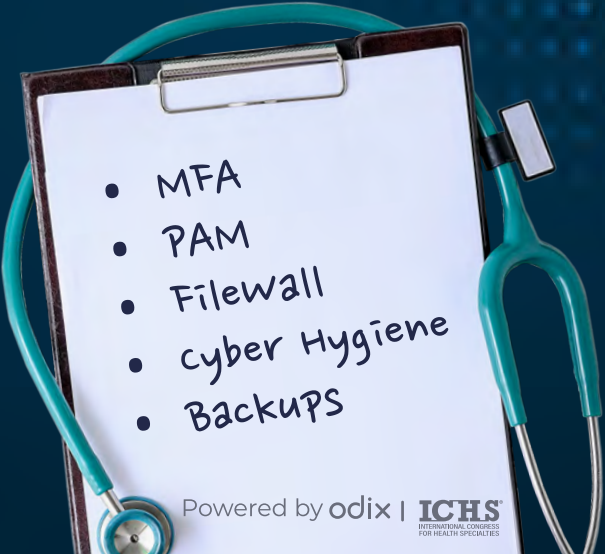


How to prevent the next CyDemic?

Written by **Alon Golan**

- 
- MFA
 - PAM
 - Firewall
 - cyber Hygiene
 - Backups

Powered by odix | **ICHS**

INTERNATIONAL CONGRESS
FOR HEALTH SPECIALTIES



H.E. Amb. Dr. Abdulsalam Al Madani



Chairman, International Congress for Health Specialties – ICHS

For decades, digital transformation in the healthcare industry has brought enormous benefits, including faster and enhanced efficiency in medical treatments, improved patient outcomes, and reduced costs. However, it has also increased the attention of threat actors who take advantage of vulnerable healthcare organizations, putting many lives at risk.

ICHS, in collaboration with odix, has issued an eBook that sheds light on the pressing issues of cybersecurity in the healthcare sector. It includes a deeper understanding of the unique challenges, risks, and opportunities of cybersecurity in the healthcare sector, and the long-term effect of neglect by stakeholders and government officials.

“How to Prevent the Next CyDemic” will serve as a guide for healthcare and IT professionals alike as they navigate the complex and evolving world of cybersecurity in healthcare, and teach how to protect sensitive data through practical cyber-education, best practices, and deep insights to avoid becoming a victim of the next Cyber-Pandemic.



Dr. Oren Eytan



CO-Founder & CEO, odix

Titled by the notorious record of “the world’s first ransomware victim”, the healthcare industry is one of the most targeted sectors decade after decade. With multiple high-profile cyber incidents on monthly basis, these attacks not just cause major financial losses, but also have a genuine impact on human lives. In its relentless effort to increase cyber-education across both technical and non-technical staff, odix is proud to join forces with ICHS and launch an eBook dedicated solely to the healthcare domain including the challenges, risks, and possible remediation for Cybersecurity threats. Join us for a deep dive as we’ll explore the past, analyze recent use cases and see what can be done today to protect the next billions of patients in need.

Table of Content

| | |
|--|-----------|
| Chairman, ICHS: Amb. Dr. Abdulsalam Al Madani & CO-Founder & CEO: Dr. Oren Eytan | 2 |
| Meet the Author | 4 |
| Why is healthcare sector so vulnerable to cyber attacks? | 5 |
| When cyber-attacks become a pandemic | 6 |
| Irreversibility – When Ctrl + Z doesn't work | 7 |
| RansoMurder | 8 |
| When medical devices becomes hacker's toys | 10 |
| A Slice of Life | 12 |
| Risks and Potential Outcomes | 12 |
| The Enemy Within | 13 |
| Cyber Taming | 14 |
| A History of Digital Neglection | 15 |
| New World Record | 17 |
| Bullying the Smallest Kid | 17 |
| We Have a Disease and We Don't Care | 18 |
| Taking the Cyber Secret to the Grave | 19 |
| Awareness, Technologies, & a Combination of the Two | 21 |
| Awareness, Technologies, and a Combination of the Two | 22 |
| Zero Excuses – One (or more) Business Continuity Plan | 23 |
| Had a Diagnostic Test Lately? | 24 |
| The Man in the CT | 25 |
| Code Red | 26 |
| Crypto is Thicker Than Blood | 27 |
| Until an Exploit Do us Part | 28 |



Meet the Author

Alon Golan

Alon's love story began amidst the hustle and bustle of Mexico City's busy streets. He was weighed down by a hefty 12-kilo laundry bag and sought assistance from an English speaker when he unexpectedly encountered his future wife. It was a chance encounter that would change the course of his life forever.

Alon Golan is a seasoned product marketing professional with over 10 years of experience in cybersecurity.

He's an avid technical storyteller with a keen eye for details. With his combined technical and creative background, he excels at translating complex technical concepts into well-articulated and compelling messaging that resonates with diverse audiences.

In his current role as Product Marketing Manager at odix,

Alon is focused on executing the company's go-to-market plan, the launch of new products and features, content creation, sales enablement collaterals, and positioning & messaging development that quantifies the value proposition.

Alon holds a Master's degree with dean's honors in Film and Media Production from the New York Film Academy. His perspective on life, work, and relationships is **"make every day count"**.



Why is the healthcare sector so vulnerable to cyber attacks?

There is an unspeakable plague the healthcare system struggling against – malicious cyber campaigns targeting every healthcare facility of any size. In the past 12 years, the healthcare sector suffers from exponential growth in the number of cyber-attacks threatening their systems.

The attacker's prime incentive consists of disruption, turmoil, and data. A successful breach can potentially have chaotic outcomes; From sensitive data exfiltration (i.e., social security numbers, financial data, medical records, etc.), to tampering with medical records' integrity, all the way to taking over critical systems, and shutting down hospitals across vast regions. If medical systems or equipment vital to patient care are compromised, or blocked, they might jeopardize the patient's well-being.

Infuriatingly, decision-makers in the healthcare system avoid addressing the severity of the threat or allocating additional resources the system so desperately craves for. Such neglecting already resulted in tragic results that affected patients around the world. And with more state-sponsored actors and cybercriminals developing sophisticated aggressive tools, the menace of a nationwide-scale cyber pandemic is very tangible.

In this four-part series, we shall explore the decades-long relationship between hackers and the healthcare sector, the deliberate neglecting by governments, and how it put everyone's lives at risk when attending the hospital for checkups or medical procedures.

When cyber-attacks become a pandemic

Healthcare organizations are the target of choice by many hacker and cybercriminal groups.

For more than a decade cybersecurity experts and government officials remonstrate the healthcare ecosystem against the increasing wave of direct cyber campaigns. Sadly, year after year the number of infected facilities keeps increasing. Those campaigns are more frequent and possess a more forceful attempt for data exfiltration and equipment tampering. The system faces two fronts: conventional financial & reputation risks as well as life-threatening threats.

The potential for endangerment is overwhelming. Reports show that in the United States alone more than four million people were affected by cyber incidents in the first quarter of 2022 only. According to a [Checkpoint report](#), The Healthcare sector was the most targeted industry for ransomware during the third quarter of 2022 suffering from an average of 1,426 weekly attacks – illustrating a staggering 60% year-over-year growth.



Irreversibility – When Ctrl + Z doesn't work

Time is a critical resource for hospitals. A facility that's unable to access medical records in a reasonable time or reliably authenticate its equipment endangers patients' life.

As available data is indispensable for hospital ongoing activity, The healthcare sector stores at any time a massive amount of sensitive information.

Falling into the wrong hands, such information can be leaked or sold over the dark web to the highest bidder. Things get more complex if medical records, which are vital for a therapeutic sequence, are blocked from access, causing the level of treatment will decrease and the treatment period shall prolong. The snowball effect of the accumulated queue will force the facility to stop providing further medical care.

“



**All it takes is one
unaware staff member
that opens an email containing
malicious code**

”

There is no need to wait for the next WannaCry variant to hit the streets (and it will), as even mediocre hackers with known exploiting tools can cause a nationwide crisis. All it takes is one unaware staff member that opens an email containing malicious code hidden inside an innocent-looking file.

To make a long story short, attacks would cause hospitals inability to function, while all ambulances and patients would have to be diverted to other facilities in the region that will experience an influx of patients, stretching their capacity, and putting more lives in jeopardy.

The 2017 WannaCry ransomware took down many hospitals that were unable to provide treatment for days. In November 2022, a ransomware attack in Sothern California affected the operations of five hospitals in the San Diego area for about a month. Even cases when a breach resulted in death.

RansoMurder

In 2020 a German woman was reported dead after being forced to reroute to a remote hospital and died from treatment delays, simply because her nearest hospital was shut down due to a ransomware attack.

In September 2021 a hospital in Alabama, USA was served with a lawsuit holding them accountable for a baby's death as a result of a ransomware attack.

The lawsuit claims that a ransomware attack that shut down hospital computers led staff to miss troubling signs, followed by severely diminished care to a mother who arrived to deliver her daughter. The doctors and nurses skipped conducting several key tests that would have indicated that the umbilical cord was wrapped around the baby's neck. As a result, the mother delivered a baby with a severe brain injury that died nine months later. Furthermore, the hospital failed to inform the mother about the attack in real time, which could allow her to deliver the baby at a different facility.

This lawsuit raised fundamental issues concerning healthcare executives' responsibilities. Their professional commitment is not only to recruit the best doctors and nurses but also includes areas like building and maintaining secured IT infrastructure.

When medical devices becomes hacker's toys

Imagine the next scenario, a western European leader develops cancer cells that needs immediate attention. He complains about lung pains and was rushed to the hospital. In the MRI checkups, the physicians don't see any abnormal indication in his body and send him home with painkillers. A few months later due to the spread of the cancer cells the leader dies. The physicians misdiagnosed cancer because it didn't appear in the scan results. At the time of the scan, a hacker removed in real-time any sign of atypical lumps.

Using the Same setup from a different angle, a perfectly healthy American, running for a state governor role is diagnosed during a routine CT scan with metastasis that requires an Immediate surgical intervention. The candidate will perform an

unnecessary invasive operation followed by a long recovery period, remarkably close to the election date.

Sounds like Science fiction? It has already been proven possible.

A Slice of Life

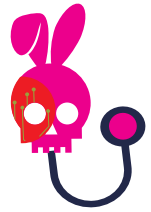
In a nutshell, Cybersecurity experts from the Ben-Gurion University – National Cyber Security Research Center, Israel, demonstrated how threat actors can exploit vulnerabilities found in X-Ray, CT, and MRI scanners to breach, and manipulate scan results which could lead to lethal misdiagnosis.

The researchers got permission from an operational hospital to engage their hacking method and intercept the taken scans.

In many facilities, the scans are not encrypted because the internal network is disconnected from the internet. However, hackers can still gain access via the hospital's Wi-Fi or physical access to the infrastructure.

Using off-the-shelf Raspberry Pi 3 series with a Wi-Fi access point acting as a MITM (Man-in-the-Middle) device, the researchers who placed it adjacent to an exposed scanner managed to access the equipment. After intercepting the data, the researchers used a deep learning neural network application named GAN (generative adversarial network) to erase and inject realistic high-resolution 3-D medical imagery (downloaded from the internet) into the original body scan. By doing so, they managed to manipulate the results in real-time, and alter the number, size, and locations of the cancer cells while preserving the same anatomy from the original.

“



Connected medical devices pose a **potential risk of being vulnerable to cyber breaches**

”

”

Risks and Potential Outcomes

Perhaps the most spine-chilling aspect of the researcher's findings was that when they hand over the falsified results, even the most experienced radiologists misdiagnose the patient's condition as they genuinely believed in the processed scan copies. The hustle worked in both scenarios when real tumors were removed, and non-existing cancer cells were injected into the scan. After the medical experts were notified of the malicious modification and received a new set of scans, they still misdiagnosed about 60% of the fabricated ones.

The research was conducted at the Ben-Gurion University, Israel in 2019 by Researchers Prof. Yuval Elovici, Prof. Ilan Shelef, Dr. Yisroel Mirsky, and Tom Mahler. To read the complete publication as appear on google scholar, click [here](#).

The Enemy Within

As medical devices are increasingly connected to the Internet, they pose a potential risk of being vulnerable to cyber breaches. In the United States alone, millions of people have electronic medical devices implanted in their bodies. Those devices use software and have a wireless function enabled.

While for the moment the risk for cyber-attacks on these personal medical devices is relatively low, according to many experts it is only a matter of time before state-sponsored threat actors would develop a way of hacking into pacemakers and insulin pumps.

A testimony that those threats are being taken care of very seriously can be found in breadcrumbs the American government leaving behind concerning imminent cyber threats:

In an interview given in 2013 to the newsmagazine “60 Minutes”, former American vice president Dick Cheney, confessed that he instructed his physicians to disable his pacemaker’ wireless function. According to Cheney, both he and “national security” officials were concerned about threat-actors to breach the device and sending orders to shock his heart into a cardiac arrest

In 2017, the US Food and Drug Administration informed the public about a voluntary recall for half a million pacemakers. The FDA was troubled that by exploiting cyber vulnerabilities on RF-supported implantable cardiac pacemakers and commercially available equipment, hackers could gain unauthorized user access to patients’ devices, and alter the code commands to cause a rapid battery depletion or administration of inappropriate pacing. According to FDA’s official statement, the reason for the recall was “to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities”.



Cyber Taming

On March 15th, 2022, U.S. Congressman Michael C. Burgess introduced new bill legislation requiring device manufacturers applying for FDA approval for their medical devices to demonstrate “a reasonable assurance of safety” concerning cybersecurity. The act was cited as the “Protecting and Transforming Cyber Health Care Act of 2022” or in short, the “PATCH Act of 2022”. While if approved in its current form, The Patch Act would become a most welcome initiative, however, it addresses only newer devices seeking FDA clearance. The older legacy medical devices, which still be used by the majority, would be vulnerable to malicious cyber intents.

On November 15, 2022, the FDA updated the Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook, a resource to help healthcare organizations prepare for cybersecurity incidents.

The bottom line, until governmental legislation comes into force, FDA recommends people with implants be responsible for themselves, track the manufacturer’s routine statement, follow remote device monitoring protocols, and stick to schedule in-office visits for software updates including patches designed to enhance device security.

A History of Digital Neglection

The questionable honor of being the first reportedly ransomware victim belongs to the healthcare sector, where in 1989 the Harvard graduate biologist, Dr. Joseph L. Popp distributed at the World Health Organization AIDS conference in Stockholm, Sweden around 20,000 floppy disks with the title “AIDS Information Introductory Diskette” or “AIDS” in short. The disk’s payload encrypts the main hard drive and asks the victims for \$189 ransom money to regain access to their Drive C: directories.

A History of Digital Neglection

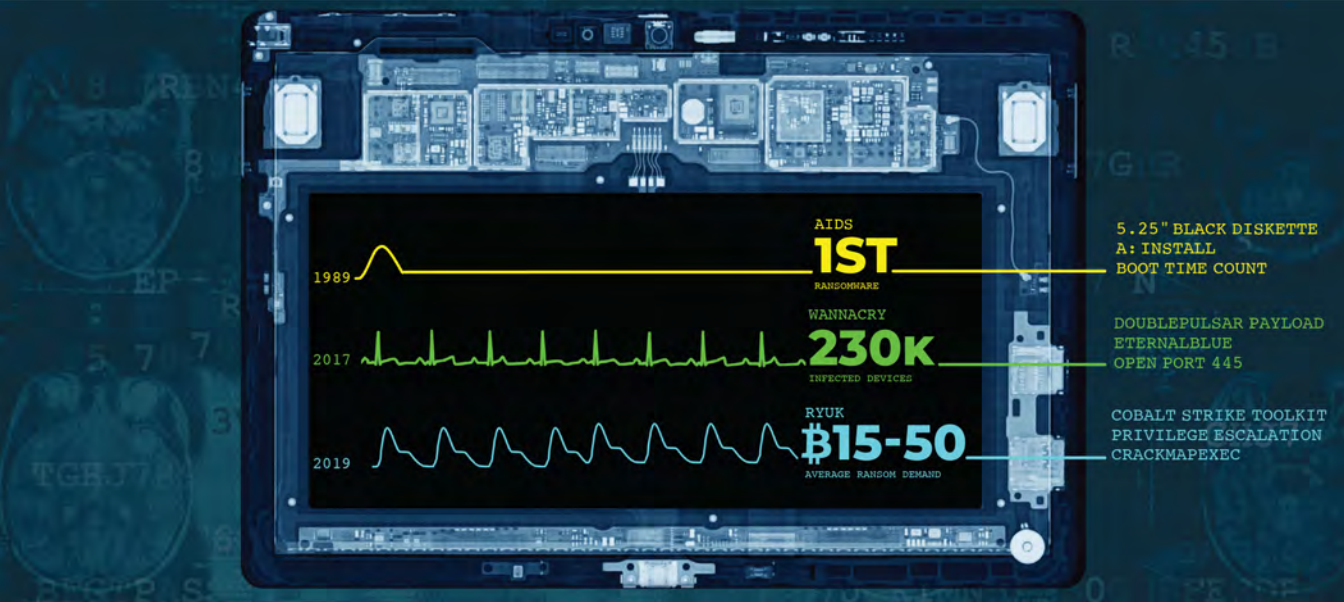
On May 12th, 2017, “WannaCry” ransomware, the mother of all cyber pandemics stormed into our life, leaving behind it scorched earth of more than 200,000 infected devices across 150 countries, including 70,000 British National Health Service (NHS)

computers, all in a record time of 24 hours. Medical records, test reports, and critical systems were denied access. Doctor treatments, appointments, and surgeries were all canceled, ambulances were diverted between hospitals and a sense of anarchy was felt all around.

In 2019, 400 dental practice offices, were affected after a known dental managed service provider was compromised by the “Ryuk” variant, exploiting their connection to the remote offices and encrypting them as well.

During the 2020-2021 COVID-19 lockdowns, attacks merely skyrocket and ransomware came more contagious. As all attention went toward healthcare facilities, many hackers took advantage of the situation making to be the first ones to hit a facility and collect the ransom payment.

In 2021 the cybercriminal groups, FIN11 and Clop were reported to hit the Accellion legacy File Transfer Appliance product, causing one of the largest healthcare data breaches of that year. Other ransomware campaigns were reported by the Irish Health Service Executive (HSE) and 850 other healthcare facilities and hospitals in the U.S. alone



New World Record

The past year is yet to be over but it already breaking records in reported cyber campaigns against healthcare facilities. The most noticeable one happened recently in October, when the second largest non-profit hospital chain in the United States, reported a cyber-attack that forced the system to reschedule crucial appointments and even take certain IT systems offline till they manage to overcome the attack. The hospital system entails more than 140 facilities across 21 states.

As many industries suffer from cyber campaigns targeting mainly Small and Medium Businesses, small hospitals are no exception.

Bullying the Smallest Kid

Smaller hospitals are more vulnerable and more likely to get cybercriminals' attention. Penetrating those facilities is relatively easier and takes less time due to a lack of resources, manpower, and cyber-awareness.

Whether hackers find a new vulnerability, develop an exploit, or even acquire a toolkit, they would rather try it on in a "safe space" before tackling cyber-resilient and robust healthcare facilities. It improves their breaching success rate and is less likely to trigger an alarm if something in their scheme needs some fine-tuning.

We Have a Disease and We Don't Care

Careless healthcare facilities put their patients' and staff's data at risk because of deliberate neglect. In many cases, the cyber breach could be easily avoided by implementing basic measures. Many attackers aren't necessarily demonstrating highly sophisticated schemes, but simply exploit known vulnerabilities to unpatched, out-of-date systems. In some cases, they simply gain access through open and unsecured connections with a contractor or third-party medical provider. And with many facilities that are unaware of the attack until weeks or months later, it's no wonder some of them suffer from multiple incidents in a single year. As an establishment that by nature is publicly available for all, it offers noticeably more entry points for attackers to find vulnerabilities. More medical systems are now interconnecting by third-party solutions connected externally to the internet, contractors, and other supply chain service providers. Furthermore, even when hospitals make the effort in deploying tools for monitoring, detection, and prevention, they often lack a sufficiently skilled labor force to proactively track and operate those systems. Put all of those ingredients together and you will get an accelerated countdown for the next system breach.

to manage a cyber-incident similarly to their associates in other sectors.

Taking the Cyber Secret to the Grave

The simple truth is that when a cyber-incident happens (and is discovered by the IT), many hospitals steer clear of discussing the matter, or delay their statement for longer after the attack occurs. The U.S. Department of Health and Human Services mandates healthcare facilities report them as soon as a cyber event that affects more than 500 people happen on their premises. In the first quarter of 2022 alone, the U.S. Department of Health was investigating 125 high-profile breaches. Sadly, in some cases, medical centers discover the breach months after it was initiated, and took their time reporting to the health department (up to 3 months later), which poses a nonexistent chance to remediate the attack or to alert peer facilities. Circling back to the [Alabama-based hospital lawsuit](#), as taught by local News 5 provided contradictory statements. While at first, they describe the event as a “standard downtime procedure to mitigate the impact on our patients”. They also reassured that the hospital “seeing a regular volume of patients at the time”. A few days later they revised their statement to “currently addressing a security incident affecting our internal network. After learning of this issue, we immediately shut down our network to contain the incident and protect all data, notified law enforcement, and engaged leading outside forensic experts to support our investigation.”

“



**2022 is yet
to be over but it already
breaking records in reported
cyber campaigns against
healthcare facilities**

”

”

In both cases, the updates were the leaser inaccurate.

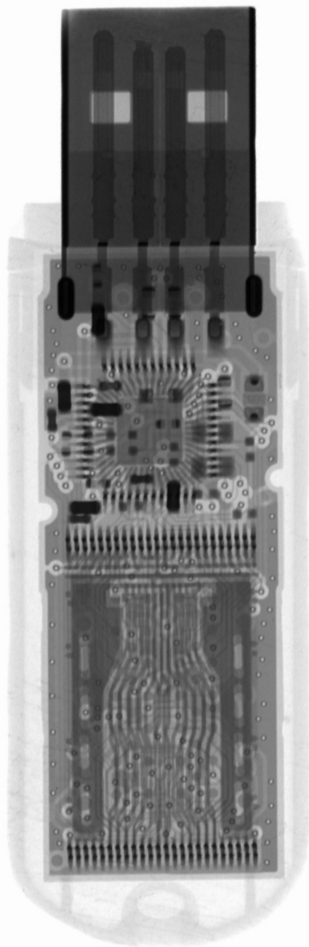
A short inquiry by the local WKRG station found that the hospital was indeed turning away some patients because of the ransomware attack. A patient of the facility told the station his doctor’s appointment scheduled for that week was unexpectedly postponed with no further explanation: “The only information they could tell me is they possibly could call me back later in the week if the computers are back up but currently they are having issues with it”. Also, When contacted by the said police department and County Sheriff’s Office, both agencies claimed they “did not take any incident reports on this”.

A short inquiry by the local WKRG station found that the hospital statements were for the least inaccurate. Demonstrating that the hospital doesn’t have (or want) the capacity to manage a cyber-incident similarly to their associates in other sectors.

Awareness, Technologies, & a **Combination** of the Two

Cyber hygiene is as important as medical hygiene. Neglecting it possesses potentially dangerous outcomes for the mass patients in a way that is hard to predict.

After decades that the healthcare system suffering from cyber-pandemic's unpredictable outcomes, there is light at the end of the tunnel; Healthcare officials expect that in the coming years, governmental modern legislation, that takes into consideration the healthcare system as a strategic asset, shall dictate strict cybersecurity strategy plans and better auditing mechanisms to standardize the cybersecurity landscape across the industry.



Meanwhile, as imminent cyber breaches are inevitable, healthcare facilities must act solo. To contain threat actors, prevent ransomware from spreading throughout their systems, and prepare for the worst, an action plan is required:

Awareness, Technologies, and a Combination of the Two

Cyber education programs should be deployed in addition to cyber prevention tools.

Cybersecurity policies and guidelines need to be spelled out and become accessible to all employees and patients alike. IT teams should regularly stress the potential threat vectors to the facility's workers. Staff at all levels with access to the hospital's network should acknowledge the importance of looking into suspicious eyes on emails and avoid clicking on suspicious links and attachments.

As cyber awareness and training are an integral part of the staff's work plan, it must have a dedicated budget clause as well as scheduled and surprise external penetration testing drills. Such drills should test the readiness of the entire staff, tech, and non-tech-savvy.

Zero Excuses – One (or more) Business Continuity Plan

Much of the challenge isn't on technology but rather on good business continuity planning. When budgeting constraints avert hospitals from replacing out-of-date or unsupported systems, A future budgeting plan is expected for the least. Such a plan should include a list of existing out-of-date technologies and a scheduled plan for renewal and replacement of such.

Tighter communication should exist inside a healthcare facility as well as with other healthcare systems.

Hospitals should be encouraged to report staff, patients, and the public domain as soon as they experience a cyber event. Transparency, integrity, and open communication are key to concluding and healing the system. Such interaction should consist of knowledge sharing and best practices for prevention and mitigation. Moreover, a facility that experienced a cyber incident should disclose in a transparent way of their findings, path of exposure, and outcomes. Such information has the potential of saving other facilities and better prepare them from experiencing the same faith.

Had a Diagnostic Test Lately?

Like new medicine, treatments, or equipment, APIs should be thoroughly tested before they are integrated with the healthcare's production network. Taking the time to thoughtfully stress-testing APIs for vulnerabilities before going live can save a lot of time, effort, and funds in the future.

We would recommend that the diagnostic tests would include an overall check if you have imposed a stronger password structure and enforce MFA (multi-factor authentication) across all systems within the organization. Invest in PAM (privileged access management tools) to mitigate the risk and elevate the level of privileged access. This will limit the ability of threat actors of gaining access to credentials and other sensitive information. To complete the circle, set tougher policies for devices external to the organization's network.

The Man in the CT

Medical equipment manufacturers should reduce vulnerabilities by analyzing and fixing any security loopholes, hosting internal pen-test to scale up their security against future threats, and applying digital signatures (or watermarks, also called "DW") on scan test results. By doing so, hospitals gain a security force multiplier; hackers struggle to get in between the equipment and the end device. The end devices can sign each scan with a secure and hidden signal to ensure the authenticity and integrity of the scanned imaging.

In addition to medical equipment, security technologies must be applied in all other IT administrative systems such as email. Extra attention must be provided to files that can include embedded malware. Introducing CDR or Deep-File Analysis technology for files arriving via multiple channels such as Microsoft 365 Exchange Online, Teams, OneDrive, SharePoint, or other sources is an effective best practice to ensure all files are malware-free.

“



**Like an earthquake,
a hospital should
implement protocols
for **cyber breaches****

”

”

Code Red

When worst comes to worst, healthcare facilities must have a well-trained, and receptive response trauma team for cyber incidents. Like an earthquake, a hospital should implement protocols for cyber breaches. It should include downtime procedures to proactively take systems offline, and address key items:

- Lists of critical assets.
- Downtime limitation plan. backups for sensitive patient data and core systems.
- up-to-date contact information with all relevant vendors and service providers who would be affected by the breach.
- How to get in touch with staff and as many as tens of thousands of patients in the event of a cyber-incident. Such a plan should go all the way to thinking of a scenario when the phone systems are unavailable.

Such a “playbook” should be available both digitally and in hard copy and include all relevant contact people in the facility and external with their responsibilities.



Crypto is Thicker Than Blood

Typically, hackers demand a ransom payment in the form of cryptocurrency. This is a risk-free, anonymous method to receive untraceable funds without anyhow having a way of tracking and identifying the destination account. Keeping threat-actors safe from the authorities.

Testimonials for underprioritizing cybersecurity budget can be found in countless annual reports demonstrating how year after year the industry investment is insufficient compared to the rising level of threats.

Cybersecurity attacks carry enormous financial expenses to hospitals, which they surely don't have. In most cases, Hospitals' post-cyber-breach unforeseen expenses include incident response & forensics teams, disaster recovery plans, and yes, in some cases also the ransom payment. It is ten times pricier than allocating budgetary foundations for prevention and detection tools, tech-savvy personnel, and cyber awareness programs.

The cost of cyber-breach in the healthcare industry keeps breaking records. For the 12th year in a row, the healthcare sector had the highest average data breach cost of any industry, which embodies a 42% increase in cost since 2020. According to an [IBM report](#), in 2022 the average total cost of a breach in the healthcare industry rose to \$10.1 million. With the rest of the business sectors "settled" with an average of \$4.35 million of cyber breaches, it is no wonder the healthcare sector, as the most expensive industry, is the golden goose of hackers and cybercriminals from around the years to come.

D=50,0 **M F A** V=0,1

D=25,0 **P A M** V=0,2

D=16,67 **H I P A A** V=0,3

D=12,5 **FILEWALL** V=0,4

D=10,0 **CYBER HYGIENE** V=0,5

D=8,33 **D I G I T A L** V=0,6

D=7,14 **W A T E R M A R K S** V=0,7

D=6,25 **B A C K U P S** V=0,8

D=5,55 **T R U C D R** V=0,9

D=5,0 **C Y D E M I C** V=1,0

D=3,33 **C Y B E R H Y G I E N E** V=1,5

D=2,5 **D I G I T A L W A T E R M A R K S** V=2,0

Until an Exploit Do us Part

With the welcoming of 2023, it seems like states are finally taking responsibility for their healthcare systems. But the transition won't happen overnight.

Governmental and municipal agencies should bolster their interface with healthcare facilities; Establish dedicated “red lines” for concurrent cyber-attacks, improve hospital preparation by conducting mutual war exercises, and allocate funds to provide a basic level of cyber readiness for smaller facilities that lack resources.

Hospital higher management should embrace the fact that investing budgets in skilled IT staff, cyber awareness programs, and state-of-the-art anti-malware tools are much cheaper than overcoming a successful cyber incident.

The threats of the next CyDemic must be voiced by patients, the IT communities, and officials at all times. Can we still prevent the next cyber-pandemic? Like with global warming, we might slow it down or reduce its destruction radius, but unless we all step up, it will be here sooner than later.

About ICHS

ICHS[®]
INTERNATIONAL CONGRESS
FOR HEALTH SPECIALTIES

The International Congress for Health Specialties – ICHS, is headquartered in the United Kingdom, and is recognized as an international platform to inspire medical and healthcare professionals from over 438 different specialties and subspecialties to provide solutions to today's most pressing challenges in the medical and healthcare fields through advancing continuing medical education, continuing professional development, research, innovation, and excellence in healthcare for all communities around the world.

ICHS is the collective global effort of experts and professionals who aspire to contribute and commit to community service for the sole purpose of helping humankind across all regions of the globe without any bias toward race, religion, ethnicity, or location.

To learn more about ICHS, visit ichs.uk



About odix

odix |

odix develops and markets advanced anti-malware tools based on its patented Content Disarm and Reconstruction (TrueCDR™) technology for preventative cybersecurity in enterprises of all sizes. odix technology prevents malware infiltration into organizational networks by removing all malicious code from a wide range of file types. Uniquely, odix protects files from unknown attacks, where legacy solutions fall short.

odix solutions are trusted by enterprises in diverse sectors such as industrial, finance, insurance, government, and others. odix operates from its headquarters in Israel and regional offices in the U.S. and Europe.

To learn more about odix, visit odi-x.com

