CYBER SECURITY IN PHARMA

2019 MARKET RESEARCH

FOREWORD

Experts forecast that 2018 can expect cyber breaches only to get bigger with hackers and technologies getting smarter.

This reality forces all organizations to bolster their defences – some are turning to machine-learning based features to automate risk detection by filtering alert data.

Alongside utilising the benefits of digitalization, such as IoT enabled manufacturing and cloud systems, the industry must too understand the cyber security vulnerabilities and respond with the needed precautions.

The sensitive data housed by healthcare, pharmaceutical and biotech firms are key targets for hackers. GDPR regulators are predicted to make an example of firms which do not take safeguarding data subjects seriously.

Healthcare

The need for tighter cyber security in healthcare has grown in recent years amid concerns about protecting patients' privacy and safety.

"Millions of connected medical devices introduce dangerous new threat vectors into the healthcare IT infrastructure and will seriously undermine patient safety and effective care delivery if left unchecked," market intelligence firm ABI Research warned last year.

Many feel that the level of spending hasn't been high enough to date. Industry commentators have urged healthcare organizations to step-up amid concerns around how frequently data is backed-up alongside required security patch updates.

Pharma

Pharmaceutical and biologics firms hold valuable IP that may not be protected by a patent yet. Research and development findings are key to informing drug manufacturer's next steps especially regarding the compositions of their future medicines, processes and products.

The interconnectivity of corporate networks make data sources like clinical trial data and lab notebooks potentially vulnerable to breaches.

Not only could breaches present a severe threat to the future of a pharmaceutical company, but also to patient safety. This is due to the fact that these entities house personal health information and medical data.

On the subject of cybersecurity concerns for pharma, Ed Francis, senior

FOREWORD

director and national life sciences industry lead at West Monroe notes: "There are a number of competing trends that are making cybersecurity more important and challenging. There is an increased desire to comingle identified and de-identified datasets (medical record, genetic, wearable, demographic, image, lifestyle, etc.)

"There is also an increase in regulatory requirements and penalties both in the United States and abroad. And there is an increased virtualization of the enterprise, requiring more data being transferred between entities and across entities outside their firewall. All of this is working together to both increase the importance and complicate the implementation of effective cybersecurity efforts."

As cyber threats intensify pharma firms will need to dedicate themselves to the governance strategies that digitally protect their assets and data subjects.

CONTENTS

FACT FILE

Types of attack: "The first category of attack is the destruction of data, especially R&D data. If data is destroyed that is not backed up, or if back up integrity is questionable, there is a serious problem. All backed up data must be exact and complete, and secure from alteration, inadvertent erasure, or loss.

"The second category of attack is the intentional alteration of data. This is more insidious because if the alteration is not detected, it can result in errors in formulations. Alteration can include the addition, deletion, or other modification of data. Pharma data integrity is critical to ensuring the safety, efficacy, and quality of drugs.

"Both of these categories of attacks require robust security defenses, including the creation of physical and logical access programs to ensure the security of offices, laboratories, data centers, computer networks, and individual computers." - Jack Plaxe, Founder & Managing Director of the Security Consulting Alliance LLC.

Reasons for a breach: Attacker motives can range from gaining financial rewards through organised crime, making political statements or even state sponsored targeting. Breaches can be a result of human error within your organization such as accidental deletion or use of a corrupted USB stick.

Trave Harmon, Chief Executive Officer at Triton Computer Corporation notes that all manufacturers are at risk of corporate espionage as many see it as a cheaper and easier route to acquiring information or innovation. "We have witnessed many times businesses have their intellectual property stolen because they either didn't think the security was important, or put no investment to protecting their data. We've been nvolved in multiple lawsuits, settlements, and more and I can tell you that with certainty theft on an unprecedented scale happens every day."

Modes: Web servers can be an infiltration point when they act as an interface to control devices. Others targets for attack include database servers. Software can be compromised using these channels through viruses, trojans and malicious software.

Multiple live medical devices are known to have fallen victim to cyber attacks because their software has gone through inadequate vulnerability testing.

Toronto based cybersecurity company Copperhead has been watching both the information security and attacker side of threats for some time. James Donaldson, CEO of the firm said:"I'm concerned that the speed of which attack tools are made and most importantly, the ease of use for non-technical attackers, has grown exponentially over the last few years.

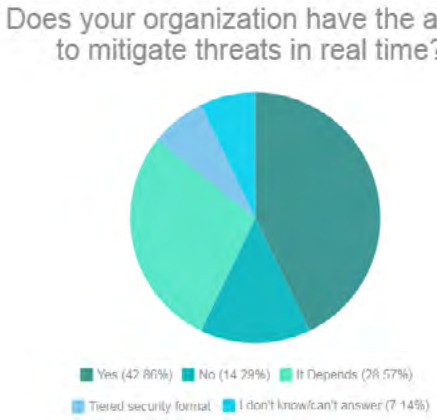
FACT FILE

"Attackers, not unlike the white-hats in the industry, recognize that vast profits can be made by simply subscribing tools for use by non-technical attackers. That way they are on top of the vertical profit structure. Infosec will have to catch up by creating solutions that non-technical users can utilize to protect their own assets from theft or breach."

Vulnerabilities: Security holes can open up from backdated operating systems or incompatibilities between systems. Inadequate software updates and patches can be key culprits.

About The Research

We asked a range of information security experts in our Pharma IQ network for their insight on various areas of cyber security. The majority of this base is from the likes of pharma and biotech companies.



The majority of this base has confidence in their company's information security, with some venturing to express a high level of confidence. This reflects their perspectives on whether their organization has the ability to mitigate threats in real time. With digital security being a consideration for all company members, it could be deemed as interesting that a large level of the respondents do not have an opinion on the organization's level of information security.

Sean Curran, Senior Director and national cybersecurity lead at West Monroe; "The industry still has some immaturity in the way they are approaching cyber. They typically focus on IP infringement and not necessarily the protection of clinical data. They are also challenged to see the full picture: The virtualization of the supply chain for some pharma companies has opened them up to a different risk profile. Across the board, I would say most don't understand their risk profile well enough to appropriately apply the right controls for cybersecurity."

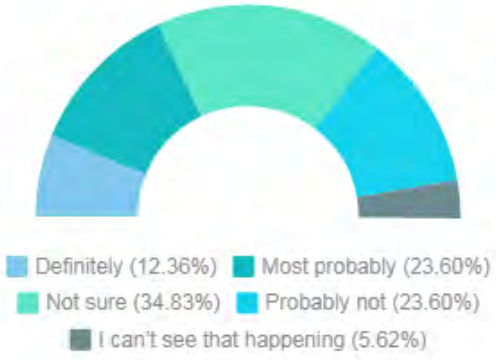
Software can be implemented to prevent data leakage and identify breaches in regards to sensitive information. Depending on the operating systems used, some legacy devices may not be discoverable by network scanning tools that identify cyber security vulnerabilities

Forecast

Cyber security spend has not been high enough in pharma and healthcare according to many industry commentators. In this regard its encouraging that according to those able to answer there isn't any forecasted drop in spend and mostly a charted increase in this area. Also the majority of respondents can see a cyber security rep being promoted to the C-suite in the next 12 months. This presence would indicate a clear commitment to this vertical.

Over the next 12 months, your company's spend on cyber security systems and procedures is likely to…

Do you think your company will promote a Cyber Security Rep to its C-Suite in the next 12 months ?



Top vulnerabilities for info systems

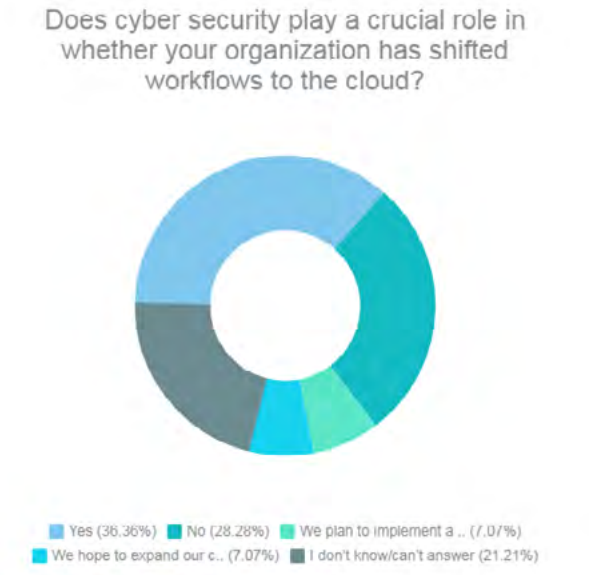
1. Lack of basic cyber hygiene (weak passwords, careless talk)
2. Sophisticated malware
3. Insider threat
4. Spear phishing
5. Social engineering
6. USB infection

Security Governance

IoT devices have little or no defence against hackers who seek to control them. Understanding vulnerabilities and risks are crucial to continuous cyber security, it only takes a lapse to produce an opening for entry. Therefore, it is slightly alarming that around 20% of the base is not grounded in a real-time view of their company's network map.

Manufacturers need to be proactive with security assessments and may want to introduce limits on how devices can be connected and accessed through network segregation via firewalls. New market entrants can get ahead in the industry via deploying security best practices from the outset to avoid costly upgrades.

The majority of respondents have documented security policies which are followed and tested. Bolstering system resilience through a governance approach can be implemented at various levels in a manufacturer's hierarchy. In the transfer of data, encryption should be considered, for instance TLS for layer encryption. In its recent Top 10 proactive control article, The Open Web Application Security Project declares that ideally data should not be saved on a mobile device. Query Parameterizaton is a programming technique used to mitigate SQL injections. SQL codes can be inserted into a web application and lead to a whole database being stolen, cleared or amended.

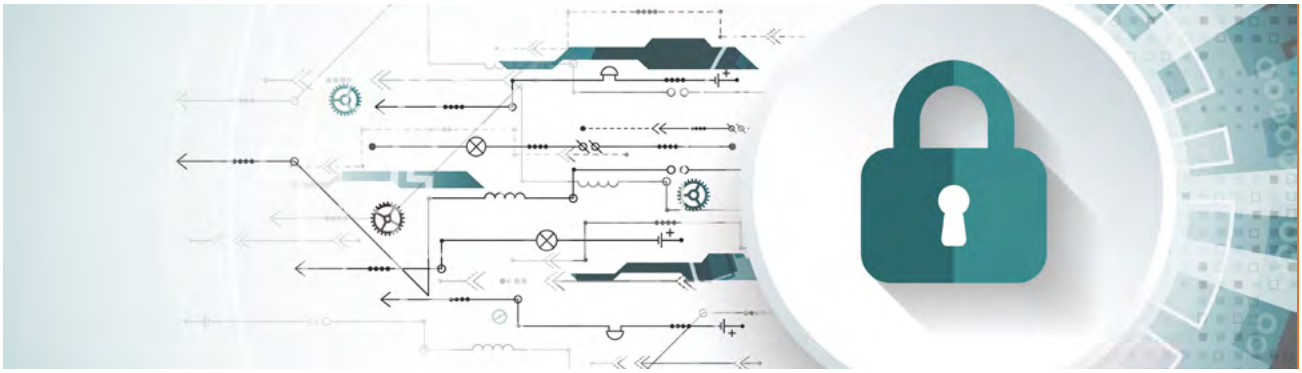


There is a marked shift to move items to benefit from the advantages of cloud access. The security of the data remains the responsibility of the user so they must ensure any investment decisions safeguard these duties. While it is comforting to see 40% agree with this, just under 30% admit it is not a crucial part of their cloud strategies.

Company Wide Awareness

Digital attacks can even be unintentional for example an infection obtained via a corrupted USB stick inserted by an administrator. The high percentage (49%) of respondents admitting there is rarely any routine awareness training sessions correlates to the previous chart stating lack of basic cyber hygiene is the most critical vulnerability for these respondents on average.

There is a lack of cohesive understanding across organizations within this data pool as shown by 49% of the respondents in the second graph above. These participants admit that the corporate risk profile is either poorly understood and not improving or only firmly understood in some departments.



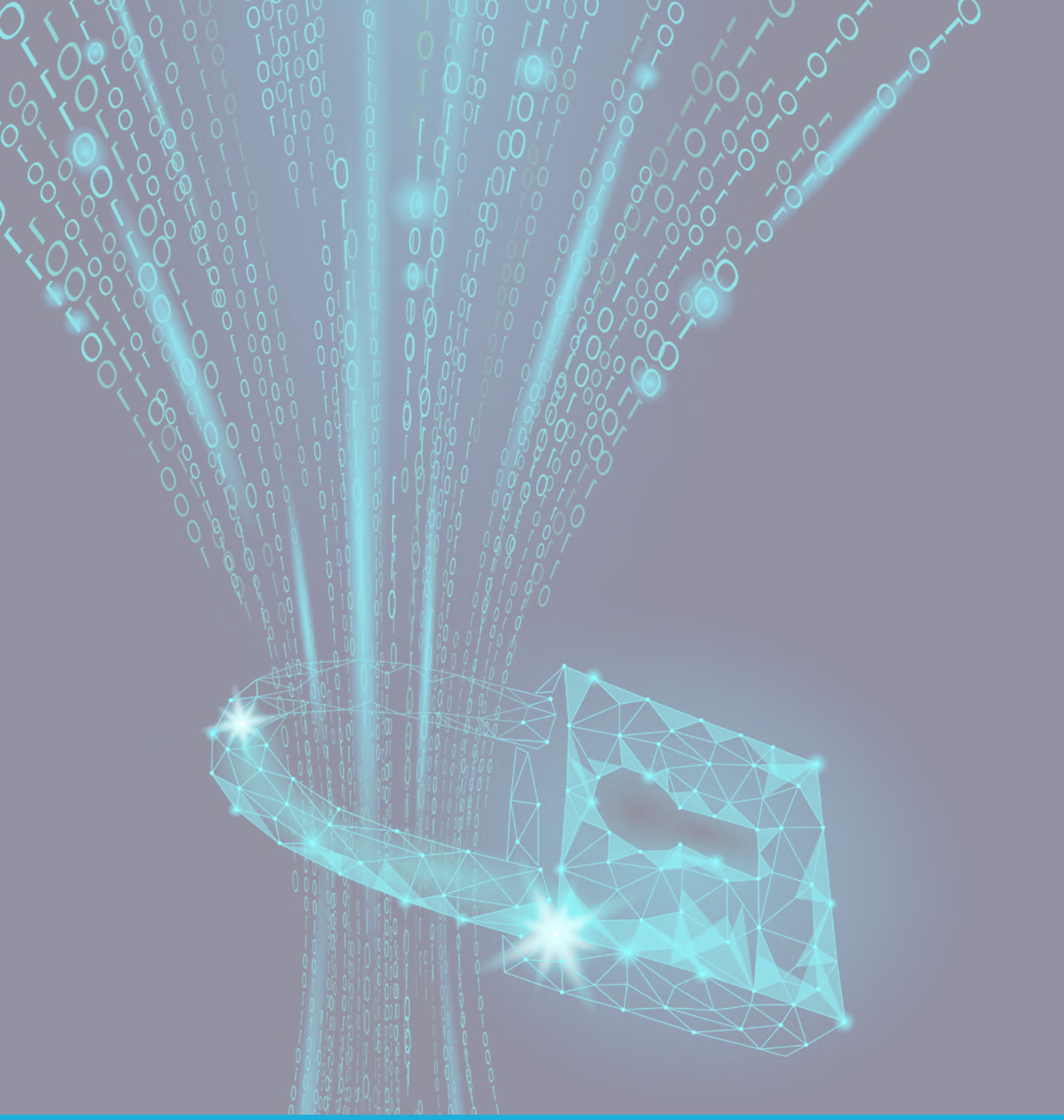
CLOSING REMARKS

Encouragement can be drawn from the level of importance placed on cyber security from the respondents as it is unlikely we would have seen this from pharma professionals a few years ago. However, there is still some way to go until cohesive security is seen across organizations and there is a full dedication to maintaining good cyber security hygiene.

As noted by Marcy Wilder, leader of global law firm Hogan Lovells Cybersecurity practice. :"The EU's General Data Protection Regulation (GDPR) includes key provisions requiring data breach reporting and imposing security obligations.

"Hackers view health systems and medical devices as high-value targets. Liability for class action and shareholder suits, regulatory penalties from enforcement actions and reputational damage associated with health data breaches continues to grow. Digital health organizations must account for the unique risks associated with health information and implement programs for cyber risk identification, management, and protection that go beyond check the box compliance efforts.

"Every digital health organization should have an Incident Response Plan (IRP) ready and reheard. Effective preparation for managing a data breach helps ensure a swift and coordinated response that can minimize harm to patients and consumers and reduce reputational impact and potential legal liability. As the threat of cyberattacks continues, nearly every digital health organization will be faced with a cybersecurity incident. Organizations that have plans in place to mitigate the risks will be better positioned to survive and thrive."



About Pharma iQ

Pharma IQ, a division of IQPC, is an international online community focusing on providing pharmaceutical professionals with knowledge, information and articles. We are dedicated to creating a learning environment for sharing ideas, best practices and solutions within the pharmaceutical community

Through Pharma IQ, you will be able to access pharmaceutical information resources such as presentations and podcasts, as well as events such as webinars, seminars and conferences.

By signing up to the Pharma IQ membership, you will gain access to our growing database of multimedia presentations from leading pharma practitioners, weekly newsletters to keep you updated on latest pharmaceutical content and Pharma IQ members-exclusive discounts on pharma events that offer solutions to your everyday business problems.

Let's Get *Social*

Stay up to date with Cold Chain Global Forum & *join us on social media!*

www.linkedin.com/groups/879897

twitter.com/CCGlobalForum

Use our hashtag ***#CCGF*** and get the chance to be entered into an on-site raffle!

Cold Chain Global Forum CANADA . 19

Temperature Controlled Life Science Supply Chains

Pharma Logistics IQ

February 26 - March 1, 2019 // Toronto, ON

www.coldchainpharm.com

JOIN US!

#CCGF