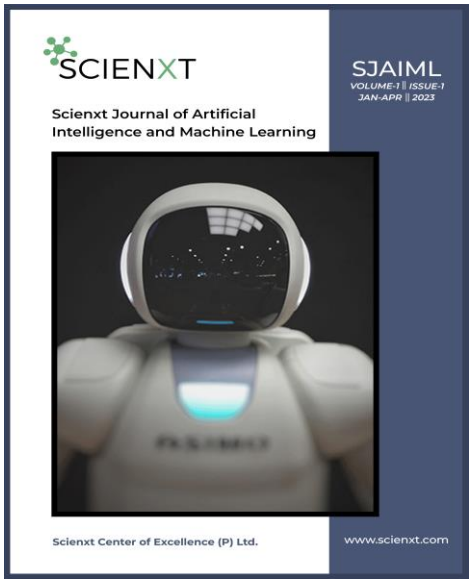

Scienxt Journal of Artificial Intelligence and Machine Learning
Volume-1|| Issue-1||Year-2023|| Jan-Apr || pp. 19-32

A study of Cyber Security-management and challenges in implementation in organizations

Narasimha Rao*[1], Supriya Raju[2]

[1,2]*Assistant Professor, Dept. of Computer Science, SVEC, Vishnupur, Bhimavaram, West Godavari District, Andhra Pradesh, India.*
Email-nsrao491@yahoo.co.in

Corresponding Author: Narasimha Rao

Abstract:

Any company that does not have robust security policies and processes in place is taking on a significant amount of unnecessary risk. If that organisation does not have security standards similar to these, then the essential data that is associated with that corporation is not secure. Access control and Password Security, authentication of data, malware scanners, firewalls, encryption, and digital signatures are some measures that are currently being utilized by organizations for the management of cybersecurity. However, these various information security standards currently available on the market each have their own unique set of challenges that they need to overcome to succeed. These challenges include a lack of infrastructure, continuous changes in threat patterns, and changes and upgrades in IT systems.

Keywords:

Cyber security, cyber threats, IT systems, Access Control, Password Security, Automated Teller Machines

1. Introduction:

Information and communication technology is undergoing a worrisomely swift increase in terms of how it should be handled in order to satisfy critical growth of organizations, and this problem is especially widespread in countries that have not yet reached their full potential [1]. The utilization of the worldwide network of networks that is referred to as the Internet as well as the Worldwide Web that is referred to as www, with everything in cyberspace being associated with one another. Cyberspace, the up-and-coming trend in today's global society, is a phenomenon that can have both detrimental and positive effects on the lives of individual people depending on how they choose to interact with it. To this day, there is no definition of cyberspace that is universally accepted and that takes into account the software domain, the hardware platform, the network of networks (the Internet), the servers, the Internet of Things (IoT), computing systems, cloud computing, informatization, big data technology, telecommunications, mobile computing, nations, corporations, and people. This is because there is no definition of cyberspace that takes into account all of these factors. This is due to the fact that there is currently no definition of cyberspace that takes all of these aspects into consideration. It takes into account everything that takes place with the activities that are carried out in the cloud and takes into account everything that takes place. This strategy has spread to practically every field in which humans participate in activities or interact with one another, including but not limited to e-health, teleconferencing, e-commerce, e-learning, e-transportation, smart homes, smart cities, education, governance, administration, management, agriculture, and e-banking [1]. The collection of measures that must be taken to prevent unauthorised users from accessing digital information and computer networks is referred to as "cyber security". Any company that does not have robust security policies and processes in place is taking on a significant amount of unnecessary risk. If that organisation does not have security standards similar to these, then the essential data that is associated with that corporation is not secure. The framework that was designed by the Payment Card Industry and Data Security Standard provides protection for a variety of payment methods, including credit cards, debit cards, and other payment methods. This structure was developed in order to guarantee the safety of financial transactions. When it comes to retaining access, the hacker who is already inside the target system is used to exploit vulnerabilities and crack passwords in order to maintain access. This is accomplished by taking advantage of weaknesses and using cracked passwords. In this day and age, the number of cybercrimes that are carried out each day is increasing, which results in an increased demand for increased network or even system security. Cybercrime is a term that refers to the commission of illegal activities via a computer

network. Since an increasing number of commercial processes are becoming automated and an increasing number of personal computers are being used to store vital information, the requirement for secure computer systems is becoming increasingly clear. As a direct result of this, worries about the security of networks have evolved into concerns about the security of the general public [2]. Because it has the capacity to protect both company and personal data, cyber security is an immensely essential topic to debate. When it comes to storing, accessing, and retrieving vital information, it is strongly recommended that all organisations that rely on digital data pay attention to cyber-security and implement some form of it. This is because cyber-security helps prevent unauthorised parties from accessing, storing, and retrieving vital information. This is due to the fact that cyberattacks can cause significant issues for organisations in a variety of different ways. An urgent requirement for new conceptual and analytical tools, as well as cyber-security research that focuses on the interaction of the technological and social components of the problem, is revealed by the study of technology security. In today's fast-paced world, ensuring the safety of one's digital possessions requires more than simply conquering challenges posed by technology. In order to recognise, evaluate, steer clear of, and react to a problem involving technology, it is necessary to disseminate knowledge that is technical as well as organisational in nature. This is due to the fact that any problem involving technology involves consideration of both kinds of information. When we refer to it, we are referring to an action or an occurrence that has the potential to allow unauthorised access to the system communication and information, as well as electronic communication networks. When we talk about it, we are referring to it as "it. "Control systems for electronic communication network operations or industrial processes that control actions to delete, erase, edit, or otherwise alter electronic information in any other way and restrict access to electronic information are both different names for the same thing. These two names are both used to refer to the same thing. Another name for this type of technology is "control systems for electronic communication networks" which is a phrase that describes its function. In addition to this, it either modifies the information that is stored electronically, restricts access to the information that is stored electronically, or removes access to the information that is stored electronically. All of these options are available. Additionally, it is feasible for unauthorised individuals to use information that has been kept in an electronic format and is not considered private. It is not possible to completely discount the likelihood of this happening [3].

2. Aspects of Cyber-Security:

A person can transmit and receive any kind of data, such as an email, audio or video file, with the simple push of a button in today's world. This includes sending and receiving emails. However, have they ever given any thought to how safe it is to deliver his data ID or transfer it to the other person safely without any information leaking? If so, it is important to know that they have. There is a possibility that the answer lies inside the realm of cyber security. The infrastructure in modern life that is now expanding at a rate that is considered to be the fastest is the Internet. The current technological environment is one that is favourable to the development of a great deal of cutting-edge technology, which is in the process of modifying the way in which humans appear. However, because of these evolving technologies, we are not able to protect our private information in a manner that is particularly effective, and as a direct result of this inefficiency, the rate of cybercrime in our modern times is increasing on a daily basis [4]. Because more than sixty per cent of all commercial transactions that take place today are carried out over the Internet, it is necessary for this sector to maintain a high level of security in order to facilitate the most transparent transactions possible and the transactions that yield the best results. As a direct consequence of this, the subject of internet safety is becoming an increasingly pressing one. The scope of cyber security includes not only the protection of information in the information technology industry but also the protection of information in a very large number of other domains, such as cyberspace and other domains related to information technology. Even the most cutting-edge technologies, such as mobile computing, e-commerce, online banking, and cloud computing, necessitate a significant level of protection. Because these technologies save a substantial amount of information about a person, it has become an imperative necessity to utilise them in a secure manner. Enhancing a nation's cyber defences and bolstering its ability to defend its important information infrastructures are both essential to the nation's security and economic well-being. Over the course of the past few years, cyber attacks have become increasingly sophisticated. Making the internet a safer place overall and protecting the individuals who use the internet has become an integral part of the procedure for developing new services and of the policy of the government. In today's world, there are a number of countries and governments that implement rigorous regulations on electronic security in order to prohibit the leakage of critical information. The goal of these policies is to prevent the disclosure of sensitive information. To what extent, on the other hand, are we as people, governments, or members of the international community aware of the threats that are posed by cyberspace, and are we appropriately prepared to foil their use in communication, business, and even conflict? To be more explicit, despite the increasing

number of people who use it, the Internet is still unregulated or only subject to a small amount of control. This is the case despite the fact that the number of people who use it continues to expand. In this day and age, there are dangers and challenges created by the absence of proper security measures in cyberspace. Cyberspace is the digital equivalent of the physical world [4].

Table.1: Adopted from Solihat and Wulansari (2021)

No.	Source	Devices	Cybercrime in the IoT
1	Network Wireless	Wireless network router, access points, sensor network	Unauthorized access and data modification
2	Network parameter devices	Firewalls, servers	Unauthorized access
3	Web	Web servers, web clients, and social networks	Copyright or intellectual property infringement, cyber defamation
4	Cloud	Cloud systems	Data theft
5	End nodes	Game consoles, mobile devices, smart TV's, readers	Distribution of malware, data theft, spamming from the crimes in the IoT

Solihat and Wilansari (2021), outlined the above-listed critical aspects of cybersecurity in table.1

3. Dealing with cyber security issues:

Utilizing newly developed approaches opens the door to the possibility of a rise in the total number of cyberattacks launched against cyberspace. Cybercriminals often change the malware signatures they use in order to take use of newly revealed technical flaws. This allows them to take advantage of newly identified vulnerabilities in software and hardware. In certain instances, they are searching for one-of-a-kind qualities of emerging technologies with the intention of locating weaknesses that can be exploited by the installation of malware. In order to gain access to a large number of people in a quick and efficient manner, criminals operating online are making use of newly emerging Internet technologies, as well as the millions and

billions of individuals who use the Internet on a regular basis [5]. Criminals are also taking advantage of the fact that there are millions and billions of people who use the Internet regularly. [5].

3.1. Access Control and Password Security:

An easy approach of providing security for the information in order to retain users' privacy is to provide protection for private information through the utilisation of a username and password. This protects the information from unauthorised access. Implementing this way of providing protection is one of the most critical actions that must be taken to assure the user's safety when using the internet.

3.2. Authentication of Data:

The data that is being transferred won't be deemed valid unless it can be demonstrated that it came from a trustworthy source and that it has not been altered in any way. Until this can be done, the data won't be considered authentic. The validity of these documents is typically checked by utilising a present that is provided by the hostile virus software package that is already installed on the PCs. In order to safeguard devices from infections, having anti-virus software that is actually effective against viruses is more crucial than having just any old anti-virus software.

3.3. Malware Scanners:

A software system that occasionally examines all files and documents for malicious code or harmful viruses inside the system malware scanners are software systems that examine all files and documents for malicious code or harmful viruses. Malware scanners are software programs that do random checks on all of a computer's files and documents to determine whether or not they contain malicious code. When it comes to dealing with samples of malicious software systems, the most prevalent types of harmful software are viruses, worms, and Trojan horses. These three categories of malicious software are utilised as sorting and identifying criteria in this industry.

3.4. Firewall:

A firewall is a software or hardware package that helps prevent harmful software, such as viruses, worms, and hackers, from entering your computer when it is linked to the internet. Firewalls are also known as intrusion prevention systems (IPS) and perimeter defence systems (PS). The firewall examines each and every incoming message, and it will either discard or

reject any messages that do not meet the security criteria that are compatible with the other messages[5].

3.5. Encryption:

Data that has been encrypted cannot be decoded without first applying the appropriate key in order to unlock it. This is because the key is used to unlock the data. In order to circumvent encryption, it would be essential to find a solution to challenging mathematical issues, such as the creation of enormous prime numbers; however, this would require an incredible amount of time and effort to accomplish. Because it uses the same key for both encoding and decoding messages, symmetric encryption offers a level of security that is comparable to that supplied by the key. This is because the key is used for both encoding and decoding the messages. As a consequence of the key being disseminated to more people, there will be openings in the security of the system that could be exploited. When adopting asymmetric encryption, the message is encrypted using a public key, while the identical message is decrypted using a private key. Asymmetric encryption is used in the great majority of modern security protocols to facilitate key distribution [6]. This is because asymmetric encryption is easier to implement.

3.6. Digital signatures:

It is possible to generate a digital signature by employing the identical mathematical processes that are used to generate an asymmetrically encrypted message. It is always possible for a user to demonstrate that he is the owner of a private key by requesting that some data be encrypted with the key in question. If you possess the public key that validates the credentials of the person, then anyone will be able to decrypt the same information for you. This approach is, in essence, the exact reverse of the public-key encryption method, and, like the public-key encryption method, it functions on the assumption that the authorised user only possesses the private key [6].

Apart from these techniques, another study stated that a major rise in collaboration and coordination not just between but also inside nation-states is another crucial component of cyber security. This is especially true between the various branches of the military, the commercial sector, and academic institutions. Academics already play a crucial role in the field of cyber security; nevertheless, companies and governments typically stifle the efforts of academics since these institutions view academics as a threat rather than an asset when it comes to cyber security. This is something that needs to change, and the cyber community as a whole needs to be more open to any research or experimentation that leads to a deeper knowledge of

cyber vulnerabilities and gaps in security systems. In particular, the general population is frequently overlooked, despite the fact that it may play a crucial role in defending against cyberattacks. This is despite the fact that it is generally disregarded. Sharing information on the most recent assaults, malware signatures, and vulnerabilities will be important for governmental entities, private companies, and academic institutions to comply with [7].

4. Multilevel approach to cyber security:

A research suggested a multilayer method to risk assessment, which is based on a set of security metrics and techniques for their computation. This approach was developed in response to the need for more accurate risk predictions. This strategy is predicated on the concept that distinct degrees of risk can be evaluated in isolation from one another. The proposed tactics are built on top of attack graphs and service dependencies as its underlying structure. They make it possible to evaluate the security of network topologies, the characteristics of potential threats and attacks, as well as integral security properties and characteristics that are computed on the basis of a cost-benefit analysis and zero-day vulnerability study. In addition, they make it possible to assess the integrity of the security properties and characteristics that are evaluated. The categorization of these qualities and the separation of the security information into static, dynamic, and historical categories makes it feasible to define separate evaluation levels. These categories also make it possible to define distinct evaluation levels [8].

According to a study in order for organisations to manage projects in a secure manner, the multilevel security basics should be applied to the project management process groups of the organisation. This will ensure that not only is the project provided securely, but also that it is completed on schedule, without exceeding the budget, and according to the requirements of the client. Prior to the occurrence of any security risk or threat is the most effective time to address security concerns; as a result, a project manager should develop a security programme with the assistance of a security professional in order to reduce security risks as early as possible in the lifecycle of the project. This will allow for the greatest reduction in security risks. This can be achieved by making certain that CIA is preserved throughout the course of the process of managing the project. As a consequence of this, it is imperative to take into account every aspect of security in order to minimise the likelihood of failure and cut down on the costs associated with overhead. This article is a description of a framework that centres attention on the deliverables associated with security. This is a framework that project managers can use to identify problems and communicate those concerns to any and all members of the team as well

as any stakeholders. This framework can be utilised by a project manager right away, beginning with the initiation phase and continuing all the way through the close phase, for the aim of expediting the execution of initiatives having to do with cyber security [9].

A study emphasized that practically all companies use web apps to protect themselves against security breaches and for day-to-day operations in their businesses. Conventional security measures are abundant and may be purchased from a variety of suppliers; but, putting these precautions into action can be challenging, which leaves a system open to attack by malevolent actors. A technique that defends against bots or scripts by utilising many layers protects both the server and the application from the additional load that is caused by the malicious software. The research also discovered that traditional methods always follow the same pattern in order to gain access to the resources of organisations, and that attackers either intentionally or unintentionally prepare scripts or bot programmes in order to slow down the application and sometimes attempt to steal data from the organisations in order to gain access to its resources. Data is the weapon in this day and age, and every firm is doing everything in its power to protect its data by utilising a wide array of strategies and methods. A multilayer method not only protects an application from unwanted requests made on the server, but it also protects data by adding an extra layer of security for the software that is running on the server side [10].

5. Challenges in implementing cyber security:

According to the findings of a recent study, the various information security standards that are currently available on the market, such as ISO/IEC 27001, Common Criteria, and System Security Engineering-Capability and Maturity Model, each have their own unique set of challenges that they need to overcome in order to be successful. The issues that have been highlighted constitute a barrier that may prohibit businesses from adopting an effective security strategy to secure their information and online services. This barrier may prevent the development of an appropriate security plan. The author emphasised that the review process of such a system consumes a large amount of time, and that this is a key point in their argument. Despite the fact that utilising Common Criteria to assess the safety of items related to information technology can be of tremendous help to the process, this is not the case. There is not enough time in the day for companies to devote resources to tasks such as defining the protection profile of the CC, waiting for vendors to prepare their target of evaluation, and then asking a testing laboratory to accredit the product in question [11]. This is because e-business is inherently dynamic; as a result, companies do not have the luxury of waiting around for

opportunities to present themselves. Research also shows that infrastructural challenges include network failure and infrastructural deficiency. Other examples of this type of challenge include debiting by Automated Teller Machines (ATMs) without disbursing cash to beneficiaries, problems not being quickly rectified by the banks, and charging by banks for the use of electronic banking methods. Each and every one of these concerns brings up important questions. Customers' faith in the monetary system suffers as a direct result of this, which in turn leads to an increase in fraudulent conduct and cybercrime [12]. It has been proposed that in order for a cashless policy to be successful, banks ought to be obligated to supply at least the bare minimal amount of infrastructure that is required. This is because cash is easier to counterfeit than other forms of payment. In addition, the government and the institutions of the financial sector need to collaborate in order to come up with adequate precautions against cybercrime. According to the findings of a study, there are a number of obstacles that need to be conquered in order to improve the level of trust that end users have in regard to ICT systems. These obstacles have been identified as having to be overcome in order to improve the level of trust that end users have. It has been determined that these obstacles need to be conquered in order to increase the amount of trust that end users have. All of these issues are linked to the cyber security threats that continue to surface on a regular basis, and they are all interconnected. These issues have been arranged into categories and investigated using primary research trends, which include dynamic risk management, attack and defence graphs, event correlation, and information exchange [13]. One piece of research came to the conclusion that the size of an organisation, the complexity of the threat situation, and the level of risk that is involved all play a role in determining whether or not it makes sense to establish a specialised cybersecurity management system with one's own full-time personnel. This conclusion was reached based on the findings of the study. Examining the level of danger that is present is one way to find out the answer to this question. Every choice that can be made comes with its own individual set of advantages and disadvantages. The capacity to concentrate attention on a particular topic and the full-time dedication of individuals who are active in security are two of the most important factors that contribute to the success of a specialized cyber security management system. Both of these factors are essential to the success of the system. One of the less desirable characteristics of this method is the fact that it leads to greater expenditures. This is one of the reasons why. An in-depth and objective examination of an organization's organizational structures, operational procedures, and culture of internal security should be carried out by businesses that want to dramatically improve the quality of their cybersecurity. Making use of

a checklist is an excellent technique for getting started in the process of determining where change is required and to what extent change is required. [14].

6. Conclusion:

Access Control and Password Security, Authentication of Data, Malware Scanners, Firewall, Encryption and Digital signatures are some measures that currently being utilized by organizations for management of cybersecurity. However, these various information security standards that are currently available on the market each have their own unique set of challenges that they need to overcome in order to be successful. These challenges include, lack of infrastructures, continuous changes in threat patterns and changes and upgrades in IT systems. This is just one of the causes. Businesses that want to significantly improve the quality of their cybersecurity should conduct a thorough and unbiased analysis of their organisational structures, operational processes, and culture of internal security. Making use of a checklist is a great way to get started in the process of identifying the areas and the degree of change that are necessary.

7. References:

(1) Sawaneh, Ing Ibrahim. (2019). The Role of Cyber Security in Minimizing Crime Rate in Post 2018.doc.

(2) Tomar, Sachin. (2021). Cyber Security Methodologies and Attack Management. Journal of Management and Service Science (JMSS). 1. 1-8. 10.54060/JMSS/001.01.002.

(3) M Solihat and R V Wulansari 2021 IOP Conf. Ser.: Mater. Sci. Eng. 1158 012017

(4) Abdou Hussien, A. (2021) Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1). Journal of Information Security, 12, 56-78. doi: 10.4236/jis.2021.121003.

(5) K. M Rajasekharaiah1, Chhaya S Dule2 and E Sudarshan, 2020 IOP Conf. Ser.: Mater. Sci. Eng. 981 022062

(6) Omkar Veerendra Nikhal "An Analytical Study on Attacks and Threats in Cyber Security and its Evolving Trends on Modern Technologies" Published in International Journal of

Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.1230-1235, URL: www.ijtsrd.com/papers/ijtsrd38195.pdf

(7) Naha, Alik. "Emerging Cyber Security Threats: India's Concerns and Options". International Journal of Politics and Security (IJPS), Vol. 4, No. 1, 2022, pp. 170-200, DOI:10.53451/ijps.996755

(8) Kotenko, I., & Doynikova, E. (2014). COMPREHENSIVE MULTILEVEL SECURITY RISK ASSESSMENT OF DISTRIBUTED INFORMATION SYSTEMS. International Journal of Computing, 12(3), 217-225. https://doi.org/10.47839/ijc.12.3.602

(9) Bhardwaj, B. (2019). Project Management: Changing the way Cyber Security works in an organization; presented at the 13th Annual UT Dallas Project Management Symposium, Richardson, Texas, USA in May 2019; published in the PM World Journal, Vol. VIII, Issue IX, October

(10) Subhranshu Mohanty. (2021). Introducing Multi Level Security in Web Applications. SPAST Abstracts, 1(01). Retrieved from https://spast.org/techrep/article/view/300

(11) Alqatawna, Ja'far. (2014). The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises. Journal of Software Engineering and Applications. 7. 883-890. 10.4236/jsea.2014.710079.

(12) H. Abdulazeez, S. Magaji, and I. Musa, "Analysis of Infrastructural Challenges, Cybercrime, and the Cashless Policy in Nigeria: Infrastructural Challenges, Cybercrime, and the Cashless Policy", ARIS2-Journal, vol. 2, no. 1, pp. 13–27, Aug. 2022.

(13) Félix Gómez Mármol, Manuel Gil Pérez, Gregorio Martínez Pérez. I Don't Trust ICT: Research Challenges in Cyber Security. 10th IFIP International Conference on Trust Management (TM), Jul 2016, Darmstadt, Germany. pp.129-136, 10.1007/978-3-319-41354-9_9. hal-01438353

(14) Pedro Ramos Brandao. Bases, Challenges, and Main Dangers for Deploying Cyber security in Industry 4.0. Advances in Wireless Communications and Networks. Vol. 5, No. 1, 2019, pp. 33-40. doi: 10.11648/j.awcn.20190501.15

Technology Innovations That Will Impact Cybersecurity in the Future

Artificial Intelligence: As we move forward into the future of automation, AI is proving to play a critical role in the realm of both cyber and cloud security. The ability to learn at the rate of AI makes it extremely important to prioritize discovering the ways that AI can assist security. It's also important to start standardizing the proper usage of AI, ensuring that businesses are prepared for its continued growth.

Blockchain/Distributed Ledger: Blockchain improves cloud security by improving data security, specifically the confidentiality (privacy), integrity and availability of data. Depending on the Blockchain solution and technology used, you can set the needed security levels for the system as a whole, as well as the individual record level as needed. Because cloud computing often involves the outsourcing of trust to a provider (that runs your IT infrastructure, stores your data, etc.), new ways of ensuring data security are needed.

High-Performance Computing: **'**Vanilla' cloud environments were typically not made to handle harsh environments like that of High-Performance Computing (HPC) Cloud Security. With the current trend of HPC workloads and infrastructure increasingly becoming cloud-like (e.g., resource pooling, rapid elasticity, on-demand self-service) or interacting with the cloud (e.g., bursting), security will become a great concern at an accelerating rate.

Industrial Control Systems: As Industrial Control Systems (ICS) advance from communicating with networks within the enterprise to interacting externally via IoT platforms and the cloud, their efficiency, effectiveness and scalability have improved. However, these advances create additional complexity and a larger attack surface, which in turn has increased the opportunity for cyber-attacks.

Internet of Things (IoT): Internet of Things (IoT) devices represent a wide variety of non-traditional devices such as medical devices, cars, drones, simple sensors and more. These unique devices often pose a security challenge due to their limited size and lack of innate security, making them difficult to secure with traditional security controls and methodologies. It is a combination of these factors that have rendered many devices vulnerable to attacks like the Mirai botnet.

Quantum Computing: Researchers worldwide are working to make quantum computing a reality. Microsoft, Google, IBM, Intel, and many governments are working on building the first large-scale quantum computer. Particular types of quantum computers, armed with a mathematical algorithm known as Shor's algorithm, can quickly factor math equations that involve large prime numbers.

Equations involving large prime numbers are what gives most traditional public key cryptography its protective capabilities, since traditional binary-based computers cannot easily factor large prime number equations. Quantum computers with enough "qubits" can factor large prime number equations in a very short amount of time, measured in minutes to days. This means that soon, a quantum computer will be able to break present-day cybersecurity infrastructure. We need to start preparing now.

Zero Trust: Zero Trust is one of the most widely talked about cybersecurity trends today. Zero Trust says no part of a computer and networking system can be implicitly trusted, including the humans operating it. Therefore, we must put measures in place to provide assurance that the systems and their components are operating appropriately, typically under a "least privilege" model and continuously verified.

Reference: https://cloudsecurityalliance.org/blog/2022/03/27/7-technology-innovations-that-will-impact-cybersecurity-in-2022-and-beyond/