****

**Data Networking And Communication**

**(*DCN*)**

**Cyber Security *Project Research Report***

***CLASS ID: 107933***

**Project Title: Cyber Security**

**Project Members:**

1. 11508 Muzamil Khan
2. 11200 Muhammad Ahmed
3. 11515 Zain Zahid

**Content:**

Defination of Cyber security 01

What is Cyber security all about ? 20

Importance of Cyber security 12

Who need cyber security ? 07

Types of Cyber Threat 08

Types of Cyber security 09

Cyber security vs Information Security 10

Challenges of Cyber security 07

Consequences of Cyber attacks 09

Managing Cyber security 12

How to approch Cyber security 12

Cyber security checklist 12

Challenges of Cyber security 12

Cyber Security In Pakistan 12

**Defination of Cyber security:**

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

**What is Cyber security all about ?**

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks. A [unified threat management](https://www.cisco.com/c/en/us/products/security/threat-response.html) system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.

**People:**

Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Learn more about [basic cybersecurity principles](https://umbrella.cisco.com/blog/2019/12/04/cisco-umbrella-top-10-cybersecurity-tips/?utm_medium=web-referral&utm_source=cisco&utm_campaign=cs-fy2020-q2-cisco-100-day-sprint&utm_term=pgm).

**Processes:**

Organizations must have a framework for how they deal with both attempted and successful cyber attacks. One [well-respected framework](https://blogs.cisco.com/security/cisco-and-the-nist-cybersecurity-framework-benefit-from-a-fresh-and-innovative-approach-to-cybersecurity) can guide you. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks. Watch a video explanation of the [NIST cybersecurity framework (1:54)](javascript:void(0);)

**Technology:**

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

**Importance of Cyber security:**

In today’s connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyber attack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open source tools. Their work makes the Internet safer for everyone.

The fact of the matter is whether you are an individual, small business or large multinational, you rely on computer systems every day. Pair this with the rise in cloud services, poor [cloud service security](https://www.upguard.com/blog/s3-security-is-flawed-by-design), smartphones and the Internet of Things (IoT) and we have a myriad of potential security vulnerabilities that didn't exist a few decades ago. We need to understand the difference between [cybersecurity and information security](https://www.upguard.com/blog/cyber-security-information-security), even though the skillsets are becoming more similar.

Governments around the world are bringing more attention to cybercrimes. GDPR is a great example. It has increased the reputational damage of data breaches by forcing all organizations that operate in the EU to:

* Communicate data breaches
* Appoint a data protection officer
* Require user consent to process information
* Anonymize data for privacy

The trend towards public disclosure is not limited to Europe. While there are no national laws overseeing data breach disclosure in the United States, there are data breach laws in all 50 states. Commonalities include:

* The requirement to notify those affect as soon as possible
* Let the government know as soon as possible
* Pay some sort of fine

**Who needs Cyber security?**

It is a mistake to believe that you are of no interest to cyber attackers. Everyone who is connected to the Internet needs cyber security. This is because most cyber attacks are automated and aim to exploit common vulnerabilities rather than specific websites or organisations.

**Types of Cyber Threats**

Common cyber threats include:

1. **Malware**, such as ransomware, botnet software, RATs (remote access Trojans), rootkits and bootkits, spyware, Trojans, viruses and worms. For example(**spyware**, **Ransomware, Keyloggers are some examples of marware software**)
2. **Backdoors**, which allow remote access. For example (A well-known backdoor example is called **FinSpy**. When installed on a system, it enables the attacker to download and execute files remotely on the system the moment it connects to the internet, irrespective of the system's physical location. It compromises overall system security.)
3. **Formjacking**, which inserts malicious code into online forms. For example (**Attacks on Ticketmaster, Feedify, British Airways, and Newegg** are only some of the Formjacking examples done by this consortium. The group injects web-based card skimmers onto eCommerce sites to steal payment card data or credit card information and other sensitive information right from online payment forms.)
4. **Cryptojacking**, which installs illicit cryptocurrency mining software. For example (In 2019,**eight separate apps that secretly mined cryptocurrency with the resources of** whoever downloaded them were ejected from the Microsoft Store. When visitors went to the Homicide Report page, their devices were used to mine a popular cryptocurrency called Monero.)
5. **DDoS (distributed denial-of-service) attacks**, which flood servers, systems and networks with traffic to knock them offline. For example ([Amazon Web Services](https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf), the 800-pound gorilla of everything cloud computing, was hit by a gigantic DDoS attack in February 2020. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS customer using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim’s IP address by 56 to 70 times. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second.)
6. **DNS (domain name system) poisoning attacks**, which compromise the DNS to redirect traffic to malicious sites. For example (DNS poisoning occurs when one of these caches is compromised. For example, **if the cache on a network router is compromised**, then anyone using it can be misdirected to a fraudulent website. The false DNS records then trickle-down to the DNS caches on each user's machine.)

**Types of Cyber security:**

Following are 5 types of cyber security.

### **1. Critical Infrastructure Cyber security:**

Critical infrastructure organisations are often more vulnerable to attack than others because SCADA (supervisory control and data acquisition) systems often rely on older software.

Operators of essential services in the UK’s energy, transport, health, water and digital infrastructure sectors, and digital service providers are bound by the [NIS Regulations (Network and Information Systems Regulations 2018)](https://www.itgovernance.co.uk/nis-directive).

Among other provisions, the Regulations require organisations to implement appropriate technical and organisational measures to manage their security risks.

### **2. Network security:**

Network security involves addressing vulnerabilities affecting your operating systems and network architecture, including servers and hosts, firewalls and wireless access points, and network protocols.

### **3. Cloud security:**

[Cloud security](https://www.itgovernance.co.uk/cloud-security) is concerned with securing data, applications and infrastructure in the Cloud.

### **4. IoT (Internet of Things) security:**

IoT security involves securing smart devices and networks that are connected to the IoT. IoT devices include things that connect to the Internet without human intervention, such as smart fire alarms, lights, thermostats and other appliances.

### **5. Application security:**

Application security involves addressing vulnerabilities resulting from insecure development processes in the design, coding and publishing of software or a website.

**Cyber security vs Information Security:**

Cyber security is often confused with [information security](https://www.itgovernance.co.uk/infosec).

* Cyber security focuses on protecting computer systems from unauthorised access or being otherwise damaged or made inaccessible.

|  |  |
| --- | --- |
| Cyber Security | Information Security |
| Focuses solely on online threats | Takes a mile-high view of the security landscape |
| Learns to think like a hacker | Deals with the protection of data from any threat |
| Develops a deep understanding of malicious software | Oversees unauthorized access/modification/disruption |
| Acts as the first line of defense | Makes plans to recover from a breach |

* Information security is a broader category that protects all information assets, whether in hard copy or digital form.

**Challenges of Cyber security:**

Mitigating the cyber security risks facing your organisation can be challenging. This is especially true if you have moved to remote working and have less control over employees’ behaviour and device security.

Below are five challenges that will impact the cybersecurity industry in the latter half of 2021.

## 1. Adapting to a Remote Workforce:

It's no secret that there's been a significant increase in the number of people working remotely. As the pandemic continues to impact communities across the globe, many companies are deciding to adopt hybrid work models if they reopen their offices or are settling for a remote workforce.

Because of a distributed work environment, the cybersecurity risks for remote employees increase in number and scale. Remote employees who use their home networks have [a much greater chance](https://www.forbes.com/sites/hillennevins/2021/05/19/new-dangers-of-working-from-home-cybersecurity-risks/?sh=5cce066e22fb) of becoming victims of security breaches. Traditional office settings ensure that in-person employees are protected, but it's challenging to guarantee protection for remote employees. Our [remote working checklist](https://www.cm-alliance.com/en-gb/remote-working-cybersecurity-checklist) is a good place for companies to start when it comes to protecting remote workers and the business itself in a remote environment.

## 2. Emerging 5G Applications:

When 5G was ushered in this past year, many industries were looking to benefit from its uses, whether it's cell phone companies offering it to their customers or manufacturers looking to improve operational efficiency. 5G will increase [the speed and responsiveness](https://www.com-power.com/blog/5g-networks-and-effects-on-radiated-emissions-and-emi-shielding) of wireless communications, and the future is looking bright for the new technology. However, new technologies come with new risks to address, and cybersecurity professionals need to look for potential threats against these evolved networks.

## 3. Blockchain and Cryptocurrency Attacks:

The world of blockchain and cryptocurrency is growing rapidly and attracting more interest that ever. As crypto transactions are digital, it's only natural that cybersecurity measures need to be taken to protect against instances of identity theft, security breaches, and other potential threats.

The last thing an investor, a crypto exchange or a company dealing with blockchain or cryptocurrency wants is for any information to become compromised. Companies must, therefore, look at seriously investing [in their IT infrastructure](https://www.jigsawacademy.com/blogs/cyber-security/challenges-of-cyber-security/#Blockchain-and-Cryptocurrency-Attacks) and protecting themselves in the event of a cybersecurity attack.

## 4. Internet of Things (IoT) Attacks:

For those unaware of the Internet of Things (IoT), it's essentially the interconnection of physical objects using various sensors that communicate with each other. As more data is transmitted between devices, gaps may exist, which leaves room for hackers or other cybercriminals to exploit information. While connected devices are known for their convenience and intelligence, it's clear that it opens up more opportunities for cybercriminals to take advantage of networks. Companies need to stay ahead of the curve by implementing a stable cybersecurity infrastructure and dedicated IT department as the world becomes increasingly interconnected.

## 5. Phishing Scams:

Though more people are becoming digitally literate, phishing is still a threat for cybersecurity professionals globally. For example, the COVID-19 vaccine has sparked an [uptick in potential phishing attacks](https://securityintelligence.com/articles/cybersecurity-trends-and-emerging-threats-2021/), making it a challenge to look out for in the latter half of 2021. There have been reports of fake vaccination emails going around, and unfortunately, online users are still falling victim to phishing scams. Companies can protect their employees by implementing access control guidelines, even when they're working from home. Cybersecurity training and awareness also emerges as a critical component when it comes to protecting the business from phishing scams.

## Consequences of Cyber attacks:

Cyber attacks can cost organisations billions of pounds and cause severe damage. Impacted organisations stand to lose sensitive data, and face fines and reputational damage. Cyber threats are a big deal. Cyber attacks can cause electrical blackouts, failure of military equipment, and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. It’s not an exaggeration to say that cyber threats may affect the functioning of life as we know it. The threats are growing more serious, too. Gartner explains, “Cybersecurity risks pervade every organization and aren’t always under IT’s direct control. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day. Increased cyber risk is real but so are the data security solutions.”

**Managing Cyber security:**

Effective cyber security management must come from the top of the organisation. A robust cyber security culture, reinforced by regular [training](https://www.itgovernance.co.uk/cybersecurity-training), will ensure that every employee recognises that cyber security is their responsibility and defaults to security instinctively. Good security and effective working practices must go hand in hand.

#### **1. Monitor the risk environment:**

Risk professionals should continuously monitor potential risks and explore new trends as they arise to determine what will be most likely to impact the organization. Quantify exposures and vulnerabilities on a big-picture scale to create a thorough understanding of the risk environment.

New cyber risk factors could include a change in common hacker strategies, a newly identified gap in the security system, or an updated technology that leaves current systems out-of-date.

There are many ways to manage cyber risks. Risk teams must decide how to handle each one:

* Avoidance means they will not partake in that activity as it is viewed to be too risky
* Acceptance, or understanding it is inevitable, and potential benefits outweigh the risks
* Control through implementing mitigation strategies to reduce the frequency or severity of an occurrence
* Transfer is available through cyber liability insurance, a new trend soon expected to be as popular as general liability insurance. These policies may cover interruption and recovery costs, liability claims, cyber theft and extortion costs, and more. Allianz Group’s [Guide to Cyber Risk](https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf)discusses cyber risk policies in detail.

#### **2. Monitor data assets:**

With the help of their team, risk professionals should identify the most valuable data assets stored in their system and monitor them regularly. Confidential information such as credit card information or trade secrets are more likely to be the target of a cyber attack, so these items should be guarded closely.

#### **3. Create a risk plan:**

The organization must develop response and continuity plans for cyber risk scenarios by brainstorming potential situations and determining a course of action for each one. It’s important to remember that with cyber issues or attacks, one problem can impact the entire organization, so be sure to incorporate multiple departments into the plan.

When the cyber risk plan has been created, it must be written down and communicated to all employees. There is no point in developing these procedures if they are not formally implemented throughout the organization and their importance stressed. Cybersecurity and risk mitigation must become an integral part of the organization’s culture and values.

#### **4. Gain management support:**

Top management must be on board with risk management activities. With the active threat that cyber risk presents, this shouldn’t be difficult to accomplish. They should embody the secure practices set out by the risk management team to send the message to employees that appropriate behaviour is expected.

#### **5. Prepare employees:**

It’s important to stress that cyber risk is not solely the responsibility of the risk department or IT. The risk management function should no longer be siloed; all departments should be encouraged to contribute.

All employees should be trained and educated to act in the most appropriate ways regarding cyber risks. The risk team should actively create awareness for issues and promote a safety culture. The cyber risk protocol should be well defined, as well as the human factor of cyber risk: many breaches come from an internal source, whether from an accidentally created vulnerability or intentional malicious action.

One common issue that stems from employees is social engineering, which uses strategies such as phishing to trick people into revealing confidential information. [More information on types of social hacking and preventing it can be found here.](https://www.intego.com/mac-security-blog/social-hacking/) Working with employees on cybersecurity reduces the potential occurrence of both of these issues.

#### **6. Build strong external relationships:**

If something does go wrong, the organization needs appropriate relationships with response teams. Public relations, media, and lawyers may be crucial in responding to a cyber attack or data breach and its aftermath. While data sharing with external parties is necessary and beneficial for almost all organizations, this does present an additional risk. The risk team should ensure that they are not over-reliant on external parties. Further, before sharing any type of data with a third party, perform due diligence on their privacy, security, and technology standards to ensure that they can be trusted with confidential information. Certifications, contracts, and other information should be acquired.

Cloud-based solutions are typically more secure than traditional storage systems (Read: [Cloud Storage is Much More Secure Than You Think](https://www.forbes.com/sites/quora/2017/09/18/cloud-storage-is-much-more-secure-than-you-think/#2ea895027403), by Forbes), but in risk management, one must always be cautious.

#### **7. Enforce security protocols:**

End-to-end security should be installed on all devices. Create and enforce password policies across the organization, with a required level of security and change frequency. If employees use their own devices to complete work from off-site, ensure that this data is also password-protected and encrypted.

Ensure that all data is regularly backed up and that all off-site back-ups are complete and up-to-date. This will ensure that if a cyber attack happens, valuable data won’t be lost.

When possible, consolidate systems and information into one source. If information is scattered across multiple locations, it will be much harder to protect and monitor. Simplifying the system can also create efficiencies for the IT team, allowing them more time to focus on actively reducing cyber risk

#### **8. Evolve with the technological environment:**

Technology is constantly changing, and systems must evolve to keep up with it. Risk teams should consider industry standards, competitors, and internal needs when deciding to implement new technology. While large pieces of equipment obviously cannot be replaced with every new iteration, they should still be updated and maintained to ensure they remain up to standard. An old, weak system is an excellent target for hackers.

Cyber risk is one of the most prevalent threats in any industry today; it’s no wonder that risk professionals are concerned about it. (For more details, next week we'll be publishing a blog post on the three main reasons to manage cyber risk). However, with careful thought and action, the risk can be reduced to a manageable level. Many hackers look for easy targets when planning their next attack, so if an organization is reasonably protected, there is a reduced risk of being a victim.

**How to approch Cyber security:**

A risk-based approach to cyber security will ensure your efforts are focused where they are most needed. Using regular [cyber security risk assessments](https://www.itgovernance.co.uk/cyber-security-risk-assessments) to identify and evaluate your risks is the most effective and cost-efficient way of protecting your organisation.

The [Institute of Risk Management](https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/) defines a cyber risk as “any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems”. [Gartner](https://www.gartner.com/en/information-technology/glossary/it-risk) gives a more general definition: “the potential for an unplanned, negative business outcome involving the failure or misuse of IT.”

Examples of cyber risk include:

* Theft of sensitive or regulated information
* Hardware damage and subsequent data loss
* Malware and viruses
* Compromised credentials
* Company website failure
* Natural disasters that could damage servers

When taking stock of cyber risks, it’s important to detail the specific financial damage they could do to the organization, such as legal fees, operational downtime and related profit loss, and lost business due to customer distrust.

**Cyber security checklist:**

Boost your cyber defences with these must-have security measures:

### **1. Staff awareness training:**

Human error is the leading cause of data breaches. It is therefore essential that you equip staff with the knowledge to deal with the threats they face.

[Staff awareness training](https://www.itgovernance.co.uk/staff-awareness) will show employees how security threats affect them and help them apply best-practice advice to real-world situations.

### **2. Application security:**

[Web application vulnerabilities](https://www.itgovernance.co.uk/web-application-penetration-testing) are a common point of intrusion for cyber criminals. As applications play an increasingly critical role in business, it is vital to focus on web application security.

### **3. Network security:**

Network security is the process of protecting the usability and integrity of your network and data. This is achieved by conducting a [network penetration test](https://www.itgovernance.co.uk/external-network-penetration-test), which assesses your network for vulnerabilities and security issues.

### **4. Leadership commitment:**

Leadership commitment is key to [cyber resilience](https://www.itgovernance.co.uk/cyber-resilience). Without it, it is tough to establish or enforce effective processes. Top management must be prepared to invest in appropriate cyber security resources, such as awareness training.

### **5. Password management:**

Almost half of the UK population uses ‘password’, ‘123456’ or ‘qwerty’ as their password. You should implement a password management policy that provides guidance to ensure staff create strong passwords and keep them secure.

**Challenges of Cyber security:**

Given the rapidly evolving technological landscape and the fact that adoption of software is ever increasing across various sectors including finance, government, military, retail, hospitals, education, energy to name a few, more and more information is becoming digital and accessible through wireless and wired digital communication networks and across the omnipresent internet. All this highly sensitive information is of a great value to criminals and evil doers which is why it is important to protect it using a strong cyber security measures and processes.

The importance of good cyber security strategies is evident in the recent high-profile security breaches of organizations such as Equifax, Yahoo, and the U.S. Securities and Exchange Commission (SEC), who lost extremely sensitive user information that caused irreparable damage to both their finances and reputation. And as the trend suggests, the rate of cyber-attacks show no sign of slowing down. Companies, both large and small, are targeted everyday by attackers to obtain sensitive information or cause disruption of services.

The same evolving technological landscape also poses challenges in implementing effective cyber security strategies. Software constantly changes when its updated and modified which introduces new issues and vulnerabilities and opens it up for various cyber-attacks. Furthermore, IT infrastructure evolves as well with many of the companies already migrating their on-premise systems to the cloud which introduces a whole new set of design and implementation issues resulting in a new category of vulnerabilities. Companies are unaware of the various risks within their IT infrastructure and hence fail to have any cyber security countermeasures in place until it’s far too late.

**Cyber security in Pakistan:**

“The art of war” is an ever-changing phenomenon and a process as to how, when and where to engage the enemy. Globally a relatively newer threat is evolving not only for states but also for the private profit driven world. Billions of dollars are illegally transferred or stolen, privacies exposed, state secrets acquired and critical public infrastructure hacked. This is the realm of cyber security. As the world becomes more and more connected via internet or digitized through information technology, the cyber security threats are increasing day by day. Pakistan is no exception to it. A nuclear state with an important geopolitical position is increasingly exposed to such threats in the cyber realm. So are the business sector and the private work. Pakistan has a large internet users’ base, an increasing digitized security apparatus as well as banking system, which depend on internet connectivity. Pakistan has also incorporated laws to tackle threat emanating from cyber- attacks, which do not seem to cover the threats in depth and wholeness. As threats evolve and come from varied foes and adversaries, we must continuously assess them and make necessary modification and rectifications in our strategy. In this perspective, the study assesses Pakistan’s cyber space, identify threats and make recommendations to eliminate those threats. It further discusses Pakistan’s legal development on the subject and the way forward.

# **Pakistan government approves new cybersecurity policy, cybercrime agency**:



The Pakistan Ministry of Information Technology has announced that a new cybersecurity policy and accompanying cybersecurity agency has been approved for the South Asian nation. The new policy aims to support both public and private institutions, including national information systems and [critical infrastructure](https://portswigger.net/daily-swig/critical-infrastructure), replacing a system whereby government institutions have separate security operations. It comes at a delicate time for Pakistan, which [recently accused India of using the Israeli spyware](https://www.reuters.com/technology/pakistan-seeks-un-probe-indias-use-pegasus-spyware-2021-07-23/) Pegasus to spy on Prime Minister Imran Khan – and designates cyber-attacks on any Pakistani institution as an attack on national sovereignty. “The IT ministry and all relevant public and private institutions will be provided all possible assistance and support to ensure that their data, services, ICT products and systems are in line with the requirements of cybersecurity,” said IT minister Syed Aminul Haq, as quoted in [local](https://www.dawn.com/news/1637334) [press](https://www.dawn.com/news/1637334).

**Conclusion:**

Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too. If you want to learn more about what is cyber security and how to deal with cyber criminals hop into our [courses section](https://www.bitdegree.org/tag/it-security-software/cyber-security) and become a hero in the digital platforms.