Building a safer future in Healthcare

The best vaccine against risk

Since it first began to spread around the world in early 2020, the coronavirus pandemic has forced healthcare providers globally to work under more extreme and constant pressure than professionals in any other sector.

But even as the global threat from COVID-19 has evolved into the 'new normal', another pandemic has shown no signs of abating, with a rate and severity of attacks on healthcare providers that's completely off the scale — including the highest number of reported data breaches by any industry sector in 2021.

According to the non-profit Center for Internet Security, 'The healthcare industry is plagued by a myriad of cybersecurity-related issues. These issues range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care.

'While other critical infrastructure sectors experience these types of attacks, the nature of the healthcare industry's mission poses unique challenges. For healthcare, cyber-attacks can have ramifications beyond financial loss and breach of privacy. Ransomware, for example, is a particularly egregious form of malware for hospitals, as the loss of patient data can put lives at risk.'

There is, however, a much brighter side to this particular coin. According to Adobe's 2021 Healthcare Trends Report, global health spending continues to increase dramatically, with the market projected to surpass $10trn by 2022, driven by a response to the COVID-19 crisis that has opened the doors to new ideas, accelerating innovation and creating a lasting shift in customer behavior.

In this whitepaper we'll therefore examine not only the impact of cybercrime on the global healthcare sector, but more importantly how providers can embrace and fully exploit the opportunities presented by this new wave of innovation — by understanding and minimizing the risks of digital transformation, and implementing the associated technologies **securely.**

Why is medical data so attractive to cybercriminals?

- **Its richness and sensitivity make it extremely valuable.**
- **It needs to be open and shareable — including being accessed remotely, opening new doors to attack.**
- **Due to budget restrictions, many healthcare providers operate outdated technology which they lack the specialist IT resources to properly defend.**
- **The limited security of medical devices makes them relatively easy entry points for cybercriminals.**
- **Many healthcare staff aren't educated in how to recognize and deal with the most basic cyberthreats.**

Small and medium-sized practices under increased pressure from cyberattacks

2020 saw cyberattacks on healthcare organizations increase significantly. While large healthcare organizations are being targeted by Advanced Persistent Threat (APT) groups and ransomware gangs, there has also been a marked increase in attacks on small- to medium-sized healthcare organizations.

A cyberattack on a large healthcare organization could allow the hackers to steal large quantities of protected health information, and ransomware attacks typically see ransom demands issued for millions of dollars. The rewards from these attacks are considerable, but large healthcare organizations tend to invest heavily in cybersecurity and often have their own IT security teams to protect and monitor their IT networks. Cyberattacks on these organizations require more skill and they can be difficult and time consuming.

Medium-sized healthcare organizations also store large amounts of sensitive data, yet their networks tend to be less well protected, which makes cyberattacks much easier and still highly profitable.

Just how difficult is it out there?

Global figures for the cyberthreats to which healthcare providers are exposed are so enormous that they can be difficult to visualize in terms of the pressures being exerted on the IT teams tasked with protecting their organizations from attack.

To help put these into context, we'll start by looking at the scale of recent cyberattacks reported at individual country level, together with the impacts on two US healthcare providers that were victims of ransomware attacks.

In the US, HIPAA Journal regularly reports on emerging cyberthreats and the issues they create for healthcare providers, while multinational law firm Pinsent Masons has looked at cyberattacks affecting healthcare providers in several European countries.

- In the **US**, HIPAA Journal reported that in July 2021, HIPAA-covered entities and their business associates reported 70 data breaches of 500 or more records, making it the fifth consecutive month where data breaches had been reported at a rate of two or more per day. Over the 12 months from August 2020 to July 2021 there were 706 reported healthcare data breaches of 500 or more records, and the **healthcare data of 44,369,781 individuals had been exposed or compromised**.
- In **Germany**, the federal government reported that **the number of successful cyberattacks on health service providers operating critical infrastructure more than doubled in 2020** compared to 2019. In a widely reported incident in September 2020, 30 servers at Dusseldorf University Hospital were held to ransom, resulting in surgery being cancelled, the emergency room closed, and a female patient reportedly dying because her ambulance had to be redirected to another hospital.
- In **France**, media reported 27 major cyberattacks against health institutions in 2020, while in 2021 providers faced around **one major ransomware attack per week**.
- In **Spain** during 2020, authorities identified up to **50,000 harmful attacks** against organizations in the health sector, of which 375 were successful.
- In **Ireland** in May 2021, a ransomware attack was detected on the Department of Health's network, **severely disabling a number of HSE systems and necessitating the shutdown of the majority of its other systems**. As a result, services relying on digital processes such as scans, referrals and diagnostic services needed to be operated manually, causing extensive delays.

So what are the consequences for a healthcare provider when it falls victim to one of these kinds of attack? As reported by HIPAA Journal, ransomware attacks on hospitals can cause huge disruption and financial losses — as attacks on US healthcare providers Universal Health Services (UHS) and Scripps Health clearly demonstrate.

UHS is one of the largest healthcare providers in the US, operating 26 acute care hospitals, 330 behavioral health facilities and 41 outpatient facilities. UHS said in March 2021 that its September 2020 Ryuk ransomware attack resulted in $67 million in pre-tax losses due to the cost of remediation, loss of acute care services, and other expenses incurred due to the attack.

Scripps Health is a California-based nonprofit operator of five hospitals and 19 outpatient facilities. In a May 2021 ransomware attack, the provider lost access to information systems at two of its hospitals, staff couldn't access the electronic medical record system, and its offsite backup servers were also affected. Without access to critical IT systems it was forced to reroute stroke and heart attack patients from four of its main hospitals, and trauma patients could not be accepted at two hospitals.

Scripps Health took four weeks to recover from the attack. Losses sustained as a result of it were reportedly expected to exceed $113 million. Of this, $91.6 million was due to lost revenue during the four-week recovery period, and $21.1 million had to be spent on response and recovery. With the protected health information of 147,267 patients compromised in the attack, several class action lawsuits were also filed against the provider over the theft of patient data.

With potential losses on this kind of scale, the costs of investing in cybersecurity capable of defending against these attacks pale into insignificance. So where exactly are healthcare providers' vulnerabilities coming from, how can these be expected to evolve, and how can providers better defend against them?

5 biggest healthcare security threats for 2021

Healthcare organizations can expect ransomware, botnets, cloud misconfigurations, web application attacks and phishing to be their top risks.

Cyberattacks targeting the healthcare sector have surged because of the COVID-19 pandemic and the resulting rush to enable remote delivery of healthcare services. Security vendors and researchers tracking the industry have reported a major increase in phishing attacks, ransomware, web application attacks, and other threats targeting healthcare providers.

Key healthcare trends and how to manage them securely

Leading commentators such as Deloitte, Forbes, McKinsey and Adobe have highlighted what they see as the key trends affecting healthcare providers in 2021 and beyond. Deloitte, for example, has stated that 'COVID-19 is accelerating change across the ecosystem and forcing public and private health systems to adapt and innovate in a short period,' and that 'Digital transformation can help individual health care organizations and the wider health ecosystem improve ways of working, expand access to services, and deliver a more effective patient and clinician experience.'

Based on a combination of these analyses and our own experiences in working with healthcare providers around the world, there are five interrelated trends we believe organizations need to deal with securely if they are to avoid the kinds of cyberattacks we've spoken about above, and benefit from the improvements in health outcomes enabled by digital transformation.

Healthcare has the costliest data breaches

Healthcare data breaches are the costliest, with the average cost increasing by $2 million to $9.42 million per incident. Ransomware attacks cost an average of $4.62 million per incident. The large year-over-year increase in data breach costs has been attributed to the drastic operational shifts due to the pandemic. With employees forced to work remotely during the pandemic, organizations had to rapidly adapt their technology. The pandemic forced 60% of organizations to move further into the cloud. Such a rapid change resulted in vulnerabilities being introduced and security often lagged behind the rapid IT changes. Remote working also hindered organizations' ability to quickly respond to security incidents and data breaches.

Trend #1: Virtual care and remote medicine

In many advanced economies, the shift from face-to-face appointments to consultations by phone or video resulting from COVID-19 has been dramatic. When the pandemic struck, the last thing overworked doctors and nurses wanted was direct contact with patients potentially infected with the virus, while the last thing those patients wanted was to spend time in busy waiting rooms for exactly the same reason.

This, combined with the lockdowns imposed by governments around the world, drove citizens in almost all demographics online in previously unimaginable numbers, including enormous increases in the numbers of remote telehealth visits between patients and clinicians – completely changing the standard processes for everything from doctor's appointments to hospital treatments.

Clearly, there will always be patients who prefer to discuss their healthcare issues with a trusted practitioner in a normal clinical setting. But now the technology to support virtual care and remote medicine has become widely available, there are many good reasons for it to continue to flourish — especially when patients can receive the same level of care as they would from a visit to a doctor's surgery or outpatient clinic, but without having to leave their home.

For overstretched medical professionals, remote diagnosis and treatment enable more patient consultations to be squeezed into their busy schedules, and can also reduce the impact of missed appointments.

How to manage virtual care and remote medicine securely

In many respects, the challenges involved in securing virtual care and remote medicine are very similar to those resulting from the explosion in remote working.

For patients of doctor's surgeries, for example, clogged phone lines and the difficulty of speaking to overworked receptionists mean it can be preferable to arrange appointments or order repeat prescriptions via text, email or the surgery's web portal – all of which need to be effectively defended.

Also, following a remote consultation, patients may be required to upload photos, videos or other information directly to their medical records — necessitating a level of cybersecurity very similar to that of remote workers being granted access to corporate systems.

For years now, there's been a well-defined structure to the threat landscape that's been relatively straightforward for organizations to defend themselves against – as run-of-the mill commodity threats targeting their endpoints have been the #1 means for attack. Being armed with a well-equipped endpoint protection platform (EPP) has therefore provided a high degree of confidence that their organization is secure.

Unfortunately, this situation is changing rapidly. In the new threat landscape, threats targeting endpoints are becoming increasingly 'evasive'. Specifically designed to bypass existing endpoint protection, these threats are hard to detect thanks to the range of evasion techniques being adopted – particularly the use of legitimate and system-native tools.

Not only are evasive threats harder to defend against, they're also more prevalent. This is because it's now easier and cheaper than ever for cybercriminals to find, combine and test ready-made tools, methods and attack scenarios — and attacks of this type promise much higher chances of success than traditional scenarios.

And of course, by staying undetected for longer, evasive threats have the time to explore and entrench themselves into an organization's infrastructure and cause the greatest amount of damage — be it a data breach, ransomware attack, directly overriding operations etc.

Trend #2: Data security and cloud adoption

Like many aspects of digital transformation, unrelenting increases in both the quality and quantity of patient data held by healthcare providers has both upsides and downsides.

On the plus side, every piece of data collected about citizens' health – from their discussions with local health professionals to the data recorded by their online searches, mobile phones, fitness trackers and other wearables — helps give healthcare providers a clearer understanding of how and where treatments and interventions may be needed.

The pandemic has also demonstrated the extent to which people are willing to share their personal data as long as the benefits of doing so are clearly communicated.

In the UK, the NHS's COVID-19 track-and-trace app (designed to identify when an individual has spent more than 15 minutes within two metres of someone who subsequently tests positive for the virus, and is therefore required to self-isolate) was one of the most divisive aspects of the government's pandemic response, prompting accusations of state snooping and excessive surveillance. Yet by July 2021, almost 27 million people in England and Wales (around 45% of the population) had downloaded and installed the app.

Conversely, a plan to make GP health data for everyone in England available to researchers and companies for healthcare research and planning highlighted just how strong citizens' privacy concerns over sensitive health data can be. The plan had to be abandoned following a huge public outcry in August 2021, during which more than a million people opted out of NHS data-sharing in just one month.

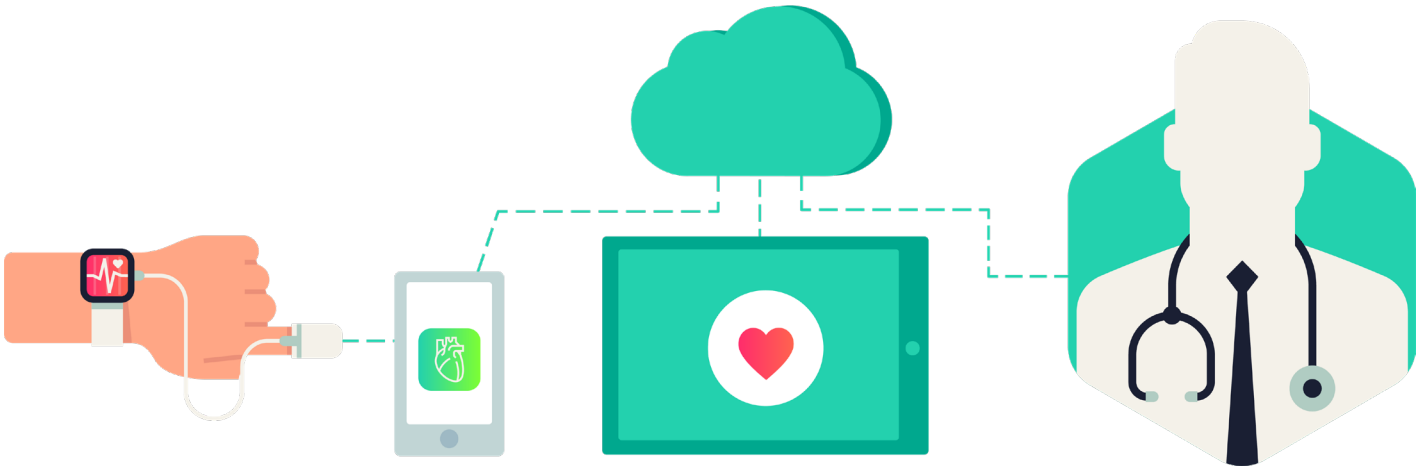
This puts healthcare providers in a difficult position. Delivering a seamless healthcare experience often requires collaboration between different providers, who therefore need to share sensitive patient data while working within the boundaries of government regulation. But to continue to drive healthcare innovation such as that envisaged by the NHS data-sharing initiative, they need to be able to reassure citizens that their data is safe and secure, and that the information they're being asked to provide is justified by the quality, capabilities and personalization of the healthcare services being offered to them.

Healthcare industry has highest number of reported data breaches in 2021

Data breaches declined by 24% globally in the first 6 months of 2021 according to the 2021 Mid-Year Data Breach QuickView Report from Risk-Based Security. The company identified 1,767 publicly reported breaches between January 1, 2021 and June 30, 2021. Across those breaches, 18.8 billion records were exposed, which represents a 32% decline from the first 6 months of 2020 when 27.8 billion records were exposed.

The report confirms the healthcare industry continues to be targeted by cyber threat actors, with the industry having reported more data breaches than any other industry sector this year. Healthcare has been the most targeted industry or has been close to the top since at least 2017 and it does not appear that trend will be reversed any time soon. 238 healthcare data breaches were reported in the first 6 months of 2021, with finance and insurance the next most attacked sector with 194 reported incidents, followed by information with 180 data breaches.

One way that providers are looking to achieve this is through increased cloud adoption. McKinsey, for example, has said that 'broad consensus exists that the use of cloud technologies could unlock digital and analytics capabilities across the healthcare spectrum…' by 'enabling them to more effectively innovate (for example, new use cases in analytics, IoT, and automation), digitize (for example, stakeholder journey transformation), and realize their strategic objectives.'

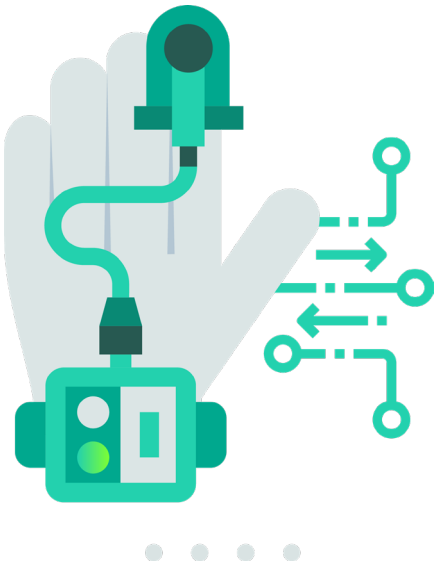


How to manage data and cloud adoption securely

Unfortunately for healthcare providers, the financial value of patient records has turned many hospitals and clinics into the equivalent of a poorly protected bank in a Wild West movie. But whereas in the movies, outlaws ran the risk of losing their lives to an unexpectedly well-armed sheriff, now all cybercriminals have to do is buy a cheap ransomware kit on the dark web, or, for a more sophisticated attack, purchase ransomware-as-a-service including a technical support hotline, advice on which organizations and/or individuals to target and how, and specialist expertise to help negotiate, secure and launder the ransom.

Breaches can also result from everything from unpatched legacy systems to human error or deliberate fraud. But whatever the cause, breaches threaten patient confidentiality and can damage an organization's reputation.

Endpoints — including servers, workstations and mobile devices — are the source of the majority of cybersecurity problems encountered by organizations. As a result, high quality endpoint protection has to be the first line of defense against attempted security breaches. And those planning to or already moving medical data to public, private or hybrid cloud environments also need to invest in specialist cybersecurity specifically designed to secure these workloads.



Lack of oversight of cybersecurity of networked medical devices in hospitals

Cybersecurity controls are required to protect medical devices that are connected to the internet, other medical devices, or internal hospital networks. Without those controls, the devices could be accessed by unauthorized individuals and patients could be at risk of harm.

If cybersecurity controls are lacking, devices could be vulnerable to an attack that could potentially impact critical healthcare systems. While there have not been any known cases of cyberattacks being conducted specifically to cause patients harm, patients may inadvertently be harmed as a result of an attack conducted for other reasons.

Trend #3: AI and the Internet of Things (IoT)

Citizens and patients may not necessarily be aware of it, but artificial intelligence (AI), the Internet of Things (IoT) and Internet of Medical Things (IoMT) are transforming healthcare by performing the same tasks humans do, but more efficiently, more quickly and at a lower cost.

McKinsey has detailed how AI has the potential to transform how healthcare is delivered, by supporting improvements in care outcomes, patient experience and access to healthcare services; increasing productivity and the efficiency of care delivery, and allowing healthcare systems to provide more and better care to more people; and helping to improve the experience of healthcare practitioners, enabling them to spend more time in direct patient care and reducing burnout.

PWC has highlighted eight key ways in which this is already underway through AI and robotics, including:

- Keeping citizens well – by encouraging healthier behavior in individuals, and helping healthcare professionals better understand the day-to-day patterns and needs of the people they care for.
- Early detection – for diseases such as cancer, early-stage heart disease and other life-threatening episodes.
- Medical diagnosis – by combining AI and machine learning to analyze vast medical datasets.
- Better decision making – based on big health data, pattern recognition and predictive analytics.
- Improved treatment – through more comprehensive disease management.
- End of life care – including using robotics to help people remain independent for longer.
- More insightful research – by streamlining drug discovery and drug repurposing.
- Enhanced training – including learning from previous responses.

IoT/IoMT, meanwhile – especially when combined with 5G mobile communication – is opening the door to advances ranging from virtual hospitals and wards, remote patient monitoring, wearable biosensors for glucose, heart rate etc., smart thermometers, connected inhalers and automated insulin delivery systems, to assistance for the elderly, hand hygiene monitoring, depression and mood monitoring, Parkinson's disease monitoring, ingestible sensors, connected contact lenses and many, many more.

But as outlined above, each of these advances brings further concerns around data and data security. **If the volume of data currently produced by medical devices has felt like a flood, IoT/IoMT are destined to unleash a tsunami of new big data — opening up previously unthought-of applications for AI, but also a new level of complexity in processing, managing and securing this ever-more sensitive data.**

In tandem with this, the poor security of the majority of IoT/IoMT devices creates its own threats. Who, for example, would want to use an automated insulin delivery system if there was even the remotest possibility it could be hacked?

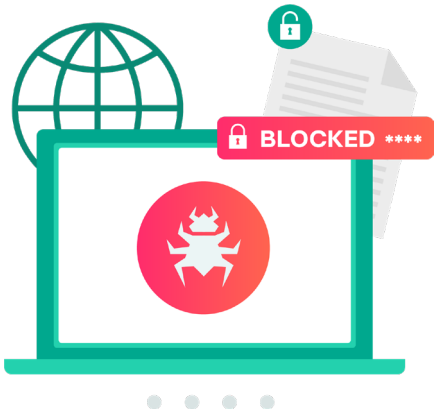
The sheer number of connected devices already creates huge administrative headaches for healthcare providers. It's estimated that a large hospital can have around 85,000 medical devices connected to its network, including MRIs, computed tomography, ultrasound, nuclear medicine and endoscopy systems, as well as systems communicating with clinical laboratory analyzers such as laboratory information systems. But these numbers may soon appear as nothing compared to what IoT/IoMT means IT security teams will be tasked with dealing with in the future.

How to manage medical devices and IoT/IoMT securely

Connected medical devices are an integral part of modern healthcare and patient care, but the security risks associated with them can be difficult to understand and mitigate. Clinics providing staff with mobile devices to facilitate their work can also face serious issues due to lack of centralized security management.

Medical devices face the risks of being a part of the corporate network, as well as those unique to the embedded systems on which they're based. Traditional antivirus solutions, however, cannot fully defend against the latest advanced, targeted and malware threats to embedded systems, including medical equipment. Embedded systems in medical devices therefore need more than antivirus – requiring cybersecurity based on a combination of Default Deny with Device Control.

IoT devices, meanwhile, require the implementation of specialist security across the IoT/IoMT ecosystem – minimizing risk and addressing cybersecurity threats to IoT systems and embedded devices through tools securing every software and hardware component of these interconnected systems — without overloading individual systems or devices or limiting overall flexibility.



Trend #4: The relentless challenge of ransomware

Healthcare hacking incidents increased by 42% in 2020

Healthcare hacking incidents increased by 42% in 2020, continuing a five-year trend that has seen hacking incidents increase each year. 470 incidents were classed as hacking-related breaches, which accounted for 62% of all breaches in the year. 31,080,823 healthcare records were compromised in the 277 incidents where the number of affected individuals is known. Many of the 2020 hacking incidents involved the use of ransomware.

It's impossible to overstate the scale of the disruption and other unique challenges posed to healthcare providers by ransomware.

We've already discussed the damage inflicted on US providers UHS and Scripps Health, but these are just the tip of the iceberg. It's often been said that when it comes to technology, where the US leads the rest of the world follows. So it's well worth reviewing these comments and statistics from HIPAA Journal, which really speak for themselves.

- The first known ransomware attack occurred in 1989 but early forms of ransomware were not particularly sophisticated and attacks were easy to mitigate. The landscape changed in 2016 when a **new breed of ransomware started to be used in attacks. These new ransomware variants use powerful encryption, and delete or encrypt backup files** to ensure data cannot be easily recovered without paying the ransom.
- Over the past five years ransomware has been a constant threat to the healthcare industry, with healthcare providers being increasingly targeted in recent years. **Attacks now see sensitive data stolen prior to file encryption**, so even if files can be recovered from backups, payment is still required to prevent the exposure or sale of stolen data.

- **Healthcare ransomware attacks cripple IT systems, prevent patient medical records from being accessed, cause disruption to patient care, and put patient safety at risk**. Recovering data and restoring systems can take weeks or months and mitigating the attacks is expensive, with considerable loss of revenue due to downtime.
- 2020 was a particularly bad year for the healthcare industry with record numbers of data breaches reported. Ransomware was a major threat, with Emsisoft identifying 560 ransomware attacks on healthcare providers in 2020. Those attacks cost the healthcare industry dearly. $20.8 billion was lost in downtime in 2020, according to Comparitech, which is more than twice the ransomware downtime cost to the healthcare industry in 2019.
- In 2020, network intrusion incidents and ransomware overtook phishing, which had been the main cause of data breaches for the past five years, as the leading cause of healthcare data security incidents. Ransomware attacks are now the attack method of choice for many cybercriminal organizations and have proven to be very profitable.

How to defend against ransomware securely

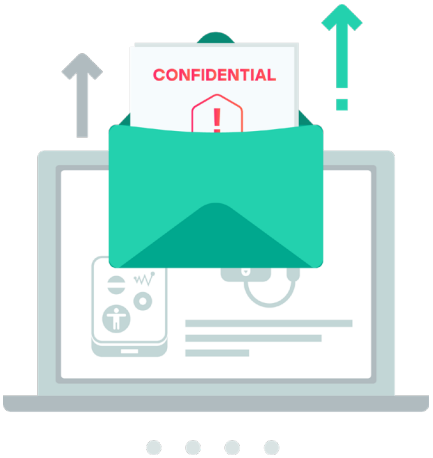
Ransomware has no place in society — let alone healthcare — which is why we're so determined to eradicate it through our participation in initiatives such as No More Ransom. This free online resource offers advice on ransomware prevention, and answers to questions on a range of topics including different types of ransomware, whether or not to pay a ransom, how to decrypt files encrypted by ransomware and more.

For organizations unfortunate enough to have suffered an attack, the site also provides a Crypto Sheriff to identify the specific type of ransomware affecting a device, and whether one of the hundreds of free tools available on the site is able to decrypt it.

Clearly, however, it's far better to try to avoid becoming a victim of ransomware in the first place, for which No More Ransom offers a range of advice including:

- Keeping corporate devices' operating systems and applications updated
- Knowing your assets and compartmentalizing them
- Securing access to Remote Desktop Protocols (RDPs)
- Monitoring data exfiltration
- Regularly testing your systems
- Reducing the likelihood of malicious content reaching your networks
- Using enhanced passwords and changing them on a regular basis
- Using strong authentication

- Managing the use of privileged accounts
- Securing your teleworking equipment
- Installing apps from trusted sources only
- Being wary of accessing company data through public Wi-Fi
- networks
- Providing your staff with cybersecurity education and awareness training
- Turning on local firewalls and disabling Windows PowerShell



Surge in healthcare insider data breaches in 2020

Following a four-year decline, insider data breaches in healthcare surged in 2020. More than 8.5 million records were exposed or compromised in those incidents – more than double the number of breached records by insiders as 2019. In fact, more records were breached by insiders in 2020 than in 2017, 2018, and 2019 combined. In 2020, 1 in 5 data breaches was an insider incident.

Insider breaches include insider errors and insider wrongdoing. 96 breaches involved insider error in 2020, of which data was obtained for 74 of the incidents. There were 45 cases of insider wrongdoing, with data obtained for 30 of the incidents. Errors by employees resulted in the exposure of the protected health information of at least 7,673,363 individuals, and insider wrongdoing incidents resulted in the exposure/ theft of at least 241,128 records.

Trend #5: The role of human actors

As if the external threats to healthcare providers weren't challenging enough to deal with, the sector also struggles the most when it comes to insider threats. Verizon, for example, in its 2018 Data Breach Investigations Report, found that healthcare is the only industry to have more internal actors behind breaches (56%) than external.

In healthcare, security efforts often focus on the network perimeter and implementing measures to block external threats, but insider threats can be just as damaging if not more so. Insiders can steal sensitive information for financial gain, take information to provide to their next employer, or abuse their privileged access to cause significant harm.

Insider breaches can also have major consequences for organizations, including reputational damage, loss of revenue, the theft of intellectual property, reduced market share and even physical harm.

Reflecting the scale of threat posed by insiders including current and former employers, contractors, or other individuals with inside knowledge about an organization, in October 2021 the US Government's Cybersecurity and Infrastructure Security Agency introduced a new Insider Threat Risk Mitigation Self-Assessment Tool to help public and private sector organizations further their understanding of insider threats and develop prevention and mitigation programs.

While large organizations are likely to have conducted risk assessments and put measures in place to mitigate insider threats, small- and medium-sized businesses tend to have limited resources and may not have assessed their risk level. The tool therefore consists of a series of questions to establish the level of vulnerability to insider threats, and provide feedback to help users develop appropriate mitigations to guard against insider threats and reduce risk to a low and acceptable level.

How to manage insider threats securely

Effective cybersecurity mandates removing practices that are inherently risky, such as:

- Continued use of software that has reached its end-of-life and is no longer supported by the software developer — as without support, patches are no longer issued to correct vulnerabilities, which can be easily exploited by cyber actors to gain access to internal networks.
- Failure to change default credentials and passwords that are known to have been compromised in data breaches or have otherwise been disclosed.
- Using single factor authentication for remote or administrative access to systems – which, while this provides a degree of security, it is not sufficient to resist the brute force tactics of hackers.

To reduce the risks posed by insider threats, putting policies in place to immediately prevent access to corporate systems by former employees should unquestionably be added to this list.

The topic of cybersecurity awareness training has also been mentioned throughout this white paper. So, given that in any environment – including the most highly regulated — people can still make honest mistakes, training that helps to reduce these errors is another vital investment.

Summary

An often quoted sentiment in healthcare goes along the lines that 'If we need prioritize spending on patient care or cybersecurity, the safety of our patients will always come first'. Laudable though this is, the broad and continually expanding nature of the healthcare threat landscape means that effective cybersecurity needs to be seen as an investment in patient care, not a drain on resources that could be better used elsewhere.

Kaspersky is a pioneer in helping healthcare providers protect data and business continuity 24/7 against cyberthreats ranging from commodity, advanced and evasive threats to targeted attacks – mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection. Our **stage-by-stage cybersecurity approach** is designed to clarify which level of security as well as which specific solutions best suit your organization. The stages provide a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring a smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security - for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing ...

3

Kaspersky Expert Security – for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** Kaspersky Security Foundations **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▪ **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security ▪ **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security ▪ **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▪ **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage ▪ **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** **Kaspersky Optimum Security** **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▪ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum ▪ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum ▪ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum **and** Kaspersky Managed Detection and Response Optimum ▪ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with Kaspersky Cybersecurity Training.

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the Kaspersky Incident Response team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with Kaspersky Managed Detection and Response, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through Kaspersky Security Assessment.

Targeted Solutions

What	How
 **Kaspersky DDoS Protection**	Covers a bandwidth of up to 2Gbps, with extensive service coverage, including attack analysis reports and anti-DDoS capability assessments. Optional automatic always-on DDoS mitigation, fortified by Kaspersky engineers running parallel checks to optimize defense according the nature of each DDoS attack.
 **Kaspersky Embedded Systems Security**	A multi-layered solution delivering unequalled protection to Windows-based embedded devices – even those with limited system resources and running discontinued OSs. Opt-in security layers including application and device controls, exploit prevention and anti-malware mean protection can be optimized for lower-powered devices - including vulnerable older PCs running unsupported OSs such as Windows XP.
 **Kaspersky Fraud Prevention**	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any business, ensuring safety and protection for clients.

Cyberthreats News: www.securelist.com
IT Security News: www.kaspersky.com/blog
Threat Intelligence Portal: opentip.kaspersky.com
Technologies at a glance: www.kaspersky.com/TechnoWiki
Awards and recognitions: media.kaspersky.com/en/awards
Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE