VICTIMISATION IN THE HEALTHCARE SERVICES SECTOR DURING THE COVID-19 PANDEMIC RESULTING FROM CYBERCRIMINAL RANSOMWARE CYBERATTACKS

World Society of Victimology
17th International Symposium on Victimology
Victimisation in a digital world:
Responding to and connecting with victims
Donostia San Sebastian, Basque Country, Spain
5-9 June 2022

Anthony Minnaar

Professor of Criminal Justice Studies/Research Associate
Department of Criminology & Criminal Justice
University of Limpopo
Sovenga, South Africa

Finding Solutions for Africa

Cybercrime & the COVID-19 Pandemic

- imposition of so-called societal 'lockdowns'
- implemented work-from-home options for their employees
- privately-owned, unsecured or insufficiently cyber secured devices (e.g. private laptops; smartphones & VPNs)
- contributed significantly to the surge in a variety of cyberattacks
- opportunistic cybercriminals viewed the pandemic as a perfect stratagem to accelerate their cybercrime exploits
- predictably, for their own profit, cybercriminals were quick to take advantage and maximised the exploitable cyber-vulnerability opportunities linked to various COVID-19 themes to entrap internet users
- to launch cyberattacks, particularly so-called Ransomware, on hospitals and healthcare services, and the development of COVID-19 vaccines, on one of the most 'cyber-vulnerable' sectors of society, namely:

  - emergency services; hospitals; clinics, and other medical facilities, such as laboratories and doctors' rooms

Ransomware

- encrypted strains of this malicious software ('malware')
- email phishing message, a software vulnerability, stolen access credentials (passwords), or other exploitable cybersecurity shortcomings on a network – encrypts files and hard drives
- gain illegal access to a computer or network system and then encrypt the data files – essentially 'locking' them down so that no legitimate users can access them
- demand a ransom and will only 'unlock' the files once payment has been received – usually in a cryptocurrency with *Bitcoin* the preferred means of payment
- files can only be recovered with a decryption key

Surge in Ransomware attacks

- Between May 2020 and May 2021, the global surge in ransomware attacks had increased by 102 percent, with significant increases in both frequency and impact
- "…new functionality and tools, increasing the ease, speed, and profitability of victimization"
- critically changed in that an estimated 50 percent of all ransomware attacks in the UK had included a threat to publish the stolen data, termed: "double extortion"
- most alarming to victims, since they shifted from merely: "…holding computing resources hostage [by encrypting] to basic blackmail using stolen data"
- early 2021 there emerged "triple extortion" - threatening to publish the encrypted data of a target's systems online, the attackers would use the encrypted data to blackmail the target organisation's clients or contacts
- to put additional pressure on a company to succumb and pay the ransom by threatening to make the ransom hack public knowledge
- early 2021 was the so-called "fileless attacks"

Ransoms…

- **an "enormous inflation" in the ransom demand amounts had also occurred**
- ***"…ransoms are being paid because the health organizations are under time constraints and pressure – exactly what the hackers are counting on"***
- **By December 2020 …ransomware was "*...quickly becoming a national emergency*"**
- **By February 2021 … "*Cyberattacks on the global healthcare sector* [were] *getting out of control, because criminals view hospitals as being more willing to meet their demands and actually pay ransoms – and the events of 2020 proved this*"**
- **By the very nature of their essential services, a ransomware attack puts extreme pressure on hospital administrators to pay the demanded ransom as soon as possible to ensure the speedy restoration of their services**

Why did the health care sector worldwide become the preferred target of ransomware during the pandemic?

- **during 2020 there were major increases in ransomware cyberattacks and sophisticated hacking attempts that shamelessly targeted hospitals, healthcare organisations and the companies involved in manufacturing and shipping critical COVID-19 vaccines worldwide**
- **beginning of March 2020 to the end of 2021 the healthcare sector remained the most targeted attack vector for ransomware, with ransomware operators taking advantage of the widespread cybersecurity shortcomings evident in the healthcare industry**
- **this targeting was deliberate, since their systems were already overwhelmed and overburdened with handling the ongoing COVID-19 pandemic**
- **healthcare, with its extremely valuable data (not only health records but also detailed social security information on individuals), combined with its continued use of outdated technology, made them a preferred target**

CYBERATTACKS ON THE HEALTHCARE INDUSTRY DURING THE COVID-19 PANDEMIC

- "…*life-saving medical devices* [being] *rendered inoperable*"
- result in patient care delays
- any interruption of services and functioning of both the health care and its support services (e.g., supply chain of research facilities, medical equipment manufacturers and emergency responders,) be avoided at all cost so as: "…to prevent …loss of life"
- as 2020 progressed and national countrywide lockdowns were instituted, so too were ransomware attacks ramped up, with cyberattacks targeting healthcare facilities, medical institutions and pharmaceutical research centres at an unparalleled rate
- varied in size and included: hospitals large and small, private and state-run; medical laboratories; small single medical practitioners' offices and even urban care centres
- No hospitals, healthcare facilities or even medical research laboratories, specifically those trying to develop COVID-19 vaccines, were spared during this surge in ransomware attacks

1st reported ransomware attack during COVID-19 pandemic on a hospital

- **In a mid-March 2020 ransomware attack on the University Hospital Brno, Czech Rep. shut down its patient information systems and ransomers asked for money to eliminate the problem**
- **Hospital administrator refused to pay and for more than two weeks the hospital was forced to shut down its computers, cancel operations and relocate patients**
- **"…[this] *incident highlights the opportunistic nature of cybercriminal groups and their willingness to demonstrate utter callousness in targeting hospitals on the front line of the fight against the coronavirus*"**

Impact of a ransomware cyberattack on a healthcare service provider

CASE OF THE IRISH NATIONAL HEALTH SERVICES

- **only 'discovered' in mid-May 2021[but]actual cyberattack had been launched in mid-March**
- **18 March 2021, someone in the Irish National Health Services' Executive had opened a spreadsheet that had been sent to them by email two days earlier. But the file was compromised with malware. The criminal gang behind the email spent the next two months working their way through the INHS networks**
- **tardiness of any cyber response from the INHS - a crucial opportunity to intervene was missed**
- **in the targeted "significant ransomware attack", more than 80 percent of the INHS' IT infrastructure was affected**
- **loss of key patient information and diagnostics**
- **resulting in severe impacts on the health service and the provision of care**
- **all their computer systems switched off, INHS doctors, nurses and other workers lost access to systems for patient information, clinical care and laboratories**

Irish NHS cont.

- cancellation of appointments and procedures at hospitals, paralysing their services and disrupting care
- "major problems" for radiology services, radiation oncology, elective surgeries and obstetrics and gynaecology appointments
- very limited access to diagnostics, lab services and historical patient records
- using a paper-based system, using pen and paper instead of their computers
- experienced significant delays due to the fallout from this ransomware attack, which slowed the pace of care and forced the diversion of some patients to other (private) medical facilities
- ramping up of COVID-19 vaccinations was in process
- processing of COVID-19 test results
- declared a "critical emergency"
- not to switch on, carry on working or leave their work devices on
- a second cyberattack the following day caused a substantial number of cancellations for outpatient services

Irish NHS cont.

- 24 May 2021, the hackers threatened to publicly release patient data unless the Irish authorities paid the demanded US$20 million ransom
- Irish Government firmly refused to pay this ransom nor to enter into any communications or negotiations with the hackers
- a ‘double extortion’ strategy by selling or publishing INHS private data if their ransom demand was not met
- to build an entirely new network, separate from the one that was affected
- to recruit, at a cost running into “tens of millions of Euros”, a large number of cyber- and IT experts to rebuild more than 2 000 distinct systems
- PWC report found that the ransomware attack did lock staff out of their computer systems and “severely” disrupted healthcare in Ireland
- the INHS information and network systems remained vulnerable (“frail”) and susceptible to even more serious attacks in the future
- “…transformational change required across the technology foundation for provision of health services and its associated cybersecurity”

Irish NHS cont.

- warned that other organisations needed to learn from and take cognisance of the hard lessons emanating from the cyberattack on the INHS
- "…criminal groups are choosing targets that will have the greatest impact on governments and the public, regardless of the collateral damage, in order to apply the most leverage" [i.e., maximise their profits]
- In February 2022, it was reported that the INHS had already spent more than US$48 million to recover from the devastating March 2021 ransomware attack
- costs associated with the ransomware attack included:
  - $14.2 million for ICT infrastructure;
  - $6.1 million to pay for outside cybersecurity assistance;0
  - $17.1 million for vendor support; and
  - $9.4 million for Office 365

Cyberattacks on healthcare are attacks on people!

- **At their most extreme, ransomware attackers interfered with healthcare systems vital in the fight against the Coronavirus**
- **Imagine you, as a patient or a member of your family, during the COVID-19 Pandemic, needed:**
  - **…urgent medical care and your ambulance is diverted;**
  - **…a prescription and your medical records are inaccessible;**
  - **…cancer treatment and radiation equipment is disrupted;**
  - **…therapy and your confidential session is published online;**
  - **…to be vaccinated and vaccines are unavailable due to supply chain disruptions?**

Some concluding remarks

- impacted significantly on patient care
- caused reputational damage
- resulted in enormous financial losses
- the encryption of files and locking down computers that typically contained electronic medical records
- being unable to access information about their patients' medical histories, the dosages of drugs that patients require and other critical medical information
- forced to resort to a paper-driven service
- some deaths during the COVID-19 pandemic, that under normal conditions might not have occurred, being a likely consequence of such a ransomware attack
- endangering as they did the lives and health (wellbeing) of patients
- putting nurses, doctors, healthcare workers at even more risk
- affecting treatment protocols
- also delaying the rollout of covid vaccination programmes

- exacerbated by the hacking of contact-tracing apps with hackers even targeting vaccine manufacturers and research laboratories
- all leading to the general disruption of the provision of medical and health services during the course of the pandemic
- Cybercriminals and ransomware operators, by adapting to the changed circumstances, took advantage of the pandemic to target vulnerable organisations – particularly in the healthcare sector
- in their attacks on hospitals and healthcare services, were opportunistically shameless in their attacks on this sector
- openly determined to make as much money as quickly as possible during the COVID-19 pandemic
- vitally needed to continue operating so as to be able to provide treatment to COVID-19 patients and thereby help save lives
- healthcare services and hospitals simply could not afford or allow their systems to be shut down ('locked out' of accessing them)
- knew that the healthcare sector would be more likely to pay a ransom to keep their operations functioning
- *"Ransomware attacks on health care systems put lives at risk, it's as simple as that"*

CyberPeace Institute Cyber Incident Tracer #Health cyberattack incidents

Table 1: CyberPeace Institute Cyber Incident Tracer #Health cyberattack incidents: 1 June 2020 to 1 June 2022

Healthcare sectors	Totals	Healthcare sectors	Totals
Patient care services	249	Pharmaceuticals, biotech companies & pharmacies	50
-hospitals	78		
-medical specialists	76	Medical manufacturing & development	34
-clinics	33	-medical manufacturer	27
-care provider	33	-medical research & developer	7
Mental health & substance abuse facility	21	National Health Systems	8
Other	33		
-laboratory & diagnostic services	15	-medical emergency response services	9
-ambulance services	3	-government	3
-telehealth & medical staff	2	-healthcare networks	1
TOTAL No. INCIDENTS			426

CyberPeace Institute Cyber Incident Tracer #Health cyberattack incidents

Table 2: Regions/countries where the majority of healthcare cyberattacks occurred: 1 June 2020 to 1 June 2022

Regions/Countries	Totals	Regions/Countries	Totals
North America	247	Europe	116
-US	234	-France	33
-Canada	13	- Germany	13
		- Spain	13
		- Switzerland	8
		- UK	7
South America	18	- Belgium	6
-Brazil	10		
Oceania	10	Other:	
-Australia	8	- South Africa	2
-New Zealand	2		
Total No. of countries			38

CyberPeace Institute Cyber Incident Tracer #Health cyberattack incidents

Impact & harm: For the period - 1 June 2020 to 1 June 2022, as reported to CPI

- Average number of records breached per incident: **160 000**
- Maximum number of records breached in a single cyberattack incident: **2 413 553**
- Total number of records breached 02/06/2020-20/05/2022: **17 444 888**

Operational impact duration per incident

- On average **19 days** duration per incident
- Maximum duration for one incident: **115 days**
- Total number of days of disruption experienced: **1 251**
- Percentage of incidents resulting in systems going offline: **56%** (*note: in 43% unknown)
- Percentage of incidents resulting in the exposure or leak of data: 71% (*note: 9% unknown)

Healthcare services cyber-vulnerabilities

- **the healthcare sector had significantly trailed other sectors of the world economy with its continued use of outdated IT systems**
- **was not part of their essential core business, for many years healthcare services underspent and under-budgeted for the expenses in updating to latest, newest cybersecurity IT systems to protect their databases, as well as their IoT medical devices linked to networks**
- **employing fewer trained IT staff, and**
- **lacking implementation of cybersecurity protocols**
- **not only protecting patient data**
- **of the safeguarding a hospital's financial data**
- **permitting controlled and secure access to medical data and patient information; and**
- **ensuring that medical equipment operates optimally when it is needed without any potential errors or disruption**
- **but suffered constantly from being under-resourced or under-skilled in terms of the implementation of effective cyber defence and protection measures on their networks**

Healthcare cyber-vulnerabilities cont.

- faced with financial decisions, which require them to prioritise the funding of staff and medical facilities that deliver front-line healthcare services, rather than investing in information technologies and cybersecurity no uniformity, no standardisation, nor standard operating procedures, with different data formats and non-uniform protocols of how individual hospitals interact with each other regarding medical records, healthcare insurance, or accounting practices
- their data systems tend to be 'stand-alone', and, therefore, more vulnerable to penetration by hackers and cybercriminals
- different care units/treatment sections could have their own data systems
- often do not have a co-ordinated cybersecurity system that overlay all of them in respect of regular updating of technical protocols
- healthcare demands for confidentiality, but also keeping some of the data private – with all of the attendant security challenges entailed in total, partial and limited privacy placed on linked datasets and information

Healthcare cyber-vulnerabilities cont.

- having so many endpoints to secure, such as tablets and smartphones
- generates huge vulnerabilities in hospital networks, since they may contain Electronic Protected Health Information records
- provide an entry or access point to such information databases, and other medical treatment machines
- cyber securing health/hospital/patient information became even more difficult with the trend, from the mid-2010s onwards, of increasing the use of mobile devices in the provision of a more flexible and enhanced patient healthcare
- lacking as they do the more powerful security features present on laptops and networked computers that have larger memory, RAM and storage capacity, makes them more easily hacked, thus creating new challenges for protecting the confidentiality and integrity of patient data
- use of 'Big Data' where patient information tended to reside in multiple locations that needed to be quickly and instantaneously accessed. That data was also extremely sensitive, with confidentiality and integrity both being key elements requiring its protection