CyberRookie CSX Fundamentals - Section 6: Security Implications and adoption of evolving technology

A threat landscape or threat environment	is a collection of threats.
The cybersecurity threat landscape is	constantly changing and evolving as new technologies are developed and cyberattacks and tools become more sophisticated
Corporations are becoming increasingly dependent on	digital technologies that can be susceptible to cyber security risk
Cloud computing, social media, and mobile computing are	changing how organizations use and share information. They provide increased levels of access and connectivity, which create larger openings for cybercrime.
Cybercriminals are usually motivated by one or more of the following:	Financial gains, Intellectual property (espionage), Politics (hacktivism)
Recent trends in the cyberthreat landscape include	Threat agents are more sophisticated, Attack patterns are now being applied to mobile devices, Multiple nation states have the capabilities to infiltrate government and private targets, Cloud computing targets, Social networks, data as an asset allows for the potential for big data breaches.
Advanced persistent threats (APTs)	are relatively new phenomena for many organizations
Although the motives behind Advanced persistent threats are not entirely new	the degree of planning, resources employed and techniques used in APT attacks are unprecedented
These threats demand a degree of vigilance and a set of countermeasures that	are above and beyond those routinely used to counter everyday security threats from computer hackers, viruses or spammers.
Many experts regard APTs as	nothing new or, simply the latest evolution in attack techniques that have been developing over many years, the term is misleading, pointing out that many attacks classed as APTs are not especially clever or novel.
An APT is	a targeted threat that is composed of various complex attack vectors and can remain undetected for an extended period of time.
It is a specifically targeted and sophisticated attack that	keeps coming after the victim
An example of an APT is	spear phishing, where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim
But most APT attacks originate from	more sinister sources
APTs are often the work of	professional teams employed by organized crime groups, determined activists or governments. This means they are likely to be well-planned, sophisticated, well-resourced and potentially more damaging
APT attacks vary significantly in their approach; however, they share the following characteristics	Well-researched, Sophisticated, Stealthy, Persistent
Well-researched APT attacks	APT agents thoroughly research their targets, plan their use of resources and anticipate countermeasures.
Sophisticated APT attacks	APT attacks are often designed to exploit multiple vulnerabilities in a single attack. They employ an extensive framework of attack modules designed for executing automated tasks and targeting multiple platforms.
Stealthy APT attacks	APT attacks often go undetected for months and sometimes years. They are unannounced and disguise themselves using obfuscation techniques or hide in out-of-reach places.

20.	**Persistent APT attacks**	APT attacks are long-term projects with a focus on reconnaissance. If one attack is successfully blocked, the perpetrators respond with new attacks. And, they are always looking for methods or information to launch future attacks.
21.	**APTs target companies of all**	sizes across all sectors of industry and all geographic regions that contain high value assets.
22.	**Staff of all levels of seniority, ranging from administrative assistants to chief executives**	can be selected as a target for a spear-phishing attack
23.	**Small companies and contractors might**	be penetrated because they are a supplier of services to a targeted victim
24.	**Individuals might be selected if**	they are perceived to be a potential stepping stone to help gain access to the ultimate target
25.	**No industry with valuable secrets or other sources of commercial advantage that can be copied or undermined through espionage is**	safe from an APT attack
26.	**No enterprise that controls money transfers, processes credit card data or stores personally identifiable data on individuals can be**	sheltered from criminal attacks
27.	**no industry that supplies or supports critical national infrastructure**	is immune from an intrusion by cyberwarriors.
28.	**APT attacks often encompass**	third-party organizations delivering services to targeted enterprises
29.	**Third party suppliers can be perceived by**	an attacker as the weakest link of large companies and government departments because they are generally less well protected.
30.	**No matter how effective a company's external perimeter security might be**	it can be of limited value unless extended across its supply chain
31.	**Threat from Intelligence agencies**	seek Political, defense or commercial trade secrets and impact is Loss of trade secrets or commercial, competitive advantage
32.	**Threat from Criminal groups**	seek Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale and impact is Financial loss, large-scale customer data breach or loss of trade secrets
33.	**Threat from Terrorist groups**	seek Production of widespread terror through death, destruction and disruption and impact is Loss of production and services, stock market irregularities, and potential risk to human life
34.	**Threat from Activist groups**	seek Confidential information or disruption of services and impact is Major data breach or loss of service
35.	**Threat from Armed forces**	seek Intelligence or positioning to support future attacks on critical national infrastructure and impact is Serious damage to facilities in the event of a military conflict
36.	**Even though no two APT attacks are exactly alike**	they often follow a similar life cycle
37.	**APTs start with**	intelligence gathering, which includes selecting and researching their target, planning the attack and collecting and analyzing data from an initial penetration
38.	**After intelligence gathering happens in an APT**	The attacker then establishes command and control, collecting targeted information. That information is then exfiltrated to the attacker's location to be disseminated or exploited.
39.	**Security for mobile technology is**	a function of the risk associated with its use

40.	**Despite positive and negative impacts, security teams must deal with**	the risk common to all mobile devices and applications
41.	**Information travels across wireless networks that are often less secure than wired networks.**	Malicious outsiders can do harm to the enterprise. Information interception resulting in a breach of sensitive data, damage to enterprise reputation, compromised adherence to regulation or legal action
42.	**Mobility provides the users with the opportunity to leave enterprise boundaries, thereby eliminating many security controls.**	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network. Malware propagation, which can result in data leakage, data corruption and unavailability of necessary data Physical theft
43.	**Bluetooth (BT) technology makes it very convenient for many users to have hands-free conversations; however, it is often left on and is then discoverable.**	Hackers can discover the device and then launch an attack. Device corruption, lost data, call interception, possible exposure of sensitive information
44.	**Unencrypted information is stored on the device.**	In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable. Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
45.	**Lost data may affect employee productivity.**	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up. Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices, and data that are not backed up
46.	**The device has no authentication requirements applied.**	If the device is lost or stolen, outsiders can access the device and all its data. Data exposure, resulting in damage to the enterprise and liability and regulation issues
47.	**The enterprise is not managing the device.**	If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. they may interact with emails or store sensitive documents. Data leakage, malware propagation, unknown data loss in the event of device loss or theft
48.	**The device allows installation of unverified/unsigned third-party applications.**	Applications may carry malware that propagates Trojan horses or viruses. The applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network. Malware propagation, data leakage, intrusion to the enterprise network
49.	**mobile technology presents risks that**	need to be managed through technical and organizational steps
50.	**As users increasingly rely on their mobile devices**	loss or theft is more likely to create disruptive conditions and may leave employees unable to work for prolonged periods of time.
51.	**unprotected and transient data, such as lists of calls, texts or calendar items**	may be compromised, allowing attackers to harvest large amounts of data
52.	**With criminal intent, perpetrators may**	be able to recover deleted data and a history of the use of the mobile device.
53.	**An additional significant risk is identity theft**	which may occur as a result of obtaining and analyzing a stolen or lost mobile device
54.	**Many mainstream OSs for smart devices mandate the link to**	a user account with the provider, thus greatly increasing the risk of losing one's digital identity with the actual device.
55.	**The link between device and account is**	sometimes subject to even greater risk when value-added services are offered as an add-on to the existing user account
56.	**Some OSs offer a**	"secure" repository for enriched user data ranging from personal information to automated credit card storage and payment functionality
57.	**The risk of entrusting such sensitive data to a mobile device ("all in one place")**	should not be neglected

58.	**From a security management perspective, several attempts have been undertaken to prevent, or at least mitigate, the threat of device loss or theft**	Cell-based tracking and locating the device, Remote shutdown/wipe capabilities, Remote SIM card lock capabilities
59.	**still a window of exposure to attackers exploring the mobile device**	possibly using analytical tools that will circumvent the standard OS features. threat is particularly significant because enforcing strong passwords and encryption on mobile devices may be restricted due to OS limitations.
60.	**As with many other technologies, mobile devices have**	rapidly pervaded enterprises at all levels
61.	**In terms of data, information and knowledge that exist across the enterprise**	many users have privileged access that is often replicated on their mobile devices.
62.	**corporate PC environments have been the target of hardening and protective measures for many years, mobile devices and their comparatively weak security mechanisms**	are more difficult to manage and control
63.	**C-suite and senior managers will often be heavy mobile users, and**	any successful compromise of their devices could certainly cause major damage.
64.	**Another important organizational risk arises from the growing complexity and diversity of**	common mobile devices
65.	**Examples such as inadvertent data roaming or involuntary GPS tagging show**	how many users simply do not understand the extended features of their devices.
66.	**the rapid succession of new generations of hardware requires**	constant adaptation on the part of users and enterprises
67.	**The comparatively long systems management cycles found in larger enterprises may**	cause difficulties when facing the usual turnaround time of approximately two years for new mobile devices and the life span of mobile OSs and applications is becoming much shorter
68.	**The resulting risk to users is aggravated by**	he fact that few enterprises offer formal or informal training for mobile device use. Users are literally left on their own when it comes to adopting and using new technology and new services.
69.	**mobile devices use service-based OSs with the ability to**	run multiple services in the background
70.	**monitoring and influencing activity is**	a core functionality of spyware and malware, as is covert data retrieval.
71.	**Data can be intercepted in real time as they are**	being generated on the device. Examples include sending each email sent on the device to a hidden third-party address, letting an attacker listen in on phone calls or simply opening microphone recording
72.	**Stored data such as**	a contact list or saved email messages can also be retrieved.
73.	**Messaging**	Generic attacks on SMS text, MMS-enriched transmission of text and contents, Retrieval of online and offline email contents, Insertion of service commands by SMS cell broadcast texts, Arbitrary code execution via SMS/MMS, Redirect or phishing attacks by HTML-enabled SMS text or email
74.	**Audio**	Covert call initiation, call recording, Open microphone recording
75.	**Pictures/Video**	Retrieval of still pictures and videos, for instance, by piggybacking the usual "share" functionality in most mobile apps, Covert picture or video taking and sharing, including traceless wiping of such material
76.	**Geolocation**	Monitoring and retrieval of GPS positioning data, including date and time stamps
77.	**Static data**	Contact list, calendar, tasks, notes retrieval
78.	**History**	Monitoring and retrieval of all history files in the device or on SIM card (calls, SMS, browsing, input, stored passwords, etc.)

79.	**Storage**	Generic attacks on device storage (hard disk or solid state disk [SSD]) and data replicated there
80.	**In combination with attacks on connectivity, the risk of**	activity monitoring/influencing and covert data retrieval is significant
81.	**Most spyware or malware once placed on a mobile device will**	require one or more channels for communicating with the attacker
82.	**While "sleepy" malware may have a period of latency and remain dormant for weeks or months**	data and information harvested will eventually need to be transmitted from the mobile device to another destination.
83.	**the command and control functionality often found in malware requires**	a direct link between the mobile device and the attacker, particularly when commands and actions are to be executed and monitored in real time
84.	**Email**	Simple to complex data transmission (including large files)
85.	**SMS**	Simple data transmission, limited command and control (service command) facility
86.	**HTTP get/post**	Generic attack vector for browser-based connectivity, command and control
87.	**TCP/UDP socket**	Lower-level attack vector for simple to complex data transmission
88.	**DNS exfiltration**	Lower-level attack vector for simple to complex data transmission, slow but difficult to detect
89.	**Bluetooth**	Simple to complex data transmission, profile-based command and control facility, generic attack vector for close proximity
90.	**WLAN/WiMAX**	Generic attack vector for full command and control of target, equivalent to wired network
91.	**the relative anonymity of wireless connectivity vectors particularly**	Bluetooth and WLAN/WiMAX
92.	**The risk of ad hoc attacks on mobile devices is**	significantly higher when anonymous connectivity is provided by third parties, for example, in airport lounges or coffee shops
93.	**While most mobile devices support all relevant browser protocols, the presentation to the user**	is modified by the mobile service provider. This is mainly done to optimize viewing on small screens
94.	**web pages viewed on a typical (smaller) device often**	show "translated" content, including modifications to the underlying code.
95.	**In UI impersonation, malicious apps present a**	UI that impersonates the native device or that of a legitimate app
96.	**When the victim supplies authentication credentials**	these are transmitted to the attacker. This is conducive to impersonation attacks that are similar to generic phishing.
97.	**Typical web view applications allow**	attacks on the proxy level and on the presentation level
98.	**This type of risk is prevalent in banking applications where**	several cases of malware have been documented
99.	**Given the attractiveness of payment data and user credentials**	web view and impersonation risk is likely to increase in the future.
100.	**With the emergence of new work patterns and the need for decentralized data availability**	mobile devices often store large amounts of sensitive data and information
101.	**confidential presentations and spreadsheets are often displayed directly from a smart mobile device rather than using**	a laptop computer
102.	**The amount of storage space found on many devices is growing and this greatly increases the risk of data leakage, particularly when**	mobile devices store replicated information from organizational networks

103.	**Identity**	Hardware/firmware and software release stats, also disclosing known weaknesses or potential zero-day exploits, International Mobile Equipment Identity (IMEI), manufacturer device ID, customized user information
104.	**Credentials**	User names and passwords, keystrokes and Authorization tokens, certificates (S/MIME, PGP, etc.)
105.	**Location**	GPS coordinates, movement tracking, location/behavioral inference
106.	**Files**	All files stored at operating system/file system level
107.	**Sensitive data leakage can be**	inadvertent or can occur through side channel attacks
108.	**Even a legitimate application may have**	flaws in the usage of the device
109.	**information and authentication credentials may be**	exposed to third parties
110.	**Mobile devices provide a fairly detailed picture of**	what their users do, where they are and their preferences
111.	**Side channel attacks over prolonged periods of time allow**	the building of a detailed user profile in terms of movements, behavior and private/business habits
112.	**Sensitive data leakage allowing the prediction of users' behavior patterns and activities is**	becoming more significant as many users prefer to set their devices to "always on" mode to benefit from legitimate services such as navigation or local points of interest.
113.	**While most mobile OSs offer protective facilities such as storage encryption**	many applications store sensitive data such as credentials or tokens as plaintext
114.	**data stored by the user is often**	replicated without encryption, and many standardized files such as Microsoft Office® presentations and spreadsheets are stored unencrypted for quick access and convenience.
115.	**Another risk associated with unsafe storage of sensitive data is**	the use of public cloud services for storage purposes
116.	**Many mobile device providers have introduced cloud services that offer**	a convenient way of storing, sharing and managing data in a public cloud
117.	**these cloud services target**	the private consumer, and the security functionality would not normally stand up to organizational (corporate) requirements
118.	**when data and information are stored or replicated in public clouds**	terms and conditions generally rule out any form of responsibility or liability, requiring the user to make individual security arrangements.
119.	**In an organizational context, these limitations may**	increase the risk of sensitive data storage, particularly in a BYOD scenario.
120.	**Mobile devices predominantly rely on**	wireless data transmission, except for the few cases when they are physically connected to a laptop or desktop computer
121.	**As a new transmission protocol, NFC**	increases the risk at very short range, for example, when transmitting payment data over a distance of several inches.
122.	**Even if data at rest is protected by encryption and other means,**	transmission is not always encrypted
123.	**Mobile users are likely to use**	unsecured public networks frequently, and the large number of known attacks on WLAN and Bluetooth are a significant risk.
124.	**Automatic network recognition, a common feature in mobile OSs, may**	link to WLANs available in the vicinity, memorizing Service Set Identifiers (SSIDs) and channels
125.	**For many major providers of public WLANs, these SSIDs**	are identical across the world
126.	**This is intentional and convenient; however, the risk of an evil twin attack increases with the use of**	generic names that the mobile device will normally accept without verification

127.	**While many enterprises have implemented VPN solutions for their users**	these may not be workable on mobile devices that are used both for business and personal transactions
128.	**Given the relative complexity of configuring and activating VPN on mobile devices, users may**	deactivate protected data transmission to access another service that does not support VPN
129.	**Even for split-tunnel VPN installations—offering a VPN to the enterprise while keeping the open link to the public network—the risk of an at-source attack is**	still high
130.	**typical word processing, spreadsheet and presentation software on mobile devices tends to be optimized for**	opening and reading rather than editing information
131.	**popular document formats such as Adobe® portable document format (PDF) are implemented, more or less, as a**	read-only solution designed for a cursory read rather than full-scale processing.
132.	**it has become common practice to insert active content into documents and PDF files which is**	known as an attack vector for malware and other exploits.
133.	**The restricted nature of mobile device applications leads to an**	increased risk of drive-by attacks because these apps may not recognize malformed links and omit the usual warnings that users could expect from the desktop versions of Microsoft Office or PDF applications.
134.	**these vulnerabilities create risk and a number of threats for end users, for example**	the insertion of illegal material, inadvertent use of "premium" services via SMS/MMS or bypassing two-factor authentication mechanisms.
135.	**Mobile devices have had a profound impact on**	the way business is conducted and on behavior patterns in society.
136.	**Mobile devices have greatly increased**	productivity and flexibility in the workplace, to the extent that individuals are now in a position to work from anywhere at any given time
137.	**Manufacturers and service providers alike have created**	both new devices and new business models such as mobile payments or subscription downloads using a pay-as-you-go model
138.	**consumerization of devices has relegated enterprises, at least in some cases, to**	followers rather than opinion leaders in terms of which devices are used and how they are used.
139.	**The impact of using mobile devices falls into two broad categories:**	The hardware itself has been developed to a level at which computing power and storage are almost equivalent to PC hardware. New mobile services have created new business models that are changing organizational structures and society as a whole
140.	**Consumerization is not limited to**	devices.
141.	**New, freely available applications and services provide better user experiences for things like**	note-taking, video conferencing, email and cloud storage than their respective corporate-approved counterparts
142.	**Instead of being provided with company-issued devices and software,**	employees are using their own solutions that better fit with their lifestyle, user needs and preferences
143.	**General mobility and location-independent accessibility have enhanced business practices and have allowed**	enterprises to focus on core activities while reducing the amount of office space used
144.	**mobile devices have brought greater flexibility, for example, in**	bring your own device (BYOD) scenarios.

145.	**when centralized procurement and provisioning of mobile devices are slow or cumbersome**	many users have developed the expectation of simply "plugging in" their own units to achieve productivity in a quick and pragmatic manner.
146.	**The obvious downside is the proliferation of**	devices with known (or unknown) security risk, and the formidable challenge of managing device security against several unknowns
147.	**as the workforce changes, there are clear signs that BYOD is**	becoming an important job motivation factor, because employees are no longer willing to accept technology restrictions.
148.	**security management should address both**	the innovative potential and the risk and threats of flexible device use because it is unlikely that restrictions or bans on certain types of devices will be effective even in the medium term
149.	**the fact that some enterprises have attempted a ban on certain devices has allowed**	the prohibited technology to gain a foothold within the corporate landscape—particularly if that technology is already widely accepted among private users
150.	**enterprises with a restrictive perspective on innovative devices will always**	be behind the threat curve and thus exposed to unnecessary risk.
151.	**Pros of BYOD**	Shifts costs to user, Worker satisfaction, More frequent hardware upgrades, Cutting-edge technology with the latest features and capabilities
152.	**Cons of BYOD**	IT loss of control, Known or unknown security risk, Acceptable Use Policy is more difficult to implement, Unclear compliance and ownership of data
153.	**According to NIST and the Cloud Security Alliance (CSA), cloud computing is defined as**	a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."
154.	**Cloud computing offers enterprises a way to**	save on the capital expenditure associated with traditional methods of managing IT.
155.	**Common platforms offered in the cloud include**	Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)
156.	**Virtualization and service-oriented architectures (SOAs) act as**	key enablers behind the scenes
157.	**cloud computing is not without its own set of risk, first and foremost of which is**	the safety and security of the data that are entrusted in the care of cloud providers
158.	**it is important for organizations to ensure that their cloud provider has a**	security system in place equivalent to or better than the organization's own security practice.
159.	**Many cloud providers are**	ISO27001 or FIPS 140-2 certified
160.	**organizations can request**	audits of the cloud provider.
161.	**The security audits should cover the**	networks, hardware and operating systems within the cloud infrastructure.
162.	**The challenge for cloud computing is**	to protect data within public and private clouds as well as ensure governance, risk management and compliance are addressed across the full, integrated environment
163.	**NIST outlines the following top security risks for cloud infrastructure:**	Loss of governance, Lock-in, Isolation failure, Compliance, Management interface compromise, Data protection, Insecure or incomplete data deletion, Malicious insider
164.	**Loss of governance**	The client usually relinquishes some level of control to the cloud provider, which may affect security, especially if the SLAs leave a gap in security defenses.
165.	**Lock-in**	It can be difficult for a client to migrate from one provider to another, which creates a dependency on a particular cloud provider for service provision.

166.	**Isolation failure**	One characteristic of cloud computing is shared resources. Although not commonplace, the failure of mechanisms that separate storage, memory, routing and reputation between different tenants can create risk.
167.	**Compliance**	Migrating to the cloud may create a risk in the organization achieving certification if the cloud provider cannot provide compliance evidence
168.	**Management interface compromise**	The customer management interface can pose an increased risk because it is accessed through the Internet and mediates access to larger sets of resources.
169.	**Data protection**	It may be difficult for clients to check the data handling procedures of the cloud provider.
170.	**Insecure or incomplete data deletion**	Because of the multiple tenancies and the reuse of hardware resources, there is a greater risk that data are not deleted completely, adequately, or in a timely manner.
171.	**Malicious insider**	Cloud architects have extremely high-risk roles. A malicious insider could cause a great degree of damage.
172.	**The CSA lists the following as the top cloud computing threats:**	Data breaches, Data loss, Account hijacking, Insecure application programming interfaces (APIs), Denial-of-service (DoS), Malicious insiders, Abuse of cloud services, Insufficient due diligence, Shared technology issues
173.	**In implementing and adapting their cloud-based strategies, enterprises tend to include**	SaaS offerings, sometimes extending this to critical business processes and related applications
174.	**Despite the fact that these service offerings may bring business advantages, they nevertheless generate**	data-in-flow vulnerabilities that may be exploited by cybercrime and cyberwarfare.
175.	**The resulting risk is exacerbated by the fact that**	many vendors and hardware providers (e.g., for mobile devices), supply cloud-based freeware designed to enforce user loyalty. This is often the case for data synchronization, handling of popular file types
176.	**The application layer within the overall IT environment is particularly susceptible to**	zero-day exploits, as witnessed by many practical examples
177.	**Even major software vendors frequently update and patch their**	applications, but new attack vectors using such applications emerge almost on a daily basis
178.	**In terms of cybercrime and cyberwarfare, the market for zero-day exploits is a lively one, and the time span from**	discovery to recognition and remediation is increasing.
179.	**recent specimens of malware show a higher level of**	sophistication and persistence than the basic varieties used by opportunistic attackers
180.	**While software vendors are quick to address malware in terms of recognition and removal, there is**	a significant residual risk of malware becoming persistent in target enterprises.
181.	**Secondary malware attacks—where APTs make use of already installed simple malware —are often**	successful where the environmental conditions are conducive to user error or lack of vigilance, namely in home user or traveling user scenarios
182.	**removal of the primary malware (a fairly simple process) often**	allays any further suspicion and causes users and security managers to be lulled into a false sense of security
183.	**The secondary and very complex malware may have**	infiltrated the system, presenting a known and simple piece of primary malware as bait.
184.	**Although cloud computing is attractive to attackers because of the massive concentrations of data**	cloud defenses can be more robust, scalable and cost-effective
185.	**top security benefits of cloud computing**	Market drive, Scalability, Cost-effective, Timely and effective updates, Audit and evidence

186.	**Market drive of cloud computing**	Because security is a top priority for most cloud customers, cloud providers have a strong driver for increasing and improving their security practices
187.	**Scalability of cloud computing**	Cloud technology allows for the rapid reallocation of resources, such as those for filtering, traffic shaping, authentication and encryption, to defensive measures.
188.	**Cost-effective of cloud computing**	All types of security measures are cheaper when implemented on a large scale. The concentration of resources provides for cheaper physical perimeter and physical access control and easier and cheaper application of many security-related processes.
189.	**Timely and effective updates of cloud computing**	Updates can be rolled out rapidly across a homogeneous platform.
190.	**Audit and evidence of cloud computing**	Cloud computing can provide forensic images of virtual machines, which results in less downtime for forensic investigations.
191.	**Benefits of Cloud Computing**	Market drive for the cloud, Scalability, Cost-effective implementation, Timely and effective updates, Audit and evidence capabilities
192.	**Risks of Cloud Computing**	Loss of governance, Lock-in to one provider, Isolation failure, Compliance, Data protection, Customer management interface compromise, Insecure or incomplete data deletion, Malicious insider