International Journal of Research and Development in Pharmacy & Life Sciences

Review Article Open Access

# Cyber Security in Pharmaceutical Industry

**Rushil Prajapati***

*Department of Pharmacy Practice, Dr. DY Patil Institute of Pharmaceutical Sciences and Research, Pimpri, Pune, India*

## Abstract

Cyber Security plays an important part in the field of information technology. Securing the information have come one of the biggest challenges in the present day. Whenever we suppose about the cyber security the first thing that comes to our mind is' cyber crimes' which are adding immensely day by day. colorful Governments & companies are taking numerous measures in order to help these cybercrimes. Besides colorful measures cyber security is still a veritably big concern to numerous. This paper substantially focuses on challenges faced by cyber security on the rearmost technologies. It also focuses on rearmost about the cybersecurity ways, ethics and the trends changing the face of cyber security. Cyber security constitutes styles which are used to confine unauthorized access to data, networks and bias which safeguards tools and technologies want to store data. The content of that data and styles are concentrated by instructional security to guard information including sequestration, integrity and vacuity.

**Keywords:** Cyber security; Information technology; Cyber attack

## Introduction

Cyber security refers to the protection of information systems (hardware, Software and associated infrastructure), the data on them, and the services they provide, From unauthorized access, harm or misuse. This includes harm caused intentionally. When there is an unauthorized system/network access by a third party, we term it as a cyber-attack. The person who carries out a cyberattack is termed as a hacker/attacker. Cyber-attacks have several negative effects. When an attack is carried out, it can lead to data breaches, resulting in data loss or data manipulation. Organizations incur financial losses, customer trust gets hampered, and there is reputational damage. To put a curb on cyber-attacks, we implement cyber security. Cyber security is the method of safeguarding networks, computer systems, and their components from unauthorized digital access. Computer security, cybersecurity (cyber security), or information technology security (IT security) is the protection of computer systems and networks from attack by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide [1-3]. The field has become of significance due to the expanded reliance on computer systems, the Internet,[3] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance [1-4]. Moreover, in some accounts of the topic, cyberspace is best understood as a 'place' in which business is conducted, human communications take place, art is made and enjoyed, relationships are formed and developed, and so on. In this place, cyber-crime, cyber terrorism, and cyber war may occur, having both 'real' and 'virtual' impacts. Taken as a whole, the CyBOK delineates a large range of topics which appear to be within the broad scope of cyber security, even if a succinct reduction of those into a short definationremains elusive. The full scope of CyBOK may serve as an extended definationof the topic—as summarised next. Controls, and focus almost exclusively on information. Stretching them to relate to cyber physical systems may be taking them too far: indeed, our working definition above privileges the notion of information (whilst also mentioning services) — whereas in the case of network connected actuators, the pressing challenge is to prevent unwanted physical actions.

## History of cyber security

Since the Internet's arrival and with the digital transformation initiated in recent years, the notion of cybersecurity has become a familiar subject in both our professional and personal lives. Cybersecurity and cyber threats have been consistently present for the last 50 years of technological change. In the 1970s and 1980s, computer security was mainly limited to academia until the conception of the Internet, where, with increased connectivity, computer viruses and network intrusions began to take off. After the spread of viruses in the 1990s, the 2000s marked the institutionalization of cyber threats and cybersecurity. The April 1967 session organized by Willis Ware at the Spring Joint Computer Conference, and the later publication of the Ware Report, were foundational moments in the history of the field of computer security.Ware's work straddled the intersection of material, cultural, political, and social concerns. A 1977 NIST publication introduced the CIA triad of confidentiality, integrity, and availability as a clear and simple way to describe key security goals. While still relevant, many more elaborate frameworks have since been proposed. However, in the 1970s and 1980s, there were no grave computer threats because computers and the internet were still developing, and security threats were easily identifiable. Most often, threats came from malicious insiders who gained unauthorized access to sensitive documents and files. Although malware and network breaches existed during the early years, they did not use them for [5-7] financial gain. By the second half of the 1970s, established computer firms like IBM started offering commercial access control systems and computer security software

***Corresponding author:** Rushil Prajapati, Department of Pharmacy Practice, Dr. DY Patil Institute of Pharmaceutical Sciences and Research, Pimpri, Pune, India, E-mail: dramirthatom.in@gmail.com

**Received:** 01-June-2023, Manuscript No: ijrdpl-23-97230, **Editor assigned:** 03-June-2023, PreQC No: ijrdpl-23-97230(PQ), **Reviewed:** 17-June-2023, QC No: ijrdpl-23-97230, **Revised:** 21-June-2023, Manuscript No: ijrdpl-23-97230(R), **Published:** 28-June-2023, DOI: 10.4172/2278-0238.1000169

**Citation:** Prajapati R (2023) Cyber Security in Pharmaceutical Industry. Int J Res Dev Pharm L Sci, 9: 169.

products. One of the earliest examples of an attack on a computer network was the computer worm Creeper written by Bob Thomas at BBN, which propagated through the ARPANET in 1971. The program was purely experimental in nature and carried no malicious payload. A later program, Reaper, was created by Ray Tomlinson in 1972 and used to destroy Creeper. Between September 1986 and June 1987, a group of German hackers performed the first documented case of cyber espionage. The group hacked into American defense contractors, universities, and military base networks and sold gathered information to the Soviet KGB. The group was led by Markus Hess, who was arrested on 29 June 1987. He was convicted of espionage (along with two co-conspirators) on 15 Feb 1990. In 1988, one of the first computer worms, called the Morris worm, was distributed via the Internet. It gained significant mainstream media attention. In 1993, Netscape started developing the protocol SSL, shortly after the National Center for Supercomputing Applications (NCSA) launched Mosaic 1.0, the first web browser, in 1993. Netscape had SSL version 1.0 ready in 1994, but it was never released to the public due to many serious security vulnerabilities. These weaknesses included replay attacks and a vulnerability that allowed hackers to alter unencrypted communications sent by users. However, in February 1995, Netscape launched Version 2.0.

## Objectives of Cyber Security in Pharma Industry

### Confidential tool

Confidential VMs can protect the confidentiality of data in the cloud by encrypting data-in-use while it's being processed. Confidential VMs take advantage of security technology offered by modern CPUs (e.g., Secure Encrypted Virtualization extension supported by 3rd Gen AMD EPYC™ CPUs) together with confidential computing cloud services. Customers can be confident that their data will stay private and encrypted even while being processed.

### Tools for confidential

**a. Encryption**

Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key). It protects sensitive data such as credit card numbers by encoding and transforming data into unreadable cipher text. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the two primary types of encryption.

**b. Access control**

Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users need to present credentials before they can be granted access such as a person's name or a computer's serial number. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.

**c. Authentication**

An authentication is a process that ensures and confirms a user's identity or role that someone has. It can be done in a number of different ways, but it is usually based on a combination.

- Something the person has (like a smart card or a radio key for storing secret keys),
- Something the person knows (like a password),
- Something the person is (like a human with a fingerprint).

Authentication is the necessity of every organizations because it enables organizations to keep their networks secure by permitting only authenticated users to access its protected resources. These resources may include computer systems, networks, databases, websites and other network-based applications or services.

**d. Authorization**

Authorization is a security mechanism which gives permission to do or have something. It is used to determine a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. System administrators are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.

**e. Physical security**

Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

**f. Integrity**

Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.

### Tools for integrity

**a. Backups**

Backup is the periodic archiving of data. It is a process of making copies of data or data files to use in the event when the original data or data files are lost or destroyed. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy. Many applications especially in a Windows environment, produce backup files using the .BAK file extension.

**b. Checksums**

A checksum is a numerical value used to verify the integrity of a file or a data transfer. In other words, it is the computation of a function that maps the contents of a file to a numerical value. They are typically used to compare two sets of data to make sure that they are the same. A checksum function depends on the entire contents of a file. It is designed in a way that even a small change to the input file (such as flipping a single bit) likely to results in different output value.

**c. Data correcting codes**

It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

**d. Availability**

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools for Availability

- Physical Protections
- Computational Redundancies

**e. Physical protections**

Physical safeguard means to keep information available even in the event of physical challenges. It ensure sensitive information and critical information technology are housed in secure areas.

**f. Computational redundancies**

It is applied as fault tolerant against accidental faults. It protects computers and storage devices that serve as fallbacks in the case of failures.

## Type of Cyber Attacks

A vulnerability is a weakness in design, perpetration, operation , or internal control, of the vulnerabilities that have been discovered are proved in the Common Vulnerabilities and Exposures(CVE)database.

An exploitable vulnerability is one for which at least one working attack or exploit exists.

- Vulnerabilities and attacks Trademarks
- Backdoor
- Denial-of-service attack
- Direct-access attacks
- Eavesdropping
- Multi-vector, polymorphic attacks
- Phishing
- Privilege escalation
- Reverse engineering
- Side-channel attack
- Social engineering
- Spoofing
- Tampering
- Malware

### Vulnerabilities and attacks trademarks

Vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable vulnerability is one for which at least one working attack or exploit exists. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts.

### Backdoor

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for many reasons, including original design or poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Backdoors can be very hard to detect, and backdoors are usually discovered by someone who has access to application source code or intimate knowledge of the operating system of the computer.

### Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet or from a range of other possible techniques, including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

### Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, key loggers, covert listening devices or using wireless microphones. Even when the system is protected by standard security measures, these may be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

### Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private computer conversation (communication), typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the Federal Bureau of Investigation (FBI) and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon by monitoring the faint electromagnetic transmissions generated by the hardware. TEMPEST is a specification by the NSA referring to these attacks.

### Multi-vector, polymorphic attacks

Surfacing in 2017, a new class of multi-vector, polymorphic cyber threats combined several types of attacks and changed form to avoid cybersecurity controls as they spread.

### Phishing

An example of a phishing email, disguised as an official email from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by confirming it at the phisher's website. Note the misspelling of the words received and discrepancy as recieved and discrepency, respectively. Although the URL of the bank's webpage appears to be legitimate, the hyperlink points at the phisher's webpage. Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. The fake website often asks for personal information, such as login details and passwords. This information can then be used to gain access to the

individual's real account on the real website. Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers are using creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized. A more strategic type of phishing is spear-phishing which leverages personal or organization-specific details to make the attacker appear like a trusted source. Spear-phishing attacks target specific individuals, rather than the broad net cast by phishing attempts.

### Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to exploit a vulnerability in the system to gain access to restricted data; or even become root and have full unrestricted access to a system.

### Reverse engineering

Reverse engineering is the process by which a man-made object is deconstructed to reveal its designs, code, and architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon.

### Side-channel attack

Any computational system affects its environment in some form. This effect it has on its environment, includes a wide range of criteria, which can range from electromagnetic radiation, to residual effect on RAM cells which as a consequence make a Cold boot attack possible, to hardware implementation faults that allow for access and or guessing of other values that normally should be inaccessible. In Side-channel attack scenarios, the attacker would gather such information about a system or network to guess its internal state and as a result access the information which is assumed by the victim to be secure.

### Social engineering

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access by, for example, impersonating a senior executive, bank, a contractor, or a customer. This generally involves exploiting peoples trust, and relying on their cognitive biases. A common scam involves emails sent to accounting and finance department personnel, impersonating their CEO and urgently requesting some action. In early 2016, the FBI reported that such business email compromise (BEC) scams had cost US businesses more than $2 billion in about two years. In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.

### Spoofing

Spoofing is an act of masquerading as a valid entity through the falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. There are several types of spoofing, including:

Email spoofing, is where an attacker forges the sending (From, or source) address of an email.

IP address spoofing, where an attacker alters the source IP address in a network packet to hide their identity or impersonate another computing system.

MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of their network interface controller to obscure their identity, or to pose as another.

Biometric spoofing, where an attacker produces a fake biometric sample to pose as another user.

### Tampering

Tampering describes a malicious modification or alteration of data. An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data. So-called Evil Maid attacks and security services planting of surveillance capability into routers are examples.

### Malware

Malicious software (malware) installed on a computer can leak any information, such as personal information, business information and passwords, can give control of the system to the attacker, and can corrupt or delete data permanently.

## Types of Cyber security

Cyber security can be categorized into SIX distinct types:

- Application security
- Network security
- Cloud security
- Mobile security
- Critical structure Security
- Internet of Things (IoT) Security

To cover all of its bases, an organization should develop a comprehensive plan that includes not only these five types of cybersecurity, but also the three components that play active roles in a cybersecurity posture: people, processes and technology.

### Application security

Most of the Apps that we use on our Cell-phone are Secured and work under the rules and regulations of the Google Play Store. There are 1.85 million different apps available for users to download. When we have other choices, this does not mean that all apps are safe. Many of the apps pretend to be safe, but after taking all information from us, the app users share information in money with the 3rd-party as well app stop working. Suddenly this comes under Cyberattack. The app must be installed from a trust-worthy platform, not from Google Chrome.

### Network security

Guard your internal network against outside threats with increased network security. Sometimes we used to utilize free Wi-Fi in public areas such as cafes, Malls, etc. With this activity, 3rd Party starts tracking your Phone over the internet. If you are using any payment gateway, then your bank account can be Empty. So, avoid using Free Network because free network doesn't support Securities.

### Cloud security

Cloud base data storage has become a popular option over the last decade. It enhances privacy and saves data on the cloud, making it excess able from any device but needs correct authentication. Some

Famous platforms are Google Drive, Microsoft Cloud, Dropbox, etc. These platforms are free to some extent if we want to save more data than we have to pay. AWS is also a new Technique that helps to run your business over the internet and provides security to your data.

### Mobile security

Mobile is the very common gadgets we use daily; everything we excess is by mobile phone online class then the mobile phone, Call to the client then the mobile phone, sending money needs a mobile phone and many more. The mobile phones made our life so easy only with a single touch we can be excess news from another country. Then this mobile phone must come under all security patches. We must lock all the payment applications by phone in-built app as well never share your phone password except with your family.

### Critical infrastructure security

All of the physical and virtual resources, systems, and networks that are necessary for a society's economics, security, or any combination of the above to run smoothly are referred to as critical infrastructure. Food and agricultural industries, as well as transportation systems, comprise critical infrastructure. The infrastructure that is considered important might vary depending on a country's particular demands, resources, and level of development, even though crucial infrastructure is comparable across all nations due to basic living requirements. Industrial control systems (ICS), such as supervisory control and data acquisition (SCADA) systems, which are used to automate industrial operations in critical infrastructure industries, are frequently included in critical infrastructure. SCADA and other industrial control system attacks are very concerning. They have the capacity to seriously undermine critical infrastructure, including transportation, the supply of oil and gas, electrical grids, water distribution, and wastewater collection. Due to the links and interdependence between infrastructure systems and sectors, the failure or blackout of one or more functions could have an immediate, detrimental effect on a number of sectors.

### Internet of things (IoT) security

Devices frequently run on old software, leaving them vulnerable to recently identified security vulnerabilities. This is generally the result of connectivity problems or the requirement for end users to manually download updates from a C&C centre. Manufacturers frequently ship Internet of Things (IoT) devices (such as home routers) with easily crackable passwords, which may have been left in place by suppliers and end users. These devices are easy targets for attackers using automated scripts for mass exploitation when they are left exposed to remote access. APIs are frequently the subject of threats such as Man in the Middle (MITM), code injections (such as SQLI), and distributed denial of service (DDoS) attacks since they serve as a gateway to a C&C centre. You can read more about the effects of attacks that target APIs here.

## Issue and Challenges of Cyber Security in Pharma Industry

### Primary threats and challenges to pharmaceutical businesses

To protect IP and ensure data privacy, pharmaceutical organizations need to urgently address a number of common challenges. Below are the top five threats we've noticed across the industry:

### Increasingly sophisticated cyber threats probe complex networks

As pharmaceutical spending is expected to grow by $367 billion during 20213 the market faces the prospect of increased attention from cyber criminals, attracted both by the value of data and IP but also perceived weaknesses in cyber defenses. Cyber criminals are growing increasingly sophisticated in how they use threats to target pharmaceutical companies. As Accenture's Cyber Threat Intelligence Report 20214 reveals, both targets and tactics are changing: "Ransomware actors are expanding data leak extortion, devising new methods to pressure victims. Their creative approaches are hitting home as they place operational resilience—already tested by the disruptive forces of the pandemic—under increased pressure." Internal Fortinet research5 found that there was a tenfold increase in ransomware in the first six months of 2021 and that Q1 saw a botnet spike, with the percentage of organizations detecting botnet activity jumping from 35% to 51%. It's clear that both the scale and sophistication of attacks pose a growing threat to vulnerable networks with multiple, distributed end points. This naturally impacts how pharmaceutical companies should address threats. The challenge is how to mitigate risk across multiple devices and complex networking structures that have rapidly evolved since the start of the pandemic. One way to mitigate these risks across multi connected devices is to enable a more secure VPN. There is an urgent need for better VPN solutions and secure network access. Given that on average, it can take 257 days for pharmaceutical companies to identify a breach, the need for more sophisticated detection and reporting becomes essential. While pharmaceutical businesses have for a long time managed risk and compliance, the growing number of remote and offsite employees, and resulting cyber threat represents a new, unpredictable challenge that needs expert consideration. If end-to-end visibility is lacking, overall security, especially in the face of growing attacks on pharmaceutical businesses, suffers.

### Security as a priority: changing attitudes and perceptions of risk

Digital transformation and an increasing reliance on data is a universal trend. McKinsey reports6 that Covid-19 has accelerated this change, as digital adoption delivered five years of growth in just eight weeks in the early part of 2020. The pharmaceutical sector is seeing similar change, and a Deloitte C-suite survey7 of pharmaceutical companies point to R&D, global markets and the digital/IT transformation of functions, as the top three strategic business priorities for the next 5 years. With this in mind, it is important to consider the impact a data breach would have on a pharmaceutical business. According to one study8, pharmaceutical and biotech companies suffer more than most businesses. The study claims that 53 percent of organizations in these sectors have already suffered from malicious activity, with the average cost of a breach in a pharmaceutical business standing at over $5m. This is more than the healthcare, energy and financial services industries. Data security needs to be a key feature of any business development, including expansion, restructure, mergers and acquisitions, or, as we have seen in recent months, a seismic shift in working practices. Cyber security, more than ever before, has to be a priority requirement for pharmaceutical businesses.

### Connecting operational technology and avoiding operational outages

Pharmaceutical companies have been front and center in researching and developing vaccines against the Covid-19 virus. As Harvard Business Review suggests in a recent article9, this would have been impossible without the enabling capabilities of a cloud computing platform. While this remains a phenomenal achievement, the reality is that too many pharmaceutical businesses retain legacy equipment within this structure, certainly within operational technology (OT)

infrastructures. Aging OT infrastructures are not uncommon in pharmaceuticals, especially in the larger, more established businesses. In some instances, legacy equipment can be over 20 years old and may no longer be supported with suitable security patches, or even worse, may never have had security at all. For the sake of operational continuity, avoiding outages and ensuring compliance, there needs to be a focus on a security fabric that can prevent IP and data theft, regardless of the age of systems. When linking OT with cloud-based network IT infrastructures, the challenge becomes how to secure these newly connected systems. In some instances, large volumes of research data is accessed, analyzed and moved across these networks, risking years of work and valuable IP reputations, so the need to find a more intelligent, inclusive approach, that secures the link, is paramount, as is the need for the ability to monitor this newly expanded multi-cloud environment. Pharmaceuticals need adaptive cloud security to enable necessary visibility and control across cloud cyber security infrastructures for secure applications and connectivity from data center to cloud. As pharmaceutical businesses look to converge these networks, to reduce costs as well as increase productivity, there is an increasing need to mitigate unforeseen risk in cyber criminals targeting what they would consider a weak point in pharmaceutical infrastructures.

### Enabling hybrid working while managing compliance and security risk

The challenge most security advisors currently still face is the difficulty in network and device security due to the influx of remote working and employees operating off-site. The rapid increase in risk is, of course, understandable, as more remote devices connect to business networks and share data across potentially insecure Wi-Fi. Securing the network and business communications becomes an urgent priority, as employees access email and data via a proliferation of remote mobile devices, such as cell phones, tablets, and laptops. Clearly, pharmaceutical companies see this as one of their biggest threats and hybrid/remote working is not going away anytime soon. As McKinsey suggests10, most organizations are facing similar challenges over hybrid working. If anything, there is a disconnect between how and where employees and employers want work to be carried out. This raises the potential for disgruntled employees and an insider threat to data. It's therefore key that each organization has a clear and fair policy for the long term, and a security capability that can manage the diverse requirements of the future of work, including the movement of people and proliferation of remote devices. There are also concerns around employee cybersecurity education and human error, leaking data, more by accident than design. Securing the data across OT and IT networks and out into remote technology environments will require security capabilities that can free up pharmaceutical businesses from complex security integrations. A single-platform approach with a security fabric that can reach across an entire organization regardless of size and location will solve the issue of vulnerable patchwork security. No more point solutions, acquisition-based vendor portfolios and best-of-breed integration-heavy solutions from GSIs.

### Securing complex ecosystems: the partner and supplier challenge

As PwC suggests in its supply chain report11, "in order to meet the demands of a fast-evolving marketplace and the shift from patient to outcome, the pharmaceutical supply chain will need to undergo a radical overhaul." The diverse demands of modern healthcare markets, coupled with increasing regulatory demands in sustainability and provenance, for example, are forcing pharmaceutical businesses to re-address supply chain partnerships and collaborations. With the growth of digital platforms and the ability to share data easily across those platforms, the risk of data theft multiplies. The complexity of these pharmaceutical ecosystems is made even more intricate as a result of M&A activity, meaning security becomes increasingly complicated as new people and businesses bring a variety of different approaches and technologies to data security. It can lead to potential weak points, especially as the attack surface continually expands with new partners in new territories. As the saying goes, you are only as strong as your weakest link and with such complex ecosystems, there is potential for many weak links. For example, smaller R&D partners can represent an increasingly critical point of entry to malicious actors. If small partners do not have the budget or skills to secure data, they could be a weak access point for cyber criminals to reach data being shared throughout the ecosystem.

## Overcome Issue and Challenges

The pharmaceutical assiduity is one of the most critical, with people across the globe counting on it for their diurnal specifics.

There are various ways from which challenges can be overcome which are enlisted as follow:

- Set up firewalls
- Use an antivirus program
- Safeguard your home router and avoid public WiFi
- Connect to VPN
- Have a backup strategy
- Use strong passwords
- Lock your device
- Beware of phishing attacks

## Conclusion

Grounded on the exploration findings, espousing digital processes can help control force chain pitfalls. Increased relinquishment of digital technologies can help pharmaceutical manufacturing companies partake data and information more effectively, secure formulas, better manage colorful business processes, and prognosticate implicit pitfalls in the future. These advancements can help enhance the company's threat operation and address cyber security issues. thus, large businesses looking to strengthen their SC adaptability can organize a variety of digital advancements by aggressively enforcing cyber security and putting a lesser emphasis on managing force chain pitfalls. Some noted limitations of this exploration include the pharmaceutical manufacturing establishment chosen for the exploration purpose limits the generalizability. still, unborn exploration can include other manufacturing enterprises. therefore, a unborn perspective could use the same model to dissect the relationship in different diligence and give a further thorough explanation.

References

1. Massy ZA, Ma JZ, Louis TA, Kasiske BL (1995) Lipid-lowering therapy in patients with renal disease. Kidney international 48:188-198.
2. Coleman JE, Watson AR (1996) Hyperlipidaemia, diet and simvastatin therapy in steroid-resistant nephrotic syndrome of childhood. Pediatric Nephrology 10:171-174.
3. Thomas ME, Harris KP, Ramaswamy C, Hattersley JM, Wheeler DC, et al. (1993) Simvastatin therapy for hypercholesterolemic patients with nephrotic syndrome or significant proteinuria. Kidney international 44:1124-1129.

4. Oda H, Keane WF (1999) Recent advances in statins and the kidney. Kidney International 56:S2-S5.

5. Amorim P, Lecrubier Y, Weiller E, Hergueta T, Sheehan D, et al. (1998) DSM-IH-R Psychotic Disorders: procedural validity of the Mini International Neuropsychiatric Interview (MINI). Concordance and causes for discordance with the CIDI. European Psychiatry 13:26-34.

6. Abdelgadir E (2012) Exploring Barriers to the Utilization of Mental Health Services at the Policy and Facility Levels in Khartoum State Sudan. University of Washington.

7. Abbo C (2011) Profiles and outcome of traditional healing practices for severe mental illnesses in two districts of Eastern Uganda. Global health action 4:7117.