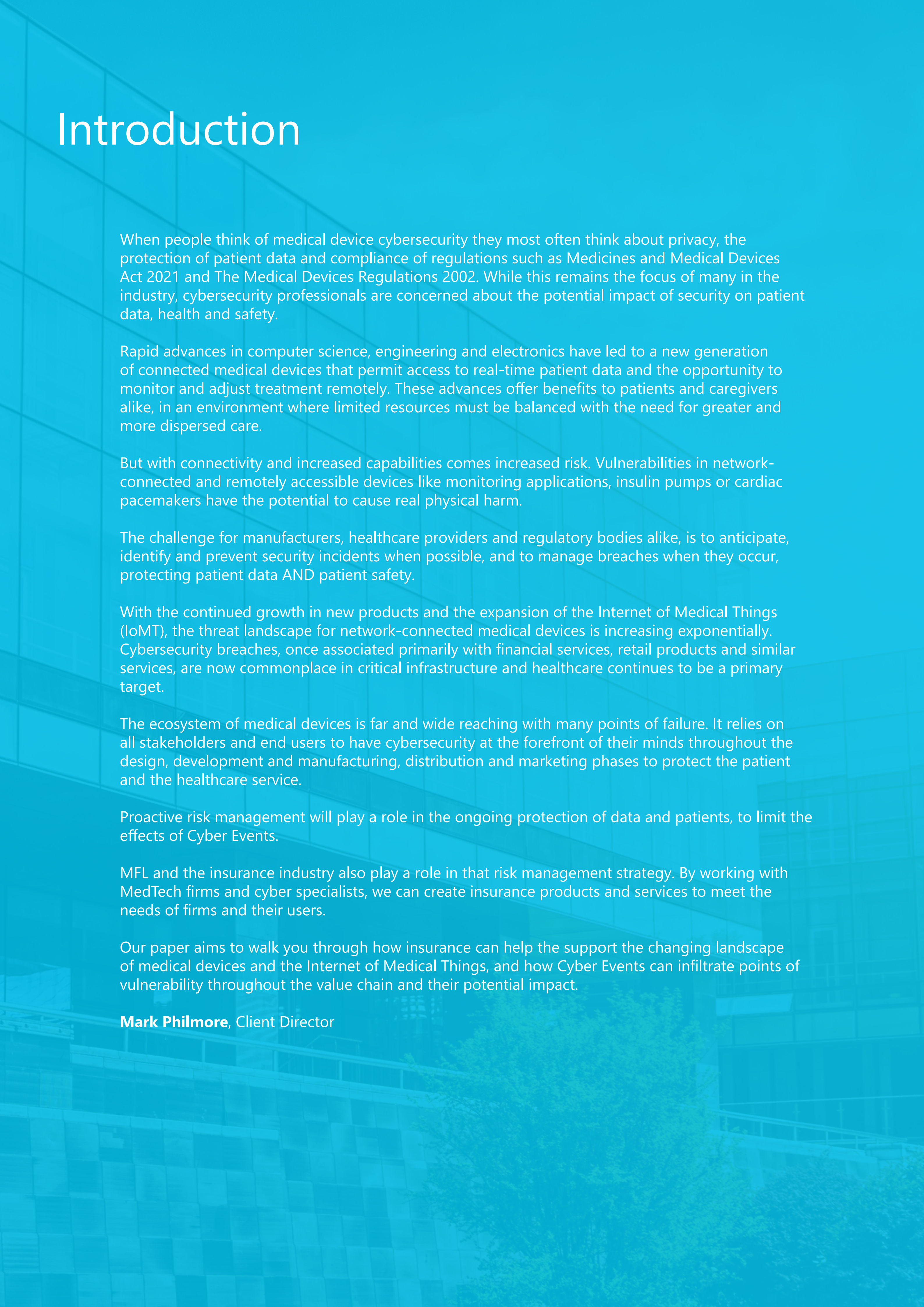
MFL
INSURANCE GROUP

MedTech and Data
Connected medical devices and cyber risks

www.mflinsurance.com



Introduction

When people think of medical device cybersecurity they most often think about privacy, the protection of patient data and compliance of regulations such as Medicines and Medical Devices Act 2021 and The Medical Devices Regulations 2002. While this remains the focus of many in the industry, cybersecurity professionals are concerned about the potential impact of security on patient data, health and safety.

Rapid advances in computer science, engineering and electronics have led to a new generation of connected medical devices that permit access to real-time patient data and the opportunity to monitor and adjust treatment remotely. These advances offer benefits to patients and caregivers alike, in an environment where limited resources must be balanced with the need for greater and more dispersed care.

But with connectivity and increased capabilities comes increased risk. Vulnerabilities in network-connected and remotely accessible devices like monitoring applications, insulin pumps or cardiac pacemakers have the potential to cause real physical harm.

The challenge for manufacturers, healthcare providers and regulatory bodies alike, is to anticipate, identify and prevent security incidents when possible, and to manage breaches when they occur, protecting patient data AND patient safety.

With the continued growth in new products and the expansion of the Internet of Medical Things (IoMT), the threat landscape for network-connected medical devices is increasing exponentially. Cybersecurity breaches, once associated primarily with financial services, retail products and similar services, are now commonplace in critical infrastructure and healthcare continues to be a primary target.

The ecosystem of medical devices is far and wide reaching with many points of failure. It relies on all stakeholders and end users to have cybersecurity at the forefront of their minds throughout the design, development and manufacturing, distribution and marketing phases to protect the patient and the healthcare service.

Proactive risk management will play a role in the ongoing protection of data and patients, to limit the effects of Cyber Events.

MFL and the insurance industry also play a role in that risk management strategy. By working with MedTech firms and cyber specialists, we can create insurance products and services to meet the needs of firms and their users.

Our paper aims to walk you through how insurance can help the support the changing landscape of medical devices and the Internet of Medical Things, and how Cyber Events can infiltrate points of vulnerability throughout the value chain and their potential impact.

Mark Philmore, Client Director

Mark Philmore ACII
Client Director

Mark heads up our Science and Technology division, working with new start-ups and established businesses.

Having worked in the insurance industry across underwriting and sales for over 35 years, and with MFL since 2003, Mark's experience is invaluable in designing insurance programmes for technology, gaming, science and life-sciences throughout the different development stages of your idea, product or business.

He loves to see businesses that we have been involved with from their inception succeed and thrive, knowing that we have, in a small way, played a part in their success.

Mark also looks after our partnership with Medilink, who are are a professional association and specialist consultancy for the life science sector in the North of England, where we support their members with their insurance requirements.

He is a qualified Chartered Insurance Broker and an Associate of Chartered Insurance Institute.

Corporate Partner

MEDILINK

The changing landscape for medical devices

Across the UK, there are approximately 6,300 life sciences businesses, generating an £80.7bn turnover, and employing more than 256,000 people.

The medical device industry is an important vertical in healthcare since it ensures the safety and well-being of people all over the world.

Innovation and access to new technologies have meant the healthcare ecosystem needs to be much broader than it was 20 years ago to achieve the future requirements of caregivers and patients whilst still achieving the quality demanded by modern medicine.

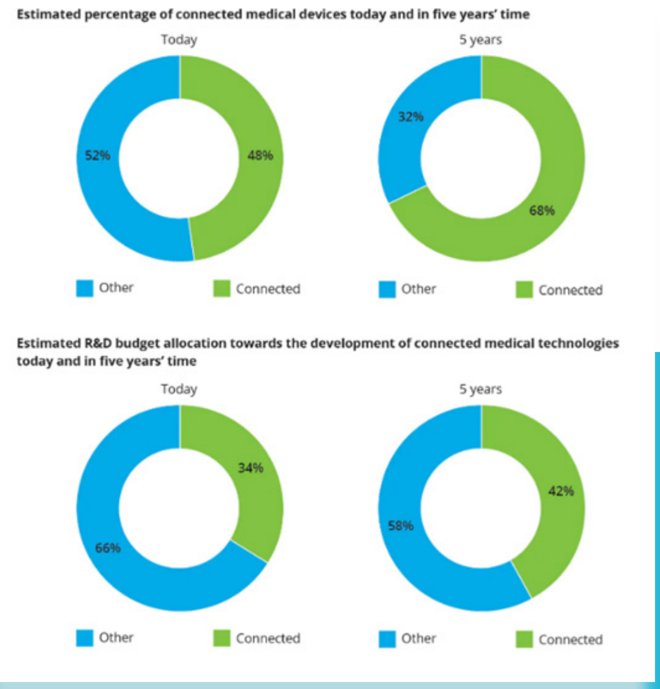
That means there needs to be a much larger healthcare footprint to innovate within, as medical devices and technologies look to improve illness screening, diagnosis and treatment, as well as the restoration and monitoring of health indicators to aid prevention.

The Internet Of Medical Things – IoMT

Over the past years, the Internet of Things (IoT) has evolved from a little-known technology into a reality that surrounds us everywhere. Smart homes and factories, wearables and smart sensors in transport take us to a new level of digitalisation. However, there are few industries in which IoT matters as much as it does in healthcare. Often, these devices are responsible not only for the convenience and speed of operations but also for human life.

The ecosystem where these devices and systems live is called the Internet of Medical Things (IoMT), which covers the entire set of sensors, data processing software and special infrastructure. IoMT helps provide patients with better care as well to optimise clinic processes and financial indicators.

A report published by Deloitte, included a survey of medical device companies with connected medical devices, where manufacturers anticipate an increase in the proportion of devices that are produced, as well as an increase in R&D investments.



Estimated percentage of connected medical devices today and in five years' time

Estimated R&D budget allocation towards the development of connected medical technologies today and in five years' time

Note. The figures from the Deloitte research survey relate to medtech companies with connected medical devices and are not representative of the medtech industry as a whole. Due to rounding the figures may not total 100 per cent. Source: Deloitte research commissioned from Research2Guidance, 2018

Key Challengers facing the IoMT

Whilst the face of our healthcare services and how we can monitor our health with wearable and monitoring devices in our homes will change, there are still key challengers facing IoMT:

Scale – a key challenge is ensuring health care organisations, clinicians and patients understand the value of connected medical devices and use them at scale to drive better economics and patient outcomes.

Regulatory change – managing the raft of regulatory change occurring is imperative for both developing connected medical devices and the success of the IoMT.

Cybersecurity – the increasing numbers and capability of connected medical devices present additional risks for data security. The scale and cost of breaches is often significant and far reaching.

Interoperability – for interoperability to work effectively, the direction of travel should be towards open platforms, based on open data standards. This will enable payers, providers and technology vendors to come together to make data more available to each another.

Maintaining trust in a digital age – as MedTech companies develop strategies and services based on the generation and transmission of patient data, they need to ensure they demonstrate clearly to patients, the public and health care professionals how their data is being used to reduce the risk of undermining the benefits that access to data can bring.

Funding, business and operating models – different types of innovation will require different business models, and progress will depend on both the innovators themselves working in new ways to take on risks and rewards.

Digital talent and building digital capability – there is increasing concern among key stakeholders that a growing skills gap will delay the deployment of IoMT solutions and constrain market growth and adoption.

Risk & Insurance– Standard policies are unlikely to cover the future needs of MedTech and Life Science businesses. Insurers will need to work with specialist Insurance Brokers to tailored Insurance products (e.g. Professional Indemnity, Product Liability, Cyber Cover, Clinical Trails, Director's & Officer's Insurance) to ensure businesses are not exposed to under-insurance or self-insurance.

Mark says

> The benefits of IoMT in medical devices is plain to see, which is evident in the anticipated increase in the number of devices and investment in the sector.
>
> Key to the success of businesses is fostering trust from stakeholders and end users. To achieve this a robust Cyber Security approach to gain trust from the patients and healthcare specialists is needed.
>
> When Cyber Events do occur, it is imperative that the insurance solutions you have in place cater for your specialists needs. Whilst one cyber-event could mean the end of your innovation, the damage of repeated cyber events across the sector could tarnish the reputation of all businesses.

Understanding the connected medical-device environment

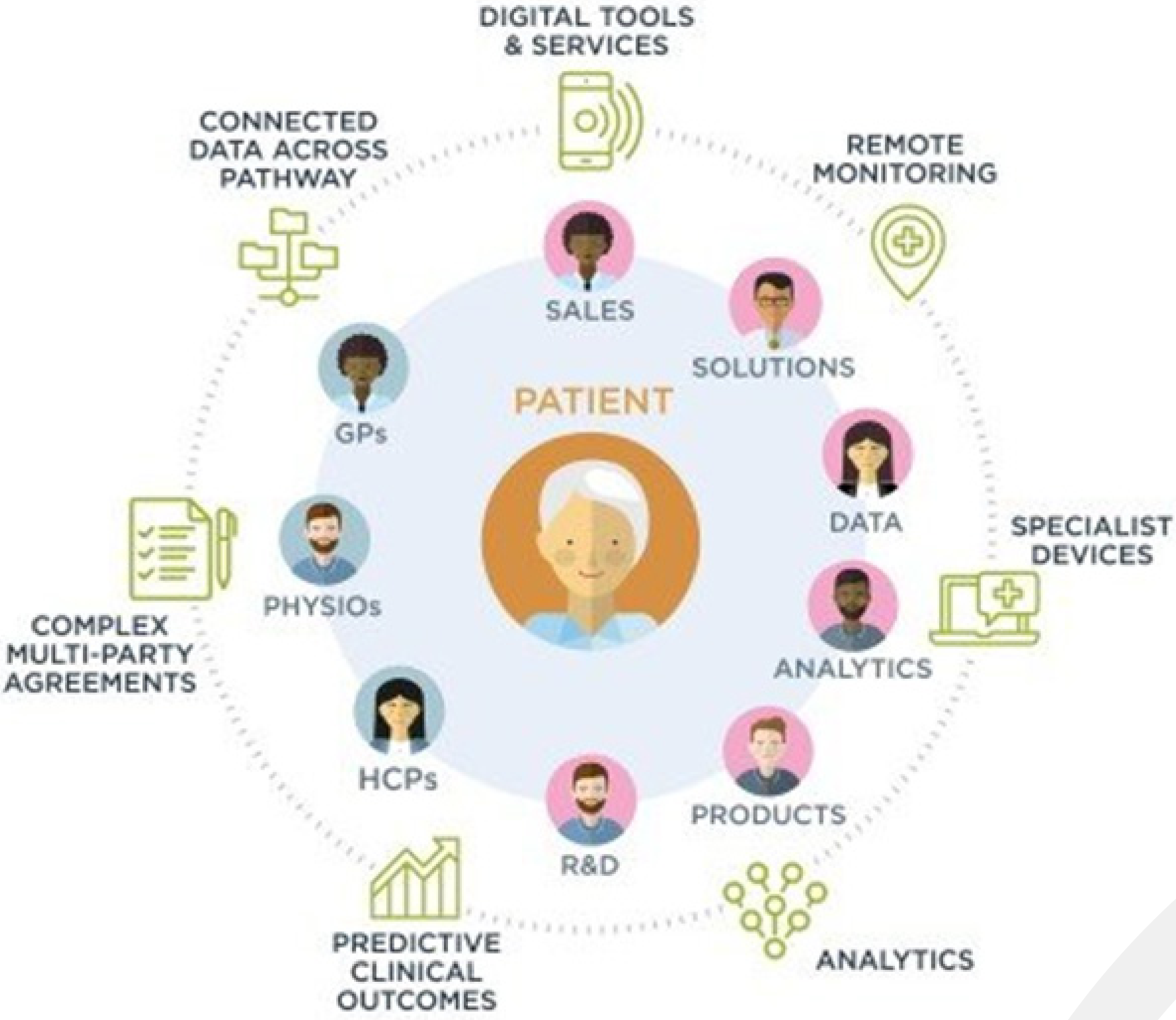
Home is where the healing is, or "care anywhere" is a phrase that is used by many care professionals when discussing the future. The pandemic accelerated many care delivery strategies as healthcare organisations increasingly evolve their care models to prepare for a future where the home becomes the central location of healing.

We saw a high volume of applications focused on supporting care in the home, including solutions for virtual specialty consults, hospital at home, remote patient monitoring and digital therapeutics.

This shift mirrors the classic, doctor house calls of old, but with a high-tech twist: the focus is definitely on high-quality healthcare brought directly to patients, where and when they need it, via virtual health technology.

Whilst Covid-19 increased the speed of change it brought with it a greater focus on improving healthcare standards, with less resource as our healthcare suffers from increased waiting lists and reduced healthcare professionals, and a downward pressure on cost control.

The result, or the opportunity, is for more and more outside innovators looking to create our healthcare services and products of the future.



https://www.paconsulting.com/insights/the-covid19-catalyst-for-MedTech/

Pinpointing the risks of connected medical devices

As the breadth and depth of services and products being offered to people continues to increase, the value chain, its stakeholders and how they work together to integrate their systems and technolgy, becomes more complex.

The complexity, and the risk, comes as the product or service moves through each phase of its journey. As suppliers and third-parties stakeholders are required to support the product or service through to commercialisation, vulnerabilites in the infrastructure and the technological bridges that connect them become system and procedural Points of Failure.

Risk Management, in particular Cybersecurity is a pivital part of that commercialisation journey. Where Points of Failure within the end-to-end product or service will be exposed and exploited by Cyber Criminals looking to 'hack' into systems for their own commercial gain.

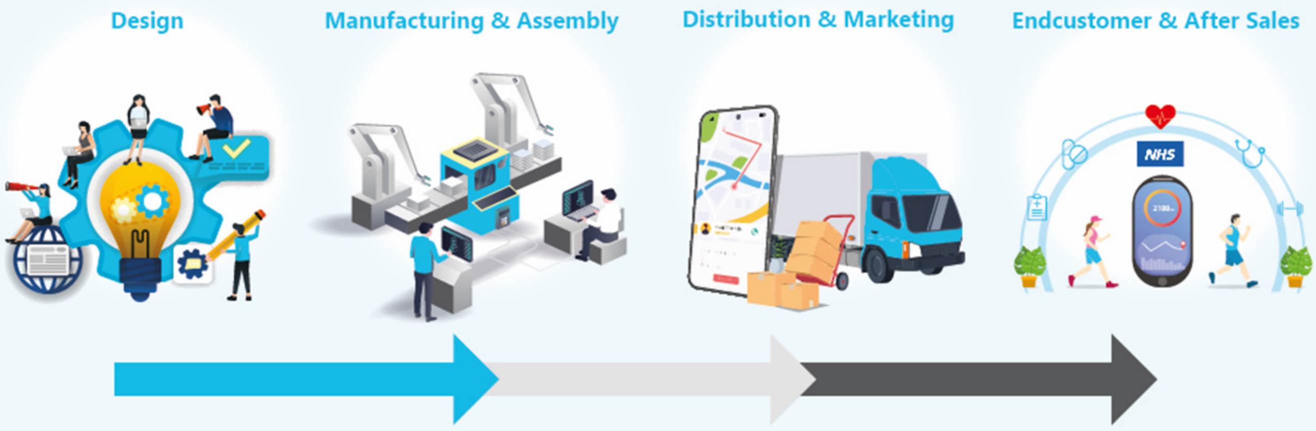
Definition

A single point of failure (SPOF) is essentially a flaw in the design, configuration, or implementation of a system, circuit, or component that poses a potential risk. It could lead to a situation in which just one malfunction, fault or intruder causes the whole system to stop working.

The below image is an example of a value chain, where each stage (or supplier) will have control of their systems. Each stage poses a SPOF in the value chain.

Depending on the interdependencies implicated in the failure and its location, a single point of failure may compromise workload availability or even the availability of the entire location/product. Productivity and business continuity decrease, and security is compromised.

If we consider that the failure of SPOF could provide an intruder access to patient data, then the impact of a breach could be more signigicant than temporary network outage.



How often do value chain shocks take place

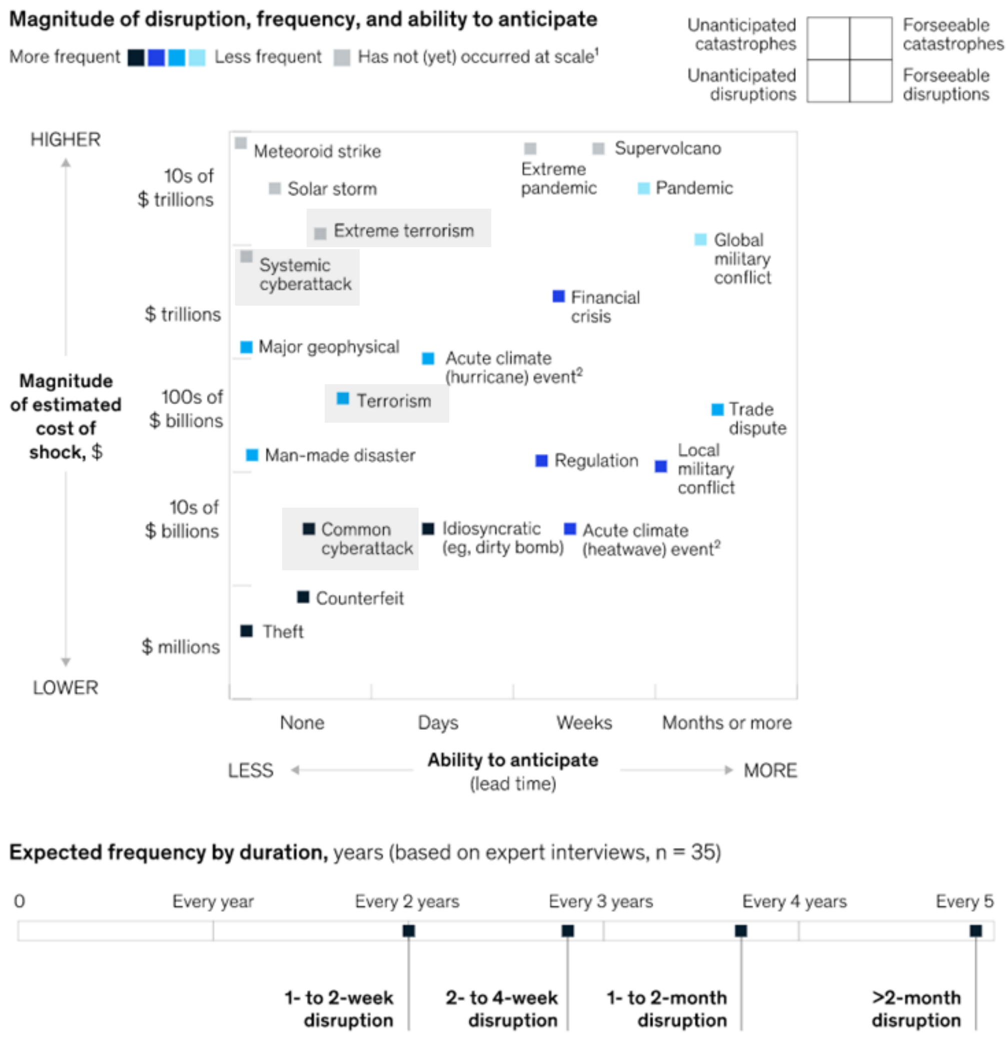
In recent years, companies have learned a lot about their value chains, as the pandemic exposed vulnerabilities in both supply-chain infrastructure and its performance—leaving many companies reflecting that, "we didn't know what we didn't know."

Now that these vulnerabilities have surfaced, there is an imperative to address them. The alternative could leave the same value chains exposed not only to future waves of the pandemic, plus other sources of disruption include force-majeure events (such as climate change or natural disasters), macroeconomic and political conditions (including trade-policy, regulatory changes or war), malicious actions (including cybersecurity events and intellectual-property theft), and counterparty issues (such as financially fragile suppliers).

Recent research from the McKinsey Global Institute (MGI) has highlighted that disruptions from a shock in one of these categories is frequent, and that on average, a shock lasting more than two months occurs every 3.7 years.

For many businesses that don't have a risk management strategy, of which selecting the correct insurance policies is included, may find that shocks can have a deterimental impact on their future viability.

Disruptions vary based on their severity, frequency, and lead time—and they occur with regularity.



[1]Shocks that have not occurred either at scale (eg, extreme terrorism, systemic cyberattack, solar storm) or in modern times (eg, meteoroid strike, supervolcano).
[2]Based on experience to date; frequency and/or severity of events could increase over time.
Source: McKinsey Global Institute analysis

McKinsey
& Company

Highlighted in the graphic are cyber incidents, which are by their nature impossible to predict but have a higher estimated cost / effect.

Using personal data in your medical device

Where your software based medical device is driven by personal data, there are legal requirements that often have real practical and technological implications - such as user verification, interface design, and the technical functionality and security of your products, tools, mobile apps and websites.

It is best to have a proper understanding of these requirements and bake them into your product during the Design phase, rather than try to make changes further down the line. The latter can trouble investors and customers about the maturity of your product, generate concerns amongst customers and end users about requests being made to change how their data is used, and often leads to patch updates to security protocols to protect the personal data and how its stored and used.

This should be seen as a potential Point of Failure as the ability to update all instances is challenging given the volume of devices you may have in healthcare settings or in the hands of your consumers / patients.

Key Design Principles

There are some key design principles you need to consider during the development of your connected medical device, these are:

Privacy by design - Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the regulations and there fundamental principles and requirements, and forms part of the focus on accountability.

- Your product must incorporate features that facilitate - rather than complicate - the ability of your organisation and your customers to achieve and demonstrate compliance with data protection, and of end users to exercise rights over their data.
- The use of mobile apps and privacy dashboards make this more immediate and accessible for end users while also increasing efficiency in managing consents, privacy notices, marketing and opt ins/outs.
- Providing individuals with easy ways to exercise their rights and more granular control over how their data is used can help you do new and exciting things with data (e.g. research, product development and AI).

Fair processing - to a large part, the extent to which personal data can be used and for what purposes depends on what individuals are told at the outset (in particular through privacy notices). Changing how data will be used usually requires updated privacy notices and terms of use for end users, and potentially contractual renegotiations with your customers, which can delay your plans and undermine trust.

Controllers and processors - whether or not you are a controller or processor (or both for different aspects of processing) will have a substantial impact on the responsibility and control you have over the data. Signing a standard data processing agreement with little thought to what it says is likely to seriously restrict your use of data. Which processors you use, and where in the world data will be hosted, will also have an impact on the complexity of your data protection compliance.

NHS policies and procedures - if being marketed to NHS customers, your app should interface with NHS systems, meet NHS information standards and facilitate NHS-specific policies, such as the national opt-out.

Accessibility - if deployed within the public sector, your app and website must meet accessibility standards.

Collaborations to develop your medical device

It is very likely that the development of your connected medical device will involve collaboration with other individuals or businesses. There are certain key issues to be aware of when entering into collaborations.

At the outset, this may be a collaboration with your business partners/ investors or third parties providing a particular contribution such as a software developer or hosted services. It is important to recognise these collaborations for what they are – a vital means of moving your product forward or its continual availability, but also the risk in terms of disclosure of confidential information, intellectual property, reliability and data theft.

To protect against this risk you should seek legal advice and have a standard form Non-Disclosure Agreement (NDA) that you can require your collaborators to enter into. You should also seek advice from your insurance broker, as to what insurances third parties should hold and for how long, and what you can include within your contractual agreements. For example, if you used a design or development agency, you may want to request that Professional Indemnity Insurance is held for a certain period of time at a specified level of cover, in case a claim arises against their works.

As your innovation, product or service develops you are likely to need more comprehensive contractual arrangements with your collaborators. This may lead to putting in place a Collaboration Agreement, for example involving your business, a university and a hospital trust with whom you are collaborating.

This agreement will document each parties' contributions and access to funding, as well as other key terms such as in relation to protection and exploitation of intellectual property.

It is important to put in place the right agreements at the right time. As your business develops your contractual arrangements will become increasingly important. They will provide certainty for your business, for example about ownership of your vital intellectual property, and this is certainly something investors will want to see, and something you will want to protect.

“Did you know

in many hosted service agreements, liability is excluded or restricted in the event of a data loss or cyber event.”

Vulnerabilities of devices in Healthcare Settings

Medical device manufacturers and hospitals are both responsible for protecting devices from cybersecurity threats and working together to manage the risks to patient safety.

While there is recognition of shared cyber responsibility on both sides, device security continues to be a casualty of the fast-moving digital world we live in.

Hospitals contend that many legacy devices and systems were not built with security in mind. Whilst MedTech firms are developing their products with security features during the initial Design phase.

The difference in circumstance can lead lack of coordination and transmission of data, which could put patients' lives in danger from outdated and unprotected medical devices.

Compounding the problem is a health system that can have tens of thousands of devices from hundreds of manufacturers connected to its network, creating an overwhelming cybersecurity management challenge for healthcare facilities already burdened with safeguarding their traditional IT assets.

Security for the life-time of the device

If cybersecurity risk is not effectively minimised or managed throughout the life of a device, it could potentially result in patient harm such as illness, injury or death as a result of delayed treatment or other impacts to device availability and functionality.

According to US cybersecurity firm Sensato, there is an average of 6.2 vulnerabilities per medical device, and the FDA (The Food and Drug Administration) has issued recalls for such critical devices as pacemakers and insulin pumps with known security issues, while more than 40% of medical devices are at the end-of-life stage, with no security patches or upgrades available.

In another example, researchers from the health care security firm CyberMDX, which was acquired in 2022 by the IoT security firm Forescout, found the seven easily exploited vulnerabilities, collectively dubbed Access:7, in the IoT remote access tool PTC Axeda. The platform can be used with any embedded device, but it has proven particularly popular in medical equipment. Attackers could potentially exploit the bugs to grab patient data, alter test results or other medical records, launch denial of service attacks that could keep health care providers from accessing patient data when they need it, disrupt industrial control systems.

"You can imagine the type of impact an attacker could have when they can either exfiltrate data from medical equipment or other sensitive devices, potentially tamper with lab results, make critical devices unavailable, or take them over entirely," says Daniel dos Santos, head of security research at Forescout.

Considertions of device security

How many devices are connected?

What types of devices are they?

e.g. phones, tablets, computers, printers, medical devices, wifi smart devices,

Which other devices or networks do they communicate with?

Is network behaviour normal and expected or anomalous

Fines from the ICO (Information Commissioner Office)

Data security incidents, under the UK General Data Protection Regulation (GDPR), are a major concern for those affected and a key area of action for the ICO.

A report by McAfee Enterprise and FireEye indicate that during the pandemic, 81% of global organisations experienced increased cyber threats with 79% experiencing downtime due to a cyber incident.
https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic

This increase in activity is in line with the increased ICO Penalty payments statistics, although 50% of this increase can be attributed to British Airways. ICO penalty fines are generally on a sliding scale based on the infringement type, with the higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

ICO and Government consultation

At the time of writing recently, the ICO issued guidance which provides clarity to health and life sciences companies relating to processing personal data for research purposes.

In the guidance, the ICO produces a non-exhaustive indicative list of activities and features that will help demonstrate that the purpose of processing is scientific research.

While it's not necessary to meet all of the features, the ICO stated that it would expect an organisation to meet more than one. This, therefore, appears to be somewhat of a balancing act.

- Activities could include formulating hypotheses, isolating variables, designing experiments, objective observation, measurement of data, peer review and publication of findings.
- Standards could include ethics guidance and committee approval, peer review, compliance with regulatory requirements and involving the public.
- Access could include publication of results and commitment to sharing research findings, however, this does not need to be open access publication
- These features are likely to be met where a health and life sciences organisation conducts a regulated clinical trial or clinical investigation. However, where the research falls outside of the regulatory formalities and in a commercial setting, including for artificial intelligence (AI) or product development, careful assessment is required.

The guidance is particularly relevant for life sciences, medical device and healthcare technology companies that use health-related data for research purposes, including as part of clinical trials, clinical investigations, or wider research. It's also relevant to health and life sciences companies that are looking to reuse data sets they already hold.

https://www.med-technews.com/MedTech-insights/MedTech-regulatory-insights/ico-draft-guidance-and-consultation-health-data/

Examples of fines

€1.5m

Health data leak disclosed in the press concerning nearly 500,000 persons in February 2021, the company Dedalus Biologie was fined 1.5 million euros.
https://edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en

£60k

St. George's Healthcare NHS Trust in London has been fined £60,000 by the UK Information Commissioner's Office after an individual's medical information was sent to the wrong address.
https://www.databreachtoday.co.uk/ico-fines-london-nhs-trust-a60000-a-4951

£35k

The Bayswater Medical Centre was fined £35,000 after it left highly sensitive medical information in an empty building
https://www.hayesconnor.co.uk/data-breach-claims/medical-data-breach-claims/

£325k

Brighton and Sussex University Hospitals NHS Trust, which was fined £325,000 for a breach involving hard drives containing healthcare information on tens of thousands of individuals that were sold on the Internet.
https://www.databreachtoday.co.uk/uk-health-records-breached-18-million-a-5261

€2.9m

Capio St. Goran is a Swedish healthcare provider that received a GDPR fine following an audit of one of its hospitals by the Swedish DPA. The audit revealed that the company had failed to carry out appropriate risk assessments and implement effective access controls. As a result, too many employees had access to sensitive personal data.
https://www.tessian.com/blog/biggest-gdpr-fines-2020/

Typical Cyber Events

The risks of cyber events are evolving rapidly, with new risks emerging as technology advances and new regulations are put in place.

Unfortunately, even some of the most tech-savvy individuals and businesses can fall victim to cyber events. While there are numerous types of criminal activities occurring online, there are a few common cyber events to be aware of:

Ransomware	Ransomware designed to block access to your computer system until a sum of money is paid.
Data breach	A Data Breach where sensitive data is copied, viewed, or stolen from your computer system.
Social Engineering, Data and Identity Theft	Social Engineering where individuals have been manipulated into divulging confidential or personal information that could be used for fraudulent purposes An example of this would be a phishing scam where the individual has received what looks like a legitimate invoice and pays it resulting in a misdirection of payment.
Human error	Human error e.g. losing a laptop with sensitive data on there.

How cyber criminals target vulnerabilities in infrastructure

Malware

Medical devices typically have no endpoint protection and are especially vulnerable to malware.

Inside threats

Due to weak authentication, malicious insiders can easily gain unauthorised access and tamper with devices

Web application attacks

Some medical devices are manageable via a web interface, creating a range of cyber risks such as code injection, cross-site scripting (XSS), DDos and path traversal.

Device misuse

Connected medical devices are often based on Windows PCs. Hospital staff can use the machines to browse the Internet or install software, creating additional risk

Spam attacks

Sophisticated attacks are capable of sending 300,000 emails per day in an atempt to gain access to a network or internet connected device.

Why are devices so vulnerable within Healthcare Settings?

- Software code has not undergone security review
- Authentication is weak or nonexistent
- Data transfer channels are often insecure and unencrypted
- Limited visibility over which devices are actively used
- Inability to monitor device activity and security incidents
- Decommissioned devices are not securely disposed of
- Software updates are unavailable, or rarely deployed

Mark Says

> **Many of these devices are not secure and are not actively managed, opening the door to a wide range of cyber-security threats.**

Insurance and how it has developed to address these issues

The origins of insurance policies mirrored how businesses historically operated.

If businesses manufactured physical items or provided advice or services for fees, their insurance policies were purchased on a standalone basis to reflect this.

Blended cover

As businesses developed and became multi-functional, for example, manufacturing and providing advice, the insurance industry transitioned to a blended approach to policy creation.

That meant that insurers provided blended products to make one product suitable for the business's risks instead of multiple standalone products, potentially leaving businesses with overlaps in cover.

The cycle of innovation and insurance

As the world develops, innovation (for example, the introduction and availability of the internet) brings new, previously unimagined risks, for instance, cyber-events.

These risks were never envisaged nor priced for by insurers.

For example, in most standalone policies, cyber-events were often not covered, and those that did provide cover, did so unintentionally by not specifically excluding them.

As a result, new policies, for example, Cyber Insurance, are created to help businesses manage their risk.

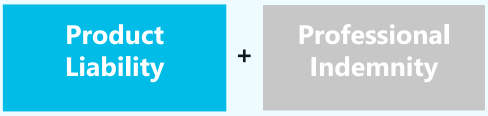
The future

As innovation within the (connected) medical device sector continues to increase, new risks will be created in relation to cyber events and data.

What we will see in the insurance sector is a further round of blending to create one product to cover all the risks a MedTech firm may need.

Some insurers have developed these 'all emcompassing' blended solutions but they are not yet at mass adoption.

Standalone products (then)

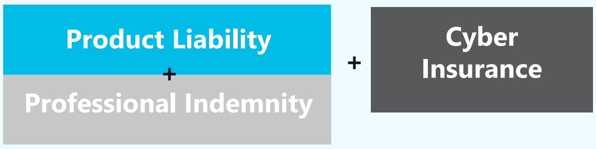


Product Liability + Professional Indemnity

Blended product (then)

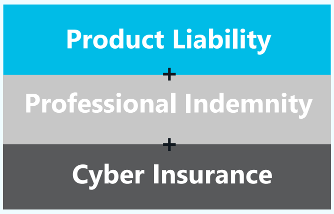
Product Liability + Professional Indemnity

Blended product (now) + new risks



Product Liability + Professional Indemnity + Cyber Insurance

Incoming / future product



Product Liability + Professional Indemnity + Cyber Insurance

9 reasons why healthcare is a big target for cyber-events

Private patient information is worth a lot of money to attackers

Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target. These organisations have to protect their patients' records.

Financial penalties – whether they be fines for not cooperating with GDPR or paying to retrieve their data from ransomware – are real and alarming for a healthcare industry that's already struggling with financing daily work demands.

IT professionals realise that the cost of securing their data with solutions like multi-factor authentication (MFA) is far less than the pay-out from ransomware or similar attacks. MFA is a solution that requires more than one piece of information to identify a user and then generates a one-time password on each login session, making it harder for hackers to steal passwords and other information.

Medical devices are an easy entry point for attackers

There aren't many downsides to innovations in healthcare technology these days. Medical devices like x-rays, insulin pumps and defibrillators play a critical role in modern healthcare. But for those in charge of online security and patient data protection, these new devices open up more entry points for attacks. Medical devices fulfill specific purposes – like monitoring heart rates or dispensing drugs. Security is not a primary concern in design. Although the devices themselves may not store patient data, attackers can leverage devices to launch an attack on a server that does hold valuable information. In a worst-case scenario, hackers can completely take over a medical device, preventing healthcare organisations from providing necessary life-saving treatment to patients.

Hackers know that medical devices don't contain any patient data themselves. However, they see them as an easy target, lacking the security found on other network devices like laptops and computers. Threats against medical devices can cause problems for healthcare organisations – giving hackers access to other network devices or letting them install costly ransomware. Secure network devices help limit the damage caused by an attack on medical devices.

Staff need to access data remotely, opening up more opportunities for attack

Collaborative working is vital in the healthcare industry, with units working together to provide the best solution for every patient. Those who need to access information aren't always sitting at their desk – they are often working remotely from different devices.

Connecting to a network remotely from new devices is risky, as not all devices will be secure. Additionally, healthcare staff are often unfamiliar with even the most basic cybersecurity best practices. Compromised devices must never gain access to the network, as just one hacked device can leave a whole organisation wide open. One option for organisations with staff working across devices is risk-based authentication (RBA). This solution makes risk analysis simpler by letting IT staff set up policies that determine the risk of a given device based on factors like the user, their location and more. Any unusual activity is then flagged to ensure that unsafe devices cannot access sensitive patient data.

Workers don't want to disrupt convenient working practices with the introduction of new technology

Healthcare staff are some of the busiest and most in-demand in the country. Staff work long hours and to tight deadlines – which means they don't have the time or resources to add online security processes to their workload. Medical professionals need slick working practices with minimal distractions.

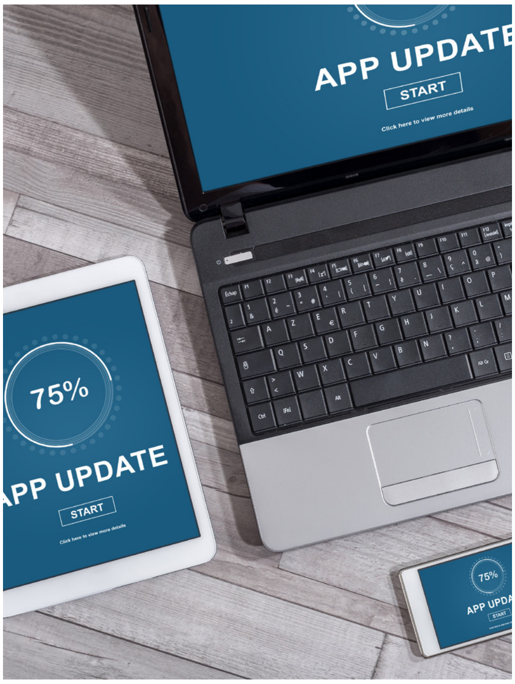
Healthcare organisations need to assess the impact of any cybersecurity measures they want to implement. IT staff should try to align security measures with existing software. Many authentication solutions work seamlessly with software like Office 365, meaning medical staff can perform their daily tasks without distraction.

Using Single Sign-On (SSO) solutions means authorised users can access multiple applications using just one set of login information – keeping their working routines quick and straightforward without compromising security. Frictionless solutions like SSO and RBA offer adequate protection against online threats without disrupting how people work.

Healthcare staff aren't educated on online risks

Medical professionals may not have the necessary expertise to recognise and mitigate online threats. Budget, resources, and time constraints mean it's simply impossible for all healthcare staff to be fluent in cybersecurity best practices.

Cybersecurity solutions are complex, but their interface needs to be simple. Medical staff requires a secure network that is quick and easy to access. And they need the peace of mind of knowing that patient data are protected. Solutions like MFA and SSO are becoming more popular as they use a secure one-time code – adding extra layers of security that don't require the user to know anything more than their login credentials.



The number of devices used in hospitals makes it hard to stay on top of security

Modern healthcare organisations are responsible for massive amounts of patient data, plus an extensive network of connected medical devices. Larger organisations can deal with thousands of medical devices connected to their network, each acting as a potential threat for attackers.

Healthcare staff are often too busy to stay educated on the latest threats to devices, leaving IT specialists with the task of protecting an entire hardware network against attacks. If just one device becomes compromised, it opens the whole network up to data breaches and medical device hacks.

There is a need for healthcare professionals to be able to manage their own devices to an extent – freeing up IT specialists to deal with broader IT and security issues within the network. Some MFA solutions offer a self-service portal, which allows users to reset security PINs and more by themselves, helping to lighten the workload on the support desk.

Healthcare information needs to be open and shareable

Confidential patient data needs to be accessible to staff, on-site and remotely, and on multiple devices. The typically urgent nature of the medical industry means a team needs to be able to share information immediately. There's no time to pause and consider the security implications of their devices.

The worry for IT staff is that the devices used to share information are not always protected. They can't always be there to assess the credentials of every device, especially in a time-critical environment. Users accessing data remotely will only need privileges for their tasks to perform. So, if they're checking their emails, they won't need to have full admin account privileges—precautions like this limit the chance of admin accounts becoming compromised.

Any solution that can save time and money by automatically regulating user permissions without putting patient data at risk is a must-have for healthcare companies. MFA solutions prevent attacks from compromised credentials or unauthorised users to ensure only the right people can access sensitive data.

Smaller healthcare organisations are also at risk

All healthcare organisations are at risk from online threats. Large enterprises hold the most data, representing a bounty for attackers and placing them as common targets. But smaller enterprises have smaller security budgets. Less complex and up-to-date cybersecurity solutions mean smaller enterprises are often seen as an easy target and a backdoor-access opportunity to target larger companies.

Effective cybersecurity solutions have become a must for healthcare organisations, as they're all in charge of sensitive patient data. Healthcare leaders are becoming more aware of the need to increase spending on cybersecurity – and there are plenty of solutions out there that are scalable to different business sizes. MFA solutions provide extra layers of security to your devices, using a combination of user passwords and one-time information that works for your company, and prevent attackers from stealing login information.

Outdated technology means the healthcare industry is unprepared for attacks

For all the incredible advances in medical technology in recent years, not every aspect of the healthcare industry has kept pace. Limited budgets and a hesitancy to learn new systems often mean that medical technology is becoming outdated. Hospitals using techniques that still release system updates should keep all software equipped with the most recent version.

These usually contain bug fixes to keep systems reasonably secure. But eventually, the software will become end-of-life, and vendors will stop providing updates. Where it's not feasible to upgrade to different, more secure software – or where medical staff don't want the hassle – it's possible to minimise the risk of cyberattacks by adding extra layers of security. If one system is compromised, then an MFA solution can limit the lateral movement of an attacker through the network, as they won't be able to log in to other protected systems.

Healthcare organisations are responsible for reacting to the latest online threats to keep their patient data secure. It's essential to allocate a budget and invest in the right solution for your enterprise. Consider how your staff like to work and keep on top of new threats as they emerge – before your systems become outdated and you struggle to protect all your devices.

About MFL

Supporting Life Science buinesses since 1997

Insurance partner to MediLink North and its members

Works with thousands of clients across the

Relationships with specialist insurers and underwriters

Deep understanding of Life Science and MedTech businesses

Corporate Partner

MEDILINK

For further information please contact the team:

Mark Philmore ACII, Chartered Insurance Broker
0113 323 1042 | 07966 233287 | mp@mflinsurance.com

www.mflinsurance.com

MFL
INSURANCE GROUP

CELEBRATING 1997-2022 25 YEARS

Affinity | Corporate | Professions | Science & Technology | Underwriting

This guide does not present a complete or comprehensive statement of the law, nor does it constitute legal advice. It is intended only to highlight issues that may be of interest to in respect of intellectual property and intellectual property insurnace. Specialist advice should always be sought in any particular case..

MFL Insurance Group Ltd is authorised and regulated by the Financial Conduct Authority, FRN No. 306684.
Register Address Barlow House, Minshull Street, Manchester M1 3DZ. Registered in England and Wales, No. 02817700.