobile devices, the days of isolated networks is even coming to a close in classified networks as we see them looking at how to move to these new infrastructures. Likewise, massively distributed IDS/IPS, although having the benefit of not requiring us to alter our networks, is likely to miss some of the traffic entering and exiting said networks. In either case, at present, conducting such operations is likely to prove difficult in a variety of ways.

5. What is Intellectual Property?

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

Modern GC have a lot on their minds (and on their desks). Contracts, litigation, and employee issues generally take up much of the day. However, there is another equally important area that generally does not get the same level of attention and care: intellectual property. Although frequently ignored, intellectual property should be nurtured and protected, as critical company assets comprise it. Unfortunately, many in-house lawyers don't understand the different types of intellectual property; therefore, they don't know the right steps to take in either protecting it or encouraging its creation. This lack of knowledge is remedied by Practical Law, a tool that provides numerous resources for in-house lawyers to easily get up to speed on four main types of intellectual property.

Patents

A patent is a government-granted monopoly to build, sell, and use your invention (and prevent others from doing so). If you are issued a patent, it's usually good for 20 years; however, there are some patents that are only good for 14 years. After 20 years, your patent expires and anyone can copy, build,and sell your invention. In exchange for the "monopoly," you must disclose the details of your invention to the public so that someone "practiced in the arts" could recreate it. To receive a patent your idea must meet four requirements:

- The subject matter must be "patentable" (as defined by Congress and the courts).
- Your idea must be "new."
- The idea must be "useful."
- Your idea must be "non-obvious."

There are three types of patents you can file for:

- **Utility patent** – Utility patents may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, composition of matter, or any new and useful improvement thereof (good for 20 years).
- **Design patent** – Design patents may be granted to anyone who invents a new, original, and ornamental design (good for 14 years).
- **Plant patent** – Plant patents may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant (good for 20 years).

See Practical Law – **Patent Application and Prosecution: Overview**

Patents can be expensive to obtain and maintain, as there are yearly or regular fees required to main them. And, like trademarks, patents are only good in the country where the patent was granted. So, in-house counsel must consider which countries and markets require patent protection.

See Practical Law – **Portfolio Development and Management**

Trademarks

A trademark can be any word, phrase, symbol, design, or combination of these things that identifies your goods or services — it's how customers recognize your company in the marketplace. We tend to use the term "trademark" generically as referring to both trademarks and service marks. A trademark is used for goods; a "service mark" is used for services.

A trademark has many benefits, including:

- Identifying the source of your goods or services
- Providing legal protection for your brand
- Guarding against counterfeiting and fraud

A trademark does not mean you own a particular word or phrase. Rather, you own the rights to how that word or phrase is used with respect to specific goods or services. Key to obtaining trademark protection is the need to identify the specific categories of goods and services the mark will cover. And, the company must actually use or provide such goods and services in the chosen categories — or have a good faith and demonstrative intent to do so.

See Practical Law – **Acquiring Trademark Rights and Registrations**

In-house counsel also need to avoid seeking trademarks that are merely descriptive of the goods or services. Unique words or phrases are far easier to protect and more likely to qualify for trademark protection. For example, "Nike" is a stronger, more unique mark than "Quality Tennis Shoes Company."

See Practical Law – **Filing a Federal Trademark Application Practice Note**

You own a trademark as soon as you start using it along with your goods or services. This is known as common law trademarks and it applies only to the geographic area where the company provides its goods or services. To obtain nationwide rights in the U.S., the company must apply to register your trademark with the United States Patent and Trademark Office (USPTO). Doing so provides broader rights and protections than an unregistered one, but the trademark is only valid in the U.S. — you must seek to register the trademark in every country where you seek protection.

Every time you use your trademark, you can use a symbol with it: "™" for goods, "℠" for services, or "®" for registered trademark. The symbol lets consumers and competitors know you are claiming the mark as yours. You can use "™" for goods or "℠" for services even if you haven't sought to register your trademark.

See Practical Law – **Trademark Registration and Maintenance Toolkit**

Critically, in-house counsel must take steps to protect trademarks by actively going after infringers — other companies using the mark or a similar mark — and ensuring that the mark does not become generic in the minds of the public (for example, "Band-Aid"). Failing to do so can cause the company to lose the mark.

See Practical Law –**Trademark Use and Protection Guidelines (Internal Distribution)**

Copyrights

Copyrights protect original works of authorship, such as paintings, photographs, musical compositions, sound recordings, computer programs, books, blog posts, movies, architectural works, and plays. There are some things that are not "creative," like titles, names, short phrases, and slogans; familiar symbols or designs; lettering or coloring; and mere listings of ingredients or contents. Copyrights protect expression and never ideas, procedures, methods, systems, processes, concepts, principles, or discoveries.

Companies can be copyright owners as the law allows ownership through "works made for hire" — works created by an employee within the scope of employment or certain independent contractors owned by the employer. Copyright law provides copyright owners with the following exclusive rights (among others):

- Reproduce the work
- Prepare derivative works
- Distribute copies by sale, transfer of ownership, or license
- Perform or display the work publicly

Works created on or after January 1, 1978, have a copyright term of life of the author plus seventy years after the author's death. For works made for hire, copyright protection is 95 years from publication or 120 years from creation, whichever is shorter. Copyrights exist automatically but you can enhance the protection by registering the work. Copyright registration is not mandatory but allows copyright owners to seek certain types of monetary damages and attorney fees.

Notable exceptions to the exclusive rights are "copyright fair use" or the use of copyrighted works that have fallen into the "public domain." As to the latter, in-house counsel must ensure any company copyrights are kept current until they otherwise expire.

See Practical Law – **Copyright Infringement Cease and Desist Letter**

Trade Secrets

While businesses have a lot of confidential information, not everything is a trade secret. A trade secret is typically something not generally known to the public, where reasonable efforts are made to keep it confidential, and confers some type of economic value to the holder by the information not being known by another party.

What exactly constitutes a trade secret can vary by state — in the U.S. — or by country. A good shorthand for what constitutes a trade secret is: any information you would not want your competitors to have. Some examples of likely trade secrets include new business models; customer and supplier information, especially around price; marketing strategy; processes and formulae; and other confidential business information.

See Practical Law – **Protection of Employers' Trade Secrets and Confidential Information**

Even if you have plans, processes, or formulae that you don't want your competitors to have, if the company doesn't take appropriate steps to keep that information confidential it can lose the ability to claim such items are trade secrets. For example, if the company has handed out copies of its future marketing plans to customers without any type of non-disclosure agreement in place or failed to label the plans as "confidential," the plans may not be treated as a trade secret.

Courts will generally look at the following factors to determine if something is a trade secret:

- Extent to which the information is known outside of the company
- Measures taken to guard the secrecy of the information
- Value of the information to competitors
- Extent to which the information is known throughout the company's employee base and others involved in the business
- Money or effort spent by the company to develop the information and how easy would it be for others to duplicate the information

See Practical Law – **Defend Trade Secrets Act Issues and Remedies Checklist.**

Understanding the different types of intellectual property is an important knowledge that all in-house counsel should master. Patents, trademarks, copyrights, and trade secrets are valuable assets of the company and understanding how they work and how they are created is critical to knowing how to protect them. With Practical Law, general counsel are only a few keystrokes away from a wide variety of information, forms, templates, and checklists that can help them master each type and know what to do to create and protect them.

6. What computer forensics do?

Computer forensics is a field of technology that **uses investigative techniques to identify and store evidence from a computer device**. Often, computer forensics is used to uncover evidence that could be used in a court of law.

What Jobs are Available in Computer Forensics?

People who have appropriate educational credentials and experience* may qualify for several different positions within the field of computer forensics. Jobs in this industry may include but are not limited to:

- **Computer Digital Forensic Investigator[2,3]:** Computer digital forensic investigators search the personal devices of suspects in order to identify information that could be relevant to a criminal case.
- **Computer Programmer:** Computer programmers write and evaluate code that computers use to function. Because computer forensics experts have an understanding of programming languages, they may also be qualified for computer programmer positions.
- **Cyber Forensics Analyst:** Cyber forensics analysts help investigators and detectives during the investigation of crimes. They recover deleted or encrypted data using processes that allow it to be admitted into court.

- **Computer Forensics Technician:** A computer forensics technician searches for information that may be relevant to an ongoing case. They search through personal devices and storage devices

What Skills Do I Need for Computer Forensics?

When training to work in computer forensics, there are several skills you'll want to acquire before you pursue a position in the field. Some of these skills may include:

- **Programming:** An understanding of programming languages is essential for digging into devices to recover difficult to find, lost or encrypted data.
- **ISO standards:** ISO standards are a set of rules and protocols dictating the best way to perform a task. Computer forensics uses these standards, making them vital to understand.
- **Operating systems:** Operating systems are what enable devices to perform their core set of functions. Because computer forensics professionals often work with broken or compromised devices, they need to understand operating systems in order to recover lost data.
- **Computer hardware and software:** Computer forensics experts need to know how the software and hardware elements of a computer work in order to find the best places to look for data. It's also useful in case a repair needs to be performed in order to recover data.
- **Organization:** Having a strong sense of organization is critical for those in the computer forensics profession. People in this field comb through data and need organizational skills in place that can help them separate irrelevant data from important information.
- **Cyber security standards:** A computer forensics expert should have a strong grasp of the standards used in the cyber security industry.
- **Analytical capabilities:** Finally, a computer forensics expert needs to be able to analyze the data that they uncover. Doing so can help them identify data that is of value for an investigation.

7. What is Internet Ethics?

1. Home
2. Markkula Center for Applied Ethics
3. Focus Areas
4. Internet Ethics
5. Internet Ethics Resources
6. What is Internet Ethics?

This article is a transcript of the video What Is Internet Ethics? In the video, Irina Raicu, director of Internet Ethics, discusses topics such as privacy, big data, net neutrality, and internet access.

Internet ethics is a really broad term. It basically refers to the analysis of the role that the internet plays in what philosophers call the development of the good life - the kind of life that we want for ourselves, for society over all, the kinds of people we want to be. Is the internet playing a positive role in the development of that kind of life or is it hampering us in some way?

And there are a lot of issues that fall under that umbrella. Everything from the role that social media plays in the creation of human relationships, to privacy, to net neutrality, to the whole question of who has and doesn't have access to the internet, to the development of the big data ecosystem, the kind of data that's collected, by whom and about whom, and for what purposes. There are a variety of questions that fall under that term and increasingly new questions because the internet has some connection to every aspect of our lives.

Privacy

One of the most interesting ethical questions on internet ethics revolves around privacy online. Can the internet continue to be a medium that invites creativity and freedom of expression and freedom of sharing information across borders even as it's becoming a tool of mass surveillance, either from corporate entities or from governments or from both?

Increasingly we find that people are concerned that their personal data is being collected and stored and used in a variety of ways that they're not really aware of, that they don't want to have used against them, or in ways that they don't anticipate, and it's becoming really a problem for what had been a fantastic way to allow people to communicate.

Big Data

One of the phenomena that the rise of the internet has led to is the collection and analysis of big data, which raises fascinating ethical questions about who or what the data is being collected about, who's being left out of that kind of data collection, who makes the decisions about what is being done with that data, and how much we can rely on it. There's aan air of objectivity and completeness about this data that turns out to be misleading, and at the same time we are relying on it as this objective source of truth on a very widespread societal level.

We allow big data now to impact the decisions we make about who goes to prison, who gets bail, who gets a job, who gets insurance, what kind of majors people might go into in college. And it's fascinating to see a kind of maturing of the field and big data proponents and analysts themselves finding out that they have a much greater responsibility than they had initially realized.

Net Neutrality

One of the ethical principles behind the development of the internet has been net neutrality, the idea that the controllers of the pipelines of the internet will not be able to pick and choose between the kinds of content that's available, that everything will be able to flow freely.

And increasingly that's being challenged as the companies that really run those pipelines try to find ways to benefit or to encourage the consumption of some content more than others. And there are regulators getting involved and there are civil libertarians and civic groups trying to argue that we want to have this impartial, neutral, internet conduit.

That will be one of the really interesting issues to watch: whether the internet continues to be a sort of neutral playground for communication and transfer of information or whether some content is favored in some way. What does that mean for freedom and access to information in general?

Access to the Internet

The Markkula Center for Applied Ethics is in the heart of Silicon Valley, and even here in Silicon Valley there are people who don't have access to the internet or who have very limited access only via their phones, or not through broadband. We hear stories about students having to sit in their cars outside of McDonald's or some other place that offers free Wi-Fi.

We need to ask whether internet access should be seen as a human right, especially in our society, in our culture. The fact that there are still vast numbers of people across the U.S. who have to struggle with this is an ethical imperative for the government and for corporations and for schools and for any other entities that deal with the broad public to consider. We should stop assuming that we all have access to the internet and that we can all use those resources. It's simply not true. The ethical question of how we create equality in a country where so much is dependent on the internet and so many people don't have access to it is really important.

-