The Healthcare sector is under a constant Ransomware siege. Why is it happening and what can be done to avoid being targeted and subsequently attacked? June 2021

The Healthcare sector has been a victim to numerous cyberattacks, these attacks are increasing in both scale and frequency. This document focuses on eight hospitals and health systems that have, apart from yesterday's hrh.ca cyberattack and this week's Oklahoma's breach, already paid a ransom to hackers and yet remain insecure. Not only were they insecure which led to their being targeted and attacked in the first place, they have continued to ignore the root cause and are prime targets for a second attack. This is nothing short of gross negligence.

Paying ransom to hackers is not recommended, however, some hospitals and health system operators have made the often-impossible choice to pay a ransom to restore their networks and hopefully regain the all-important PII data, sadly this is not always the case. Like a good farmer, many cybercriminals year after year to harvest their crop. It will not stop until internet security is addressed.

Earlier this week the Cancer Centre of Southwest Oklahoma reported their breach on June 4 which affected 8,000 individuals. In an online notice to patients, Cancer Centre of Southwest Oklahoma said its vendor Elekta, which provides cloud-based storage for the practice's EHR, discovered unusual activity on its network earlier this year.

ccswok.com shows an F and 0 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

The Humber River Hospital based in Toronto, located near Wilson Street and Keele Street is a leading hospital in Canada and alerted the authorities of a major cyberattack yesterday the 15 June 2021. HRH have a very impressive Technical Command Centre that has the moto: 'Breakthrough Intelligence'. Sadly, nobody managed or ensured they had website connected internet security, so not so intelligent.

hrh.ca shows an F and 0 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

Scan Summary

F

Host:	www.hrh.ca
Scan ID #:	19678668 (unlisted)
Start Time:	June 16, 2021 7:11 AM
Duration:	6 seconds
Score:	0/100

University Hospital evolved from a long-standing history of providing primary health care services for generations of families in the city of Newark, New Jersey. In fall of 2020 UHNJ suffered a cyberattack and paid $675k ransom. The hospital maintained insecure websites with invalid digital certificates and despite no less than six emails to their CEO, UHNJ remain Not Secure to this day.

Uhnj.org shows an F and 0 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

Scan Summary

Host:	uhnj.org
Scan ID #:	19680574 (unlisted)
Start Time:	June 16, 2021 10:55 AM
Duration:	4 seconds
Score:	0/100

Attleboro, Massachusetts-based Sturdy Memorial Hospital began notifying patients that some of their protected health information had been stolen by hackers. In exchange for an undisclosed amount, hackers gave assurance that the acquired PHI would be destroyed, the hospital said in a May 28 online statement.

Sturdymemorial.org shows an F and 15 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

University of California San Francisco Health confirmed that it paid $1.14 million to hackers after a June 1 ransomware attack on its medical school's computer servers.

cgl.ucsf.edu shows an F and 20 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

Scan Summary

F

Host:	www.cgl.ucsf.edu
Scan ID #:	19664682 (unlisted)
Start Time:	June 15, 2021 9:20 AM
Duration:	2 seconds
Score:	20/100

Hackensack (N.J.) Meridian Health said it paid an undisclosed amount in ransom to stop a cyberattack that had caused a two-day shutdown of its computer network, according to a December 3, 2019, report.

Hackensackmeridianhealth.org shows an F and 0 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

Scan Summary

F

Host:	www.hackensackmeridianhealth.org
Scan ID #:	19664549 (unlisted)
Start Time:	June 15, 2021 9:06 AM
Duration:	7 seconds
Score:	0/100

Tuscaloosa, Alabama-based DCH Health System said it had paid hackers an undisclosed ransom to restore access to locked systems at its three hospitals in October 2019.

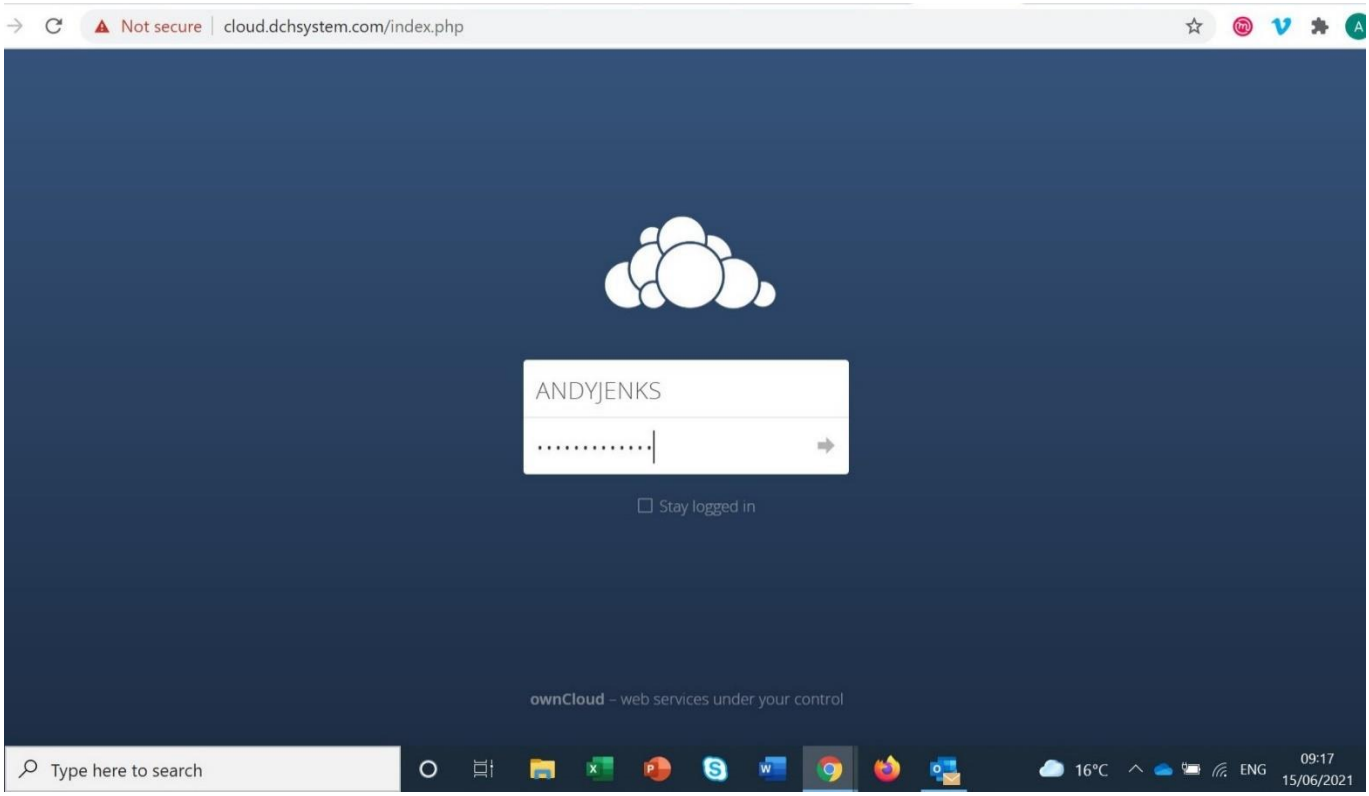
Cloud.dchsystem.com shows an F and 0 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.

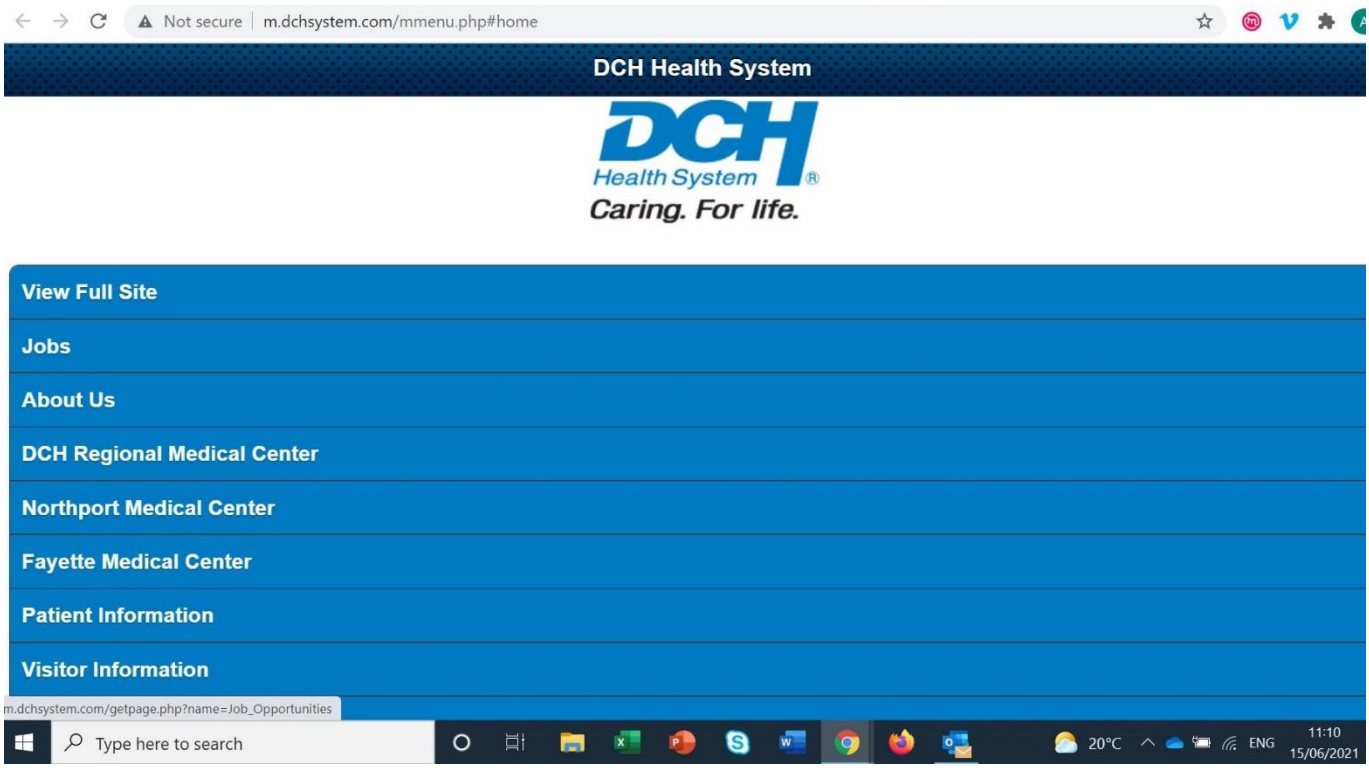
Scan Summary

Host:	cloud.dchsystem.com
Scan ID #:	19664651 (unlisted)
Start Time:	June 15, 2021 9:18 AM
Duration:	3 seconds
Score:	0/100

Greenfield, Indiana-based Hancock Health forked over $55,000 in ransom after files on part of its network were locked, a hospital spokesperson confirmed to Becker's Hospital Review in January 2018.

Hancockregionalhospital.org shows an F and 0 security Rating which is made up of a plethora of insecure exposed, vulnerable, and easily exploited website and Internet connectivity issues.





All the above Healthcare organisations cited in this document as well as last week's Cancer Centre of Southwest Oklahoma and yesterday's Humble Hospital breach, clearly demonstrate sub-optimal and Not Secure websites by being F rated, the worst possible Internet security rating. These ratings are available using Open-Source Intelligence (OSINT) technology and can be identified easily by cyber criminals during their reconnaissance. Due to their exposed and exploitable positions, these websites and organisations make for an easy target and victims to launch attacks. Cyber criminals are safe in the knowledge their victim, in this case the Healthcare operators, will be totally unaware until a demand is made.

End-point protection and virus checks can effectively be totally redundant as are many other security measures due to the access being accepted and undetected and now from the inside… Website access can mean unbridled access which can lead ultimately to ***Domain Admin Access*** as was the case in the recent SolarWinds breach and the subsequent breach of over 18,000 organisations - customers of this company.

There is one sure way to make a substantial difference to reduce attacks on the Healthcare sector, and to ensure it is more secure, reduce cyberattacks and ransomware sieges. That is to ensure Internet connected websites/domains are secure and fit for purpose, not simply digital doorways, and access points.

Whitethorn Shield® provides immediate Actionable Intelligence, controls and management for all internet connected domains and subdomains ensuring security is managed and not assumed. With seventeen Ransomware attacks a day in the US alone, can you really afford to make such assumptions?

The average total cost of Ransomware attacks is in excess $2 million, add disruption, potential legal liabilities, and reputational/brand damage and this is something you really want to avoid.

Contact Us

CIP would be delighted to work collaboratively with your organisation to improve your Internet facing Security posture. We offer our Whitethorn Shield® actionable intelligence solution as a fully managed Service, for a more detailed discussion in relation to our findings and recommended remediation together with a comprehensive overview of our Whitethorn® and Whitethorn Shield® Service please contact:

Burke Stephenson – Cyber Security Consultant

burke.stephenson@cybersecip.com

+44 (0) 7584706612

Cybersec Innovation Partners, 24/25 The Shard, 32 London Bridge Street, London, England, SE1 9SG,