Pharma Data Theft on the Rise: Protecting your Data in the Digital Age

Table of Contents

Table of Contents 1

Introduction 2

Contextual trends: 3

Do digital solutions help or hinder Information security? 6

ELN and LIMS systems 6

Cloud vs server 8

Internet of things (IoT) solutions 9

What is important before selecting a provider? 10

What is Labforward's approach to ensuring IT and cybersecurity? 11

An engineer's perspective: what we do to protect your data 12

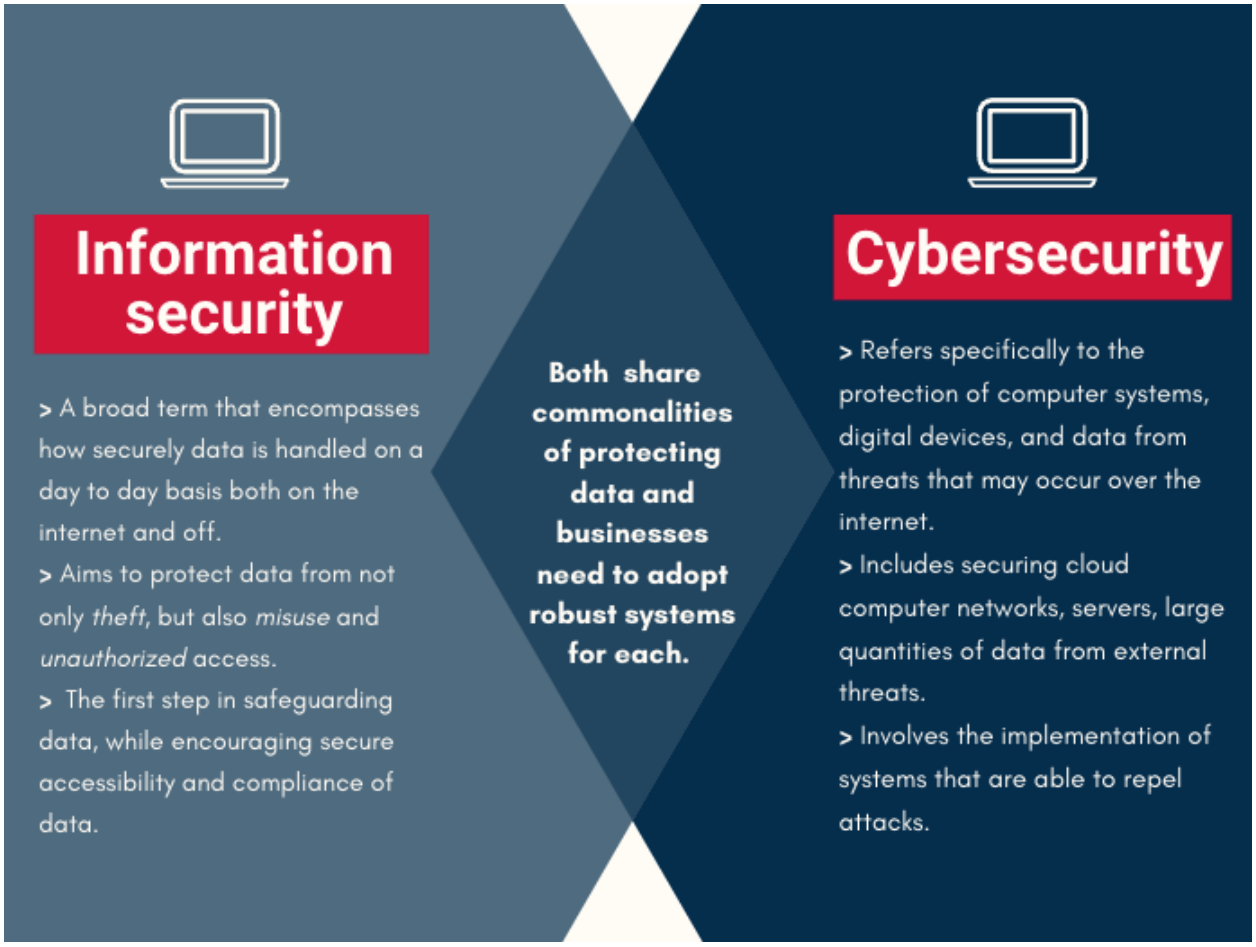
Conclusions 13

Pharma Data Theft on the Rise: Protecting your Data in the Digital Age

Pharma, Healthcare, Biotech and other sectors in R&D are increasingly becoming the targets of hackers. It's now more important than ever before to stay vigilant against cybersecurity threats and implement comprehensive information security strategies.

Introduction

As more pharma laboratories undergo digital transformation, concerns have been raised about the security of research and healthcare data. Increasingly, pharma has been the target of sophisticated and damaging cyber-attacks, in part driven by the attention healthcare and research sectors have received during the pandemic. In order to grasp the scale of the threat, it is important to fully understand what is meant by Information security, cybersecurity and the distinction between both terms.



Information security is a broad term encompassing how a company or organization handles their data on a day to day basis. It is the overarching processes that ensure the security of computer networks, hardware, and software that are used to store and share digital information. In comparison, cybersecurity is a narrower term, sometimes viewed as a subset of Information security. It focuses on predominantly the protection of computer systems, digital devices, and data from unauthorized access, usually pertaining to hackers. Both terms share the commonalities of protecting data, devices and people from ransomware, hackers and phishing attacks in the digital age, while ensuring the confidentiality (information is available only to authorized users), integrity (information is accurate and complete) and availability (authorized users have access to information when they need it) of data. But what can small, medium and large pharma organizations do to, on the one hand, ensure successful digital transformation, and on the other ensure the security of their data? Organizations regardless of size should implement a systematic approach to manage risks and protect their valuable information assets. In this article we delve into key topics in the discussion of security and uncover ways laboratory teams in both industry and academia can protect themselves against IT and cybersecurity threats.

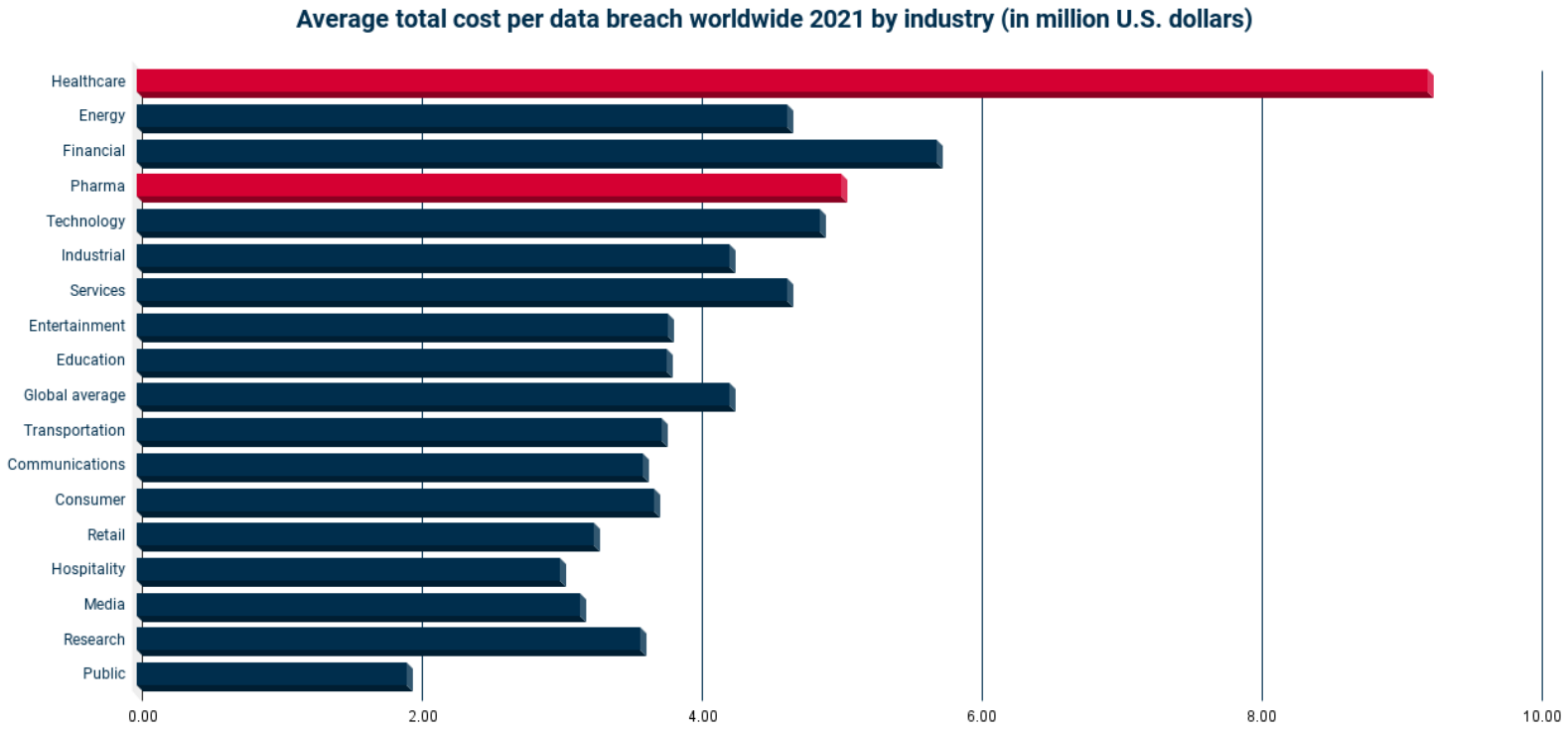
Contextual trends:

December 2020 saw the European Medicines Agency (EMA) being hit by a cyber-attack that gave access to documents pertaining to the COVID-19 Pfizer vaccine[1]. Then, in 2021 an estimated 45 million people were affected by healthcare cyber-attacks[2], an increase from 34 million (29%) in 2020. This demonstrates that as healthcare and research gains more media attraction, this likely results in a rise in the threat to IT and cybersecurity. Paired with this, the nature of feelings brought out by the pandemic has amplified these threats. The strong sentiments people feel in regards to vaccines, either positive or negative, has triggered greater focus on healthcare and research sectors; and as hackers tend to follow trends to cause disruption, this means that those working in research and development and healthcare need to stay vigilant and current with security trends and practices.

In addition to this, the widespread, rapid, adaptation to a work-from-home setting put additional pressure on security teams[3]. In many cases, individuals used their computers outside of the secure networks of their organization, making them more susceptible to cyber-attacks. A study exploring cybersecurity trends reinforces this, stating that people working remotely caused a decentralization in many organization's landscapes that subsequently created "new

[1] BBC: *Pfizer/BioNTech vaccine docs hacked from European Medicines Agency,* BBC. (9/10/2020)
[2] Landi, H. *Healthcare data breaches hit all-time high in 2021, impacting 45M people,* Fierce Healthcare. *(01/02/2022)*
[3] Boehm, J. Kaplan, M. Sorel, N. Sportsman, & Trevor S. *Cybersecurity tactics for the coronavirus pandemic*, Mckinsey. (23/03/2020) p.2

vulnerabilities" that "malicious actors"[4] were able to exploit. As a result, it's estimated that cybercrime today equals a "$1 trillion dollar drag on the global economy"[5]. The cost of a successful attack is incredibly expensive on an organizational level. Not only are there significant legal repercussions to a loss of data, but also the costs to determine the causes of a data breach are likely to be extensive. The graph below depicts the average cost per sector in data breaches in 2021. Healthcare is shown to have the highest cost, with pharma being the fourth industry most financially affected by cybercrime. Crucially, if we look at the global average, the cost in healthcare is more than double, demonstrating the scale of the problem.



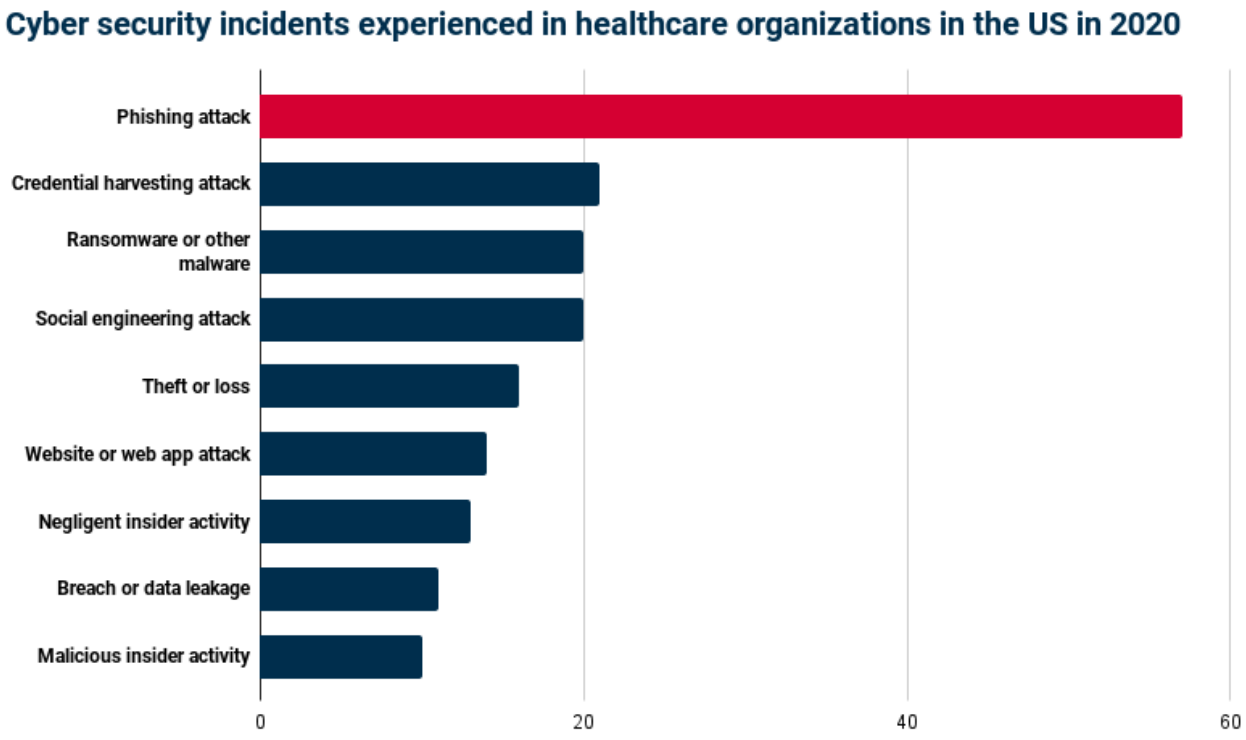
6

It is also worth noting the importance of the forms of cyber-attacks that are taking place. A report (below) depicts that in the US, phishing attacks had the highest share of cybersecurity incidents in healthcare organizations in 2020. This is particularly interesting as phishing attacks do not require much technical expertise. The high prominence of phishing attacks could be

[4]Statista,"WordwideCybersecuritySpending"
https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/
[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[6] "Average cost of data breaches worldwide as of 2021, by industry"

explained by their success in exploiting not computers but people's ignorance of information security.

Human error is a major security risk. Just recently, a notable data protection software and appliance technology developer, experienced a damaging hit, after an unknown number of end-user clients lost their backup data. This happened as the result of human error when the company was moving the backend operations from an internal data center to the Google Cloud Platform, in order to add resilience to the system. Only this backfired. Considering this, to a greater extent, it is not just enough to have robust IT systems in place, but there needs to be an awareness of cyber and information security importance *throughout* an organization. In a Forbes article that emphasizes the importance of the "human firewall" it's stated that "strong security is not just about a chief information security officers immediate team; it's about how strong and resilient the entire enterprise is from a human standpoint"[7] In the laboratory setting from the managerial level, down to individuals working in R&D or a QC laboratory. *And* also within the solution providers organization structure.



[7] Forbes Insight "The Importance Of Training: Cybersecurity Awareness As A Firewall" (2019) https://www.forbes.com/sites/insights-fortinet/2019/08/27/the-importance-of-training-cybersecurity-awareness-as-a-firewall/?sh=ff144ed8b4bf

So what is the solution? Unfortunately, there is not a one-size-fits all solution to guarantee information security and cybersecurity, as it is subject to quick change. Hackers are always working to thwart security measures and so it is especially important to stay up to date with all the latest developments in information security. That being said, it is also possible to minimize risks with good practices and procedures. Good endpoint security measures (securing entry-points of end-user devices), identity access management, data security, network security initiatives, good organization data practices and employee training are likely to translate to a robust security system. With these in place, small to large businesses can protect themselves against both external and internal threats. Thus, as cyber-attacks continue to rise in scale, complexity and sophistication, it is vital that a comprehensive strategy is put in place and frequently reviewed to ensure maximum levels of protection, particularly in a time where laboratories are looking to digitize processes.

Do digital solutions help or hinder Information security?

There is often a misperception that the security of data is somewhat compromised after it's digitized and this has led to many research teams being apprehensive to adopt digital processes in the laboratory. Coupled with this, some are less likely to store their data on the cloud for fear of Information security breaches, opting for on-premise servers instead. However, while digitizing research inevitably triggers conversations about Information security, it should not prevent teams from implementing these solutions.

ELN and LIMS systems

ELNs (Electronic Laboratory Notebooks) and LIMS (Laboratory Information Management Systems) are commonly used in many laboratories around the world. They are both forms of software that provide researchers with an online platform to record research documentation. With increasing pressures from international regulatory bodies to improve the findability, accessibility, interoperability and reproducibility (FAIR) of research data, the adoption of solutions that digitize documentation processes has increased substantially. This is largely because of the extensive benefits of going digital, particularly when considering the pitfalls of the previously relied upon paper lab notebooks.

The drawbacks of paper lab notebooks are as follows:

1.) Data can be difficult to find. A simple task like searching for raw data from an experiment performed in the past could take a scientist hours to find.

2.) Data can be lost or incomplete due to employee departure.

3.) Data recorded can also be illegible, incomplete or incorrectly recorded.

Notably these issues with paper lab notebooks revolve around information security. If a researcher is unable to recover important data from an experiment that took place a couple of years ago or if that paper lab notebook has been damaged in some way making the information illegible, that poses a very real and in many circumstances impactful information security threat. If a researcher then has to redo an experiment as a result of this data loss, it will have significant financial and productivity repercussions that could've been avoided. There is a tendency for the terms information security and cybersecurity to be conflated. While related, information security encompasses all aspects of measures taken to safeguard data, and in consideration of this definition, paper lab notebooks are not that secure.

But are digital solutions better?

Notably, attitudes have changed in regards to digital laboratory solutions since the pandemic. In many cases, where paper lab notebooks were used, research teams were unable to access their data, and with restrictions over when you could go to your place of work, this was incredibly disruptive. Comparatively, those who had an ELN or LIMS solution could access complete research records from anywhere, making it invaluable for many teams. An NIH study conducted in 2017 highlights the benefits of such systems stating that they facilitate "long-term storage, reproducibility, and enhanced availability of experiment records across multiple devices, ensuring standard operating procedure compliance and providing interfaces to instrumentation, supporting IP protection, collaboration, and open science". Simply storing your data on a computer means that data can be searched for, shared, backed up and readily accessed when required. So in consideration of this, many argue that digital solutions actually enhance information security.

However there still remains to be apprehension for choosing digital methods over the traditional paper lab notebook, and 'security' is often at the heart of this hesitation. Despite helping not hindering overall information security, there are cybersecurity concerns that inevitably arise when storing data digitally. As aforementioned, cybersecurity refers to the prevention of unwanted access to data, typically in the form of hackers but not always. Many ELNs and LIMS solutions give research teams more control over how their data is accessed. Data can be strictly controlled and monitored, with all actions recorded by a full audit trail. Administrators can choose who is able to view, edit or share data, giving increased protection not possible with the paper lab notebook. With ELNs and LIMS you can centrally permit users from exporting data, whereas when storing data in files, anyone with access to the computer can copy them. Thus protecting data from unwanted access internally to a greater extent improves with a digital solution.

But what about external access? Well, this is largely dependent on other factors such as the digital solution provider, whether data is stored on a server or the cloud, what measures have been put in place to safeguard data and whether a team has been properly trained in understanding how to mitigate risks of storing data digitally. If all these factors are properly addressed and maintained on a consistent basis, then digital solutions can be a more effective and secure way of documenting research, particularly when considering the numerous other advantages of using such a solution.

Cloud vs server

The common belief is that on-premise data storage is more secure than the cloud. Subsequently, security is often the first thing discussed when businesses consider adopting a cloud-based solution. However, this 'great data myth' as Microsoft Azure MVP Sam Cogan puts it, is a flawed perception. Cogan argues instead that as a cloud provider's entire reputation hangs in the balance of providing a secure environment for hosting data, "any significant breach would severely impact user confidence and directly impact their revenue"[8]. As a result, cloud providers often make significant investments in security, personnel and software to ensure the utmost protection of their entire infrastructure and cloud user data. Security is then regularly monitored and updated accordingly.

So what is the reality? What are the biggest threats in storing your data on the cloud?

An OECD case study found that digital security gaps for cloud services mostly "result from a lack of *user awareness* or *education*, a failure to fully implement "security-by-default" principles, a misperception of risks and a difficult attribution of responsibility across the value chain"[9]. Indeed, this emphasizes once again the importance of an organization-wide awareness of security matters. The cloud can be safe, but it requires *all* employees in the organization to take security seriously.

> "With the right setup, both cloud and on-premise servers can be secure places to store data, but a thorough, constant assessment of the security infrastructure is required to maintain this"

Sometimes the decision whether to store data on cloud or local server is based purely on financial capability. Large organizations often have the means to take care of security themselves and in some instances already have the infrastructure in place to protect their data.

[8] "The great data myth: Is cloud really less secure than on-premise?" https://techmonitor.ai/technology/cloud/great-data-myth-cloud-less-secure-on-premise
[9] UNDERSTANDING THE DIGITAL SECURITY OF PRODUCTS: AN IN-DEPTH ANALYSIS p.46

In these cases, there's not much difference between public and private clouds, it depends largely on the systems in place and the practices to ensure security. Crucially, with the right setup, both cloud and on-premise servers can be secure places to store data, but a thorough, constant assessment of the security infrastructure is required to maintain this. Not all software providers offer a choice of cloud or server, so a careful look into what each solution provides is essential when looking to invest in implementing digital software or when deciding to store data on the cloud.

"For organizations with limited financial resources and therefore less means to guarantee information security, we definitely recommend cloud solutions. For larger organizations with the resources and processes in place to ensure information security it really doesn't matter if they go for cloud or on-premise, the decision has to be made based on other factors."

Mario Russo, CTO at Labforward

Internet of things (IoT) solutions

While documentation software and data management solutions are becoming increasingly common in the laboratory, IoT has only recently emerged and is being quickly picked up by many different industries, including pharma and R&D. Defined broadly by IBM, the IoT "is the concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices"[10] with the ability then to control and monitor equipment by using internet access. The adoption of IoT is largely viewed as a positive step towards creating a more connected, productive environment which maximizes machine potential and researcher time. However, as an OECD report surmises, the quick adoption of IoT products has in some cases led to the creation of technologies that "lack basic security features", given the rush to dominate the market quickly. Thus, security concerns become even more important to discuss when considering the adoption of IoT in the laboratory.

But how does securing IoT technology differ with other forms of innovation?

Well, according to Bruce Schneier, the author of "Here to Kill Everybody: Security and Survival in a Hyper-connected World", the emergence of IoT has caused the two basic paradigms of security to converge creating new challenges and realities. The first paradigm of security is born from dangerous technology that can be a long and costly process to create to ensure the quality and infallibility of the products. Think cars, planes, pharmaceuticals, construction etc. Whereas

[10] IBM: Clark, Jen. (2016)
"What is the Internet of Things (IoT)?" https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

the second is the "fast-moving, freewheeling, highly complex,"[11] world of software (ELN's and LIMS fit into this paradigm) that is highly adaptable and agile to security threats. The problem is that with the rapid introduction of IoT enabled devices, these paradigms are colliding, in some cases uncontrollably. Schneier concludes that IoT developers need a blend of both paradigm's security approaches, creating on the one hand stable, robust products with consistent checks and balances throughout the production stages, and on the other, a flexible product that is able to quickly adapt to any vulnerabilities found.

> "IoT developers need a blend of both paradigm's security approaches"
>
> Bruce Schneier, author of "Here to Kill Everybody: Security and Survival in a Hyper-connected World"

So how are IoT solutions being adapted to the laboratory environment and what are the security challenges, product creators and customers face?

Firstly, it's important to note that implementing IoT into the laboratory does not mean running production plants from the cloud. If the machines fail to operate correctly, this would severely impact production processes thus directly affecting profit. The use of IoT solutions in the laboratory currently is mostly in aid of monitoring equipment and directly generating data, which may be aggregated and analyzed through private servers or clouds. Currently, IoT developers have to keep up to date with good Information security practices, consistent and frequent checks and balances, in order to harden IoT devices so they are resistant to unwanted access. IoT products operating in Europe need to consider GxP (if operating in the pharma/laboratory industry) and EU regulations, and those working to produce solutions for the laboratory need to keep in mind QC validation which can be a challenge for developers. Furthermore, it is a constant process to keep these IoT systems up to date with the latest changes in security recommendations that can create a challenge for developers. What becomes clear, is that when an organization selects a provider, they need to have complete faith in the Information security systems and processes of that company.

What is important before selecting a provider?

It is vital to check that before selecting a provider of an IoT solution that it upholds excellent IT and cybersecurity practices.

[11] Vice: Schneier, Bruce. "Patching is failing as a security paradigm" (https://www.vice.com/en/article/439wbw/patching-is-failing-as-a-security-paradigm)

Taking into account whether the provider has:

- **A transparent information security policy -** Ensuring that your provider is completely transparent with what measures they are taking to ensure the security of your data is essential. Some attacks can go unnoticed, and many organizations have in the past chosen to protect their brand reputation over disclosing that some assets have been compromised[12]. By selecting a trusted provider that can demonstrate constant review and updates of security accordingly, is a key step in protecting your data.
- **Clear information security certifications and registrations** - Check if the provider holds any certificates e.g. ISO 9001:2015 or ISO 27001. Moreover look into whether the vendor has written policies and procedures on information security, or if they're in the process of getting a certificate.
- **Adherence to data privacy and protection regulation (GDPR) -** Looking into whether your provider adheres to GDPR is a good indicator of how much a company prioritizes IT and data privacy. A 2017 survey conducted by Marsh & McLennan noted that "organizations preparing for or compliant with GDPR over 1.5 times more likely to report an increase in cyber risk management spending than those at organizations that had not yet started"[13]. Ultimately, companies that invest in ensuring GDPR compliance tend to adopt more cyber risk management practices as a whole.
- **Complete control over access to data -** It is important to ensure that your provider has the technical and organizational measures in place that offer complete control over access to your data. They must be able to deter unauthorized access and demonstrate that they are constantly monitoring access rights while ensuring "ongoing confidentiality, integrity, availability and resilience of processing systems and services"[14].
- **Software vulnerability oversight** - Check if your provider uses tools that continuously test their software for possible security threats. Also linking to transparency, it's useful to see if your provider has a coordinated vulnerability disclosure (CVD), CVD ensures vulnerabilities are addressed prior to being made public.
- **External audits** - External audits can be a really good way for a company to ensure that it is compliant with data protection criteria, thereby ensuring that a company complies with regulations.

What is Labforward's approach to ensuring IT and cybersecurity?

Building greater connectivity between researchers, their equipment and their data is one of our core objectives at Labforward. We want to transform the laboratory with high quality products

[12] OECD: "smart-policies-for-smart-products" 2021
https://www.oecd.org/digital/smart-policies-for-smart-products.pdf
[13]Marsh&McLennan
https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Cyber-Survey-Report-2017.pdf
[14]Article 32, GDPR. https://gdpr-info.eu/art-32-gdpr/

so that it is an environment that fosters innovation and creativity but also encourages precision and compliance. For us to achieve our overarching goals we recognize that having a reliable, resilient and robust Information security strategy is vital.

Customers use our platforms on a day to day basis. Whether they opt for the cloud or server, security is always at the forefront of any decisions we make with our products. We've implemented various security measures within our solutions and as a company that put us in the best position to, on one hand, ensure that our products are agile and quickly able to respond to any discovered vulnerabilities; and on the other hand, ensure that every step of the production process factors in potential risks and how these can be solved. When it comes to our security policy, as a company we take a transparent approach, as we want to show that when it comes to storing your data on our platform, we have consistent and thorough checks to ensure the utmost protection of our customers' intellectual property.

An engineer's perspective: what we do to protect your data

It is important to note that there is not just one step to Information security and it's certainly not something you can just 'add-on' at the end of developing a new feature or update. Labforward's approach is that security plays a vital role throughout all stages of the software development lifecycle and any changes implemented have to go through thorough checks to make sure that they won't expose the software to vulnerabilities that can be exploited.

So what do we do in our development and implementation processes that help us secure your data? Well, we make sure that security is considered at every stage - from the inception to the final result and beyond. Here's how:

- At the planning stage, when ideas are being drafted it is the optimal time to conduct a risk analysis, to envisage all things that could potentially go wrong and how these risks can be mitigated and eliminated. Thinking about possible implications and worse-case scenarios is good practice as it then shapes what the engineering team develops. Our changes then are built in *consideration* of security and not as a last thought. Our Laboperator Connector Boxes for example, follow CIS guidance that develops, validates, and promotes best Information security practices. Before any changes are implemented, careful consideration of this guidance is followed.
- Further conversations happen at every stage, for example, when the code is complete, there are reviews by the engineering team to ensure that this code is not opening up any vulnerabilities. At this stage, engineers also run plenty of trial tests on our testing environments to make sure that there are no security implications from the new code. In

this way, security is embedded into every aspect of product development, from a new feature's inception to its release.

- After the release, it is important to ensure that server and cloud components alike are regularly checked. All our products use automated security and penetration testing tools. Furthermore, we ensure that all of our code bases are continuously checked for best security practices using static analysis tools.
- When it comes to security it's also useful to keep good relations with external partners and Information security leaders, especially in regards to compliance. At Labforward, we take the approach to consult with industry leaders to make sure that we have up to date general security practices, but also ensure that we're staying on top of new IoT security recommendations, as further information becomes available.
- Ensuring security goes far deeper than just on a product level is really important. As highlighted previously, risk often arises due to complacency of staff rather than solely technical deficiencies. Therefore, it is important for all Labforward team members, particularly those in engineering, to stay up to date with the latest developments in IT and cybersecurity practices. We have organized regular training sessions, workshops and development Fridays in order to keep everyone engaged with this topic. Furthermore, internal training for all team members has been an important part of our Information security strategy.

It certainly helps to be surrounded by a team of passionate people who are all knowledgeable about current trends and make consistent efforts to keep up to date with the latest news in software engineering. In this way, security is not just one person's responsibility, but something that is worked on and executed as a collective within the Labforward team.

Conclusions

To summarize, in a time where the pandemic has heightened awareness of the importance of healthcare and Pharma, it is crucial that organizations take Information security seriously. That means not just implementing antivirus software, developing robust systems etc. but educating *all* personnel on the best ways to protect themselves online. While digital solutions actually tend to enhance your *information* security, storing data online inevitably opens the door to cyber-attacks. That's why it is crucial to carefully select a trusted provider, especially if you're storing data on their cloud. Disruptive technology such as IoT offers many opportunities for Pharma and healthcare sectors alike, but a blend of approaches is needed to ensure on the one hand the infallibility of the product and on the other, the ability to quickly adapt to discovered vulnerabilities. And if you think that IoT security is complex, just wait for the implementation of machine learning and AI into the laboratory! The Smart Labs of tomorrow are around the corner, but we need to ensure that as we embark on digitization journeys, we stay vigilant against security threats in an ever-changing technological landscape.

Bibliography:

McKinsey & Company: Jim Boehm, James Kaplan, Marc Sorel, Nathan Sportsman, and Trevor Steen
https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-tactics-for-the-coronavirus-pandemic

OECD: "smart-policies-for-smart-products" 2021
https://www.oecd.org/digital/smart-policies-for-smart-products.pdf

"Average cost of data breaches worldwide as of 2021, by industry"

Statista,"WordwideCybersecuritySpending"
https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/

Forbes Insight "The Importance Of Training: Cybersecurity Awareness As A Firewall" (2019) https://www.forbes.com/sites/insights-fortinet/2019/08/27/the-importance-of-training-cybersecurity-awareness-as-a-firewall/?sh=ff144ed8b4bf

The great data myth: Is cloud really less secure than on-premise?" https://techmonitor.ai/technology/cloud/great-data-myth-cloud-less-secure-on-premise

IBM: Clark, Jen. (2016)
"What is the Internet of Things (IoT)?" https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

Vice: Schneier, Bruce. "Patching is failing as a security paradigm" (https://www.vice.com/en/article/439wbw/patching-is-failing-as-a-security-paradigm)

BBC: *Pfizer/BioNTech vaccine docs hacked from European Medicines Agency,* BBC. (9/10/2020) https://www.bbc.co.uk/news/technology-55249353

Landi, Heather. *Healthcare data breaches hit all-time high in 2021, impacting 45M people,* Fierce Healthcare. *(01/02/2022)*
https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

Boehm, J. Kaplan, M. Sorel, N. Sportsman, & Trevor S. *Cybersecurity tactics for the coronavirus pandemic*, Mckinsey. (23/03/2020) p.2
https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-tactics-for-the-coronavirus-pandemic