Statement of Joshua Corman

For Senate Health, Education, Labor & Pensions Committee (HELP)

Full Committee Hearing
"Cybersecurity in the Health and Education Sectors"

May 18, 2022

Opening:
Chair Murray, Ranking Member Burr, and distinguished Members of the Senate Committee on Health, Education, Labor, and Pensions, thank you for the opportunity to testify today.

My name is Joshua Corman. I am a Philosopher, Hacker, Protector, and Puzzler… driven to make the world a safer place. Nearly 9 years ago, I founded "I am The Cavalry" (dot org) - a volunteer, cyber safety initiative focused on public safety and human life in the internet of things – or as we like to say: *"where Bits & Bytes meet Flesh & Blood"*. Most recently, I designed and drove what became the *CISA COVID Task Force* (under the CARES Act emergency hiring authority). I am an adjunct faculty for the CISO Certificate Program at Carnegie Mellon University's Heinz College. Lastly, I testified to the *2016 Presidential Commission on Enhancing National Cybersecurity*[1] and served on the (405c) *Health Care Industry Cybersecurity Task Force*[2] – initiated by Congress in the Cybersecurity Act of 2015.

Bottom Line Up Front:
Attacks on healthcare are increasing in volume, variety, and impact - with consequences now include the loss of life. While directionally-correct steps have been taken, we're getting worse faster than we're getting better. Bold actions and assistance will be required to change this trajectory, address these market failures, lack of incentives, and historical under-investments.

I'd like to bring you good news. However, the more consequential the subject matter, the more important it is to be forthright and avoid exaggeration in either direction. The candid truth is, I am more concerned about the cybersecurity of US healthcare than I ever have been.

Note: For events which occurred during my emergency Federal service (which ended January 14, 2022), I will err on discussing public and/or published materials.

Attackers have gotten stronger, but defenders have not - and many got weaker. The number of healthcare attacks have grown. The costs of the ransom payments have grown.[3] The impact of attacks are no longer merely measured by record count, fines, ransom payments, or recovery costs… but including double-digit millions of lost revenue and worse… degraded patient care and human life.[4] Crisis adjustments, made in a

[1] 2016 Presidential Commission on Enhancing National Cybersecurity https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf
[2] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[3] RTF Report: Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force https://securityandtechnology.org/ransomwaretaskforce/report/
[4] CISA Insights Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf..

hurry, added more technologies and attack surfaces. Financial constraints have forced reduced investments in cybersecurity staff and operating budgets.

The majority of healthcare regulations have focussed on the confidentiality of records. However, "**Cyber Safety is Patient Safety**". I love my privacy; I'd like to be alive to enjoy it. Yes, defensible connected technologies will require investment - as will the talent to defend them. Scrubbing-in before surgery takes time/money – *and* this vital hygiene practice dramatically reduces post-op infection, complications, and mortality rates. As technology increasingly plays a role in the delivery of modern healthcare, cyber-hygiene is no longer negotiable. While many have exclaimed they can't afford to do more, I tried to channel my inner Stan Lee: With Great Connectivity, Comes Great Responsibility…

With seams and cracks in healthcare noted in our 2017 405c report,[5] the pandemic widened and shattered those issues for many.

The pandemic brought an untenable, perfect storm of a record high need for patient care in the face of record high adversary activity, and severely diminished resources with which to defend the healthcare delivery environments.[6]

Degraded and delayed care affects patient outcomes.[7] Cybersecurity disruptions can cause and exacerbate delays and degrade care for a hospital, town, region, or even at the state level.[8]

Zooming out, while the country has 16 designated critical infrastructure sectors - with 55 National Critical Functions spanning them - Healthcare and "provide Medical Care" during the pandemic may be respective first among equals. Overall pandemic strains have not merely affected the general population, but have had material impact to the skill-workers and the critical infrastructure workforce that support foundational, life-line critical functions that underpin society (food, water, power, transportation, and brittle supply chains, etc.). As the CISA COVID Task Force came to an end in January, I was alerting CISA, the White House, Federal and Private Sector leadership of material erosions (10, 20, and 30%) to critical infrastructure workforce and difficult-to-replace skill workers - as they succumb to: death from COVID, death from non-COVID, injury, burnout, retirement, and alterations to their family support structure.

Adversaries are disrupting the bottom of Maslow's Hierarchy of Needs.[9] Insecurity at the

[5] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[6] Ransomware Hits Dozens of Hospitals in an Unprecedented Wave https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/.

[7] Delays in Emergency Care and Mortality during Major U.S. Marathons https://www.nejm.org/doi/full/10.1056/nejmsa1614073.

[8] Hospitals say cyberattacks increase death rates and delay patient care https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients.

[9] Maslow's hierarchy of needs https://en.wikipedia.org/wiki/Maslow%27s_hierarchy_of_needs.

base of his famous pyramid is not tenable for an individual - and certainly not sustainable for a country. Do not mess with Maslow…

Context:
My sentiment below becomes more true with each passing year:

> ***Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security.***

When I first wrote this, my hope was to prevent high consequence failure in cyber-physical-systems and critical infrastructure. Yet over the last 2 years, we have seen successful attacks and disruptions to:

- The *water* we drink[10,11]
- The *food* we put on our tables[12,13,1415]
- The *oil & gas* that fuels our cars and our homes[16]
- The *schools* our children attend[17,18,19]
- The timely *access to patient care* - with mortal consequences - during the strains of a pandemic[2021]

[10] A Hacker Tried to Poison a Florida City's Water Supply, Officials Say https://www.wired.com/story/oldsmar-florida-water-utility-hack/.
[11] Hackers Tried to Poison California Water Supply in Major Cyber Attack https://www.newsweek.com/san-francisco-water-plant-hack-cyber-attack-poison-supply-1601798.
[12] Ransomware Hits a Food Supply Giant—and Underscores a Dire Threat https://www.wired.com/story/jbs-ransomware-attack-underscores-dire-threat/.
[13] Ransomware gang strikes Iowa agriculture business New Cooperative, the latest hack on food supply chain https://www.cyberscoop.com/blackmatter-new-cooperative-ransomware-iowa/.
[14] 'Cyber event' knocks dairy giant Schreiber Foods offline amid industry ransomware outbreak https://www.cyberscoop.com/schreiber-foods-cyber-event-ransomware-agriculture-food/.
[15] AGCO's business operations disrupted by ransomware attack https://www.securitymagazine.com/articles/97576-agcos-business-operations-disrupted-by-ransomware-attack.
[16] Hackers Breached Colonial Pipeline Using Compromised Password https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.
[17] Ransomware Has Disrupted Almost 1,000 Schools in the US This Year https://www.vice.com/en/article/4awyvp/ransomware-has-disrupted-almost-1000-schools-in-the-us-this-year.
[18] Texas, California, New York, Louisiana, Missouri lead list of states with most ransomware attacks on schools: report https://www.zdnet.com/article/texas-california-new-york-and-louisiana-missouri-lead-list-of-states-with-most-ransomware-attacks-on-schools-report/.
[19] Hackers prey on public schools, adding stress amid COVID pandemic - Albuquerque, NM https://www.pbs.org/newshour/education/hackers-prey-on-public-schools-adding-stress-amid-covid-pandemic.
[20] Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.
[21] Ransomware Attack Hits Universal Health Services https://www.wsj.com/articles/ransomware-attack-hits-universal-health-services-11601341873.

- The *municipalities* who run our towns and our cities[22,23,24]
- ….even *Federal agencies* charged with public safety and national security…[25,26]

…stuff… is on fire…

We were prone. We were prey. Our predators finally noticed. Their largely-unchecked aggression has emboldened them. With blood in the water from the strains of the pandemic, healthcare found itself in a feeding frenzy.

Escalation over the last few years in Healthcare:
In early 2016, because of hard-earned trust built between I am The Cavalry and the FDA,[27] I had the privilege to serve on the CISA 2015 405c Congressional Task Force on these matters.[28] Our task force started shortly after an untargeted SamSam ransomware hit Hollywood Presbyterian Hospital in LA - diverting ambulances to other facilities, canceling surgeries, and even moving critical care patients.[29] It ended near Mother's Day weekend 2017 with WannaCry wreaking havoc on UK healthcare - manifesting many of our worst fears.[30] Prior to knowing this would happen, the banner graphic in our report to congress earlier that week stated bluntly:

"HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION"

[22] Amid a surge in ransomware attacks, cities are taking some of the biggest hits https://www.washingtonpost.com/politics/amid-a-surge-in-ransomware-attacks-cities-are-takingsome-ofthe-biggest-hits/2021/09/02/9bd5d654-0a84-11ec-aea1-42a8138f132a_story.html.

[23] Hackers have been holding the city of Baltimore's computers hostage for 2 weeks https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers.

[24] Four months on from a sophisticated cyberattack, Alaska's health department is still recovering https://www.zdnet.com/article/four-months-on-from-sophisticated-cyber-attack-alaskas-health-services-is-still-recovering/.

[25] DHS, DOJ And DOD Are All Customers Of SolarWinds Orion, The Source Of The Huge US Government Hack https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=a170ec825e68.

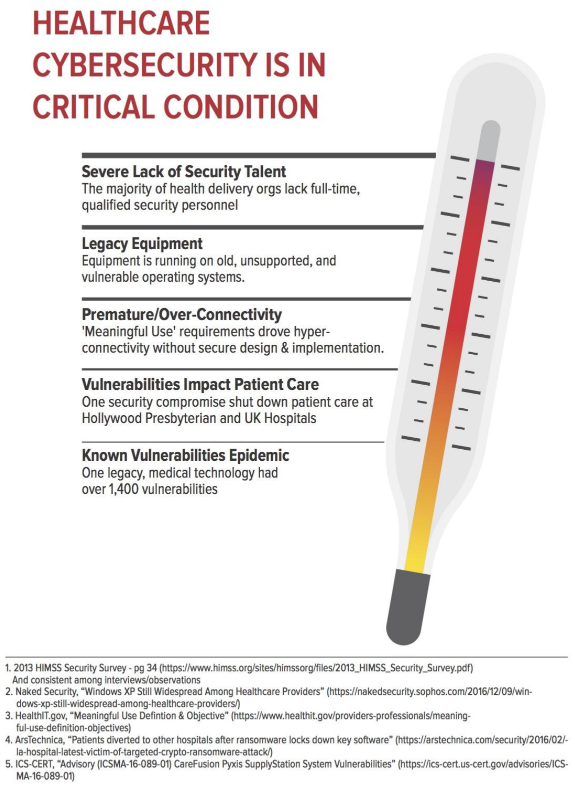
[26] Suspected Russian hackers spied on U.S. Treasury emails - sources https://www.reuters.com/article/us-usa-cyber-amazon-com-exclsuive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG.

[27] Hippocratic Oath for Connected Medical Devices https://iamthecavalry.org/issues/medical/oath/.

[28] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[29] Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers https://www.csoonline.com/article/3033160/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html.

[30] NHS could have avoided WannaCry hack with 'basic IT security', says report https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office.



HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

1. 2013 HIMSS Security Survey - pg 34 (https://www.himss.org/sites/himssorg/files/2013_HIMSS_Security_Survey.pdf) And consistent among interviews/observations
2. Naked Security, "Windows XP Still Widespread Among Healthcare Providers" (https://nakedsecurity.sophos.com/2016/12/09/windows-xp-still-widespread-among-healthcare-providers/)
3. HealthIT.gov, "Meaningful Use Defintion & Objective" (https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives)
4. ArsTechnica, "Patients diverted to other hospitals after ransomware locks down key software" (https://arstechnica.com/security/2016/02/-la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/)
5. ICS-CERT, "Advisory (ICSMA-16-089-01) CareFusion Pyxis SupplyStation System Vulnerabilities" (https://ics-cert.us-cert.gov/advisories/ICSMA-16-089-01)

Almost exactly five years later, the situation has grown much more severe.[31] Without bold leadership and swift action, I fear we're not yet to the worst of it.

In June of 2017, while in Tel Aviv CyberWeek explaining to our UN counterparts how lucky we all got with WannaCry, Russia's NotPetya escaped its intended blast radius of Ukraine causing more than $10B of damage worldwide - with $1B alone to Merck Pharmaceuticals.[32] It was at that time that I challenged that international policy cohort to consider a "Cyber-No-Fly-Zone" on at least hospitals (chronicled in the *Sandworm* book).[33] I argued that harms from cyber-munitions against hospitals - intentional or otherwise - should be severely punished and sanctioned. While most allies are loath to enact norms or treaties about cyber-conflict, it is routinely discussed that attacks from a Nationstate, harming country-designated "critical infrastructure" could constitute an act of war.[34] NOTE: Healthcare is designated Critical Infrastructure.

[31] 5 Years That Altered the Ransomware Landscape https://www.darkreading.com/endpoint/five-years-that-changed-the-ransomware-landscape.

[32] The Untold Story of NotPetya, the Most Devastating Cyberattack in History https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[33] Sandworm by Andy Greenberg https://www.penguinrandomhouse.com/books/597684/sandworm-by-andy-greenberg/.

[34] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9.

Over the next few years, the ransomware revolution grew bolder and more sophisticated, expanding their appetite to more types of prey.[35] The unavailability of what's important to *you*, can be made valuable to *them*.

As the pandemic reached US soil in early 2020, in the Sandbox at the RSA Conference, I warned then-Director Krebs that I expected a larger volume and variety of ransom attacks on hospitals. I offered a "director's cut" of our 2017 report to congress for him and his team - when the time was right. A few weeks later he called. He did not ask for the briefing. Instead, he asked if I would serve my country for a year. I'll next outline what happened over the next two years.

Cyber-Attacks during COVID-19:
As feared, unscrupulous threat actors started attacking hospitals and medical supply chains for vital and scarce supplies like Personal Protective Equipment (PPE).[36] Scores of volunteer cybersecurity do-gooders formed groups like the CTI League (Cyber Threat Intelligence League) to assist governments in identifying bad actor infrastructure.[37] CISA had already launched what they called PROJECT TAKEN to help hospitals (approximately 85% of whom lacked a single, experienced cybersecurity person on staff).[38,39] As I was being on-boarded through the CARES Act, the country was additionally organizing around what became Operation Warp Speed (OWS). Our eventual CISA COVID Task Force took responsibilities with both - across the interagency.[40]

In addition to engaging and attempting to protect OWS entities, my initial focus was prioritizing a long list of smaller, but potentially vital suppliers to the official OWS funded entities. Using a strategy I dubbed our "Ball Bearings" analysis… We spotted smaller, weak links in the vaccine supply chains who if disrupted could have a profound impact on American lives and interests.[41,42] A recurring uncomfortable reality was that most of these entities lacked even the most basic of cybersecurity. As was the case with healthcare delivery organizations (HDOs), these ball bearings were "*Target Rich, but Cyber Poor*". We were going to have to meet them where they are, and bring

[35] WSJ Mounting Ransomware Attacks Morph Into a Deadly Concern https://www.wsj.com/articles/mounting-ransomware-attacks-morph-into-a-deadly-concern-11601483945.
[36] PPE, COVID-19 Medical Supplies Targeted by BEC Scams https://threatpost.com/ppe-covid-19-medical-supplies-bec-scams/154806/
[37] CTI League https://cti-league.com/.
[38] US cyber officials try to channel Liam Neeson in responding to coronavirus threats https://www.cyberscoop.com/project-taken-liam-neeson-dhs-cybersecurity-coronavirus/.
[39] Health Care Industry Cybersecurity Task Force Report https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
[40] THE COVID-19 VACCINES WEREN'T HACKED — THIS TASK FORCE IS ONE REASON WHY https://www.theverge.com/2021/7/8/22568397/covid-vaccine-cybersecurity-cisa-task-force.
[41] CyberCast Season 3 Episode 18 - How CISA's COVID-19 Task Force Protected Hospitals and the Vaccine Supply Chain https://www.youtube.com/watch?v=gI40RaxCfIk.
[42] Business Insider - Meet the government worker who cut through months' worth of federal bureaucracy in 10 days to help millions of Americans get vaccinated https://www.businessinsider.com/cisa-kenrda-martin-covid-vaccine-bureaucracy-2021-6.

fit-for-purpose methods to identify and buy down the risks that we could. This later became the foundation for what I've been calling the "*Pragmatic Security Suite*".

September saw an uptick in attacks on hospitals. The large, publicly traded hospital network known as UHS suffered a fairly serious ransomware attack.[43] This was my first big opportunity to work across the interagency. It was far more challenging than I was expecting. The good news: this was part of why the CARES Act was enacted – to help combine experience and skills to better serve the public throughout the pandemic. Given that UHS is publicly traded, several of the impacts were eventually disclosed - including a declared $67MM in lost revenue from the ordeal.[44,45]

While many across the healthcare sector discussed the growing impacts of records lost, fines levied, dollars paid to ransoms and restoration services, and now significant lost business… I began to fear that these service disruptions would be measured in degraded and delayed care, patient outcomes, and even lost lives.

Not long after the UHS experience, I helped to rally HHS, FBI, and CISA to issue a joint three-agency (Tri-Seal) Alert to warn the sector of a credible threat to disrupt plural US Healthcare entities concurrently - in close proximity to the US Presidential Election.[46] While we did our best to warn, far too many already strained hospitals fell victim to these more aggressive attacks. At the time, there were some who doubted the intelligence,[47] but in subsequent coverage and reporting from WIRED, the Wall Street Journal, and others… proved the intent to disrupt and intercepted communications reveal just how serious and perilous this was for the country.[48] These attacks felt at least state-tolerated… but more recent reporting suggests they were even state directed.[49] Not only are hospitals designated critical infrastructure, but they are also more taxed and strained than sustainable - without cyber-disruption.

Some victims of this campaign suffered severe and protracted effects on patient care. One such public example was in Vermont - covered in a harrowing story in the NYT.[50] In

[43] UHS Hospitals hit by Ryuk ransomware, forced to shut down systems https://www.securitymagazine.com/articles/93482-uhs-hospitals-hit-by-ryuk-ransomware-forced-to-shut-down-systems.

[44] Cyberattacks Cost Hospitals Millions During Covid-19 https://www.wsj.com/articles/cyberattacks-cost-hospitals-millions-during-covid-19-11614346713.

[45] United States Securities and Exchange Commission - United Health Services, Inc. https://www.sec.gov/Archives/edgar/data/0000352915/000156459022006717/uhs-10k_20211231.htm.

[46] Alert (AA20-302A) - Ransomware Activity Targeting the Healthcare and Public Health Sector https://www.cisa.gov/uscert/ncas/alerts/aa20-302a.

[47] Healthcare Providers Were Warned of a Ransomware Surge Last Fall. Some Still Aren't Sure How Serious the Threat Was https://therecord.media/healthcare-providers-were-warned-of-a-ransomware-surge-last-fall-some-still-arent-sure-how-serious-the-threat-was/.

[48] Ransomware Hits Dozens of Hospitals in an Unprecedented Wave https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/.

[49] Leaked Ransomware Docs Show Conti Helping Putin From the Shadows https://www.wired.com/story/conti-ransomware-russia/.

[50] Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

an attempt to assist future victims, the University of Vermont Medical Center eventually published a detailed report of how this attack affected their oncology capabilities.[51]

Major attacks would later degrade and delay care in other regions and states. After the Scripps attacks in San Diego, Dr. Christian Dameff began writing about how an attack on one hospital can drive significant surplus case loads onto proximal, alternative care facilities - with cascading effects.[52,53,54,55]

Excess Deaths and Loss of Life:
Delays affect mortality rates.[56] Cyberattacks can cause delays - big ones.[57]

In early 2021, I asked the team an uncomfortable question:
Can these cyberattacks contribute to loss of life?

With some analysis and data science, we were able to measure how they can.

The simplified abstraction is this:
Ransoms can strain hospitals to levels associated with Excess Deaths.[58]

We studied a state hit hard by ransomware - for a statistically significant observation period. In the same state, with the same population, during the same pandemic, controlling for hospital type and size, locations hit by ransom both achieved these excess death danger zones sooner and stayed there longer than their peers.

Sanitized versions of these models and methods were published in late 2021.

[51] JCO Oncology Practice: Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect https://ascopubs.org/doi/full/10.1200/OP.21.00116.
[52] San Diego EDs Deluged With Patients After Cyberattack https://www.medpagetoday.com/meetingcoverage/acep/95357.
[53] Annals of Emergency Medicine - Research Forum Abstract: 108 Emergency Department Crowding Resulting from a Local Health System Cyberattack https://www.annemergmed.com/article/S0196-0644(21)00959-8/fulltext.
[54] Annals of Emergency Medicine - Research Forum Abstract: 7 Impact of a Hospital Cyberattack on EMS Arrivals at Neighboring Emergency Departments https://www.annemergmed.com/article/S0196-0644(21)00856-8/fulltext.
[55] Annals of Emergency Medicine - Research Forum Abstract: 162 Regional Emergency Department Census Impacts During a Cyber Attack https://www.annemergmed.com/article/S0196-0644(21)01014-3/fulltext.
[56] Delays in Emergency Care and Mortality during Major U.S. Marathons https://www.nejm.org/doi/full/10.1056/nejmsa1614073.
[57] Hospitals say cyberattacks increase death rates and delay patient care https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients.
[58] The Pandemic Revealed the Health Risks of Hospital Ransomware Attacks https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks.

On October 1st, CISA Published a collection of this analysis in a report called: *“Provide Medical Care Is In Critical Condition”*.[59] The Excess Death / Hospital Strain data science instrument was subsequently published on November 18th, 2021 in the CDC MMWR (Morbidity and Mortality Weekly Report) called “Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic”.[60] To make these dense reports more accessible, we recorded a short CISA Webinar as well.[61]

As CISA was about to publish our statistical evidence regarding loss of life, the Wall Street Journal published a front page story about a baby who died after a complicated birth at an Alabama hospital that had recently suffered disruptions from a cyberattack.[62]

A bit more on the Excess Deaths
The CISA COVID Task Force had been analyzing risks and system dynamics related to the National Critical Function (NCF) known as “Provide Medical Care”. In February 2021, when the country hit the sobering milestone of 500,000 Americans lost to COVID,[63] we had also achieved an additional 150,000 Americans lost to what the CDC tracks as Excess Deaths. Excess Deaths are defined as the difference between expected deaths and actual deaths - by month, condition, and state. As we dug into the year of Excess Deaths, several things concerned us. Unlike COVID deaths affecting primarily 65+ year olds, 25-44 year olds were the fastest growing portion of these Excess Deaths. A review of the top causes revealed several time-sensitive conditions for which delayed access to care is known to affect mortality rates (heart, brain, pulmonary, etc). I know from my Cavalry and 405c Task Force work that, for example:

> Even 4.4 minutes can affect mortality rates for heart attacks (NEJM)[64]
> 1-4 hours is critical to save brain/life with strokes; the Golden hour(s)

We chose to study these Excess Deaths more closely - and to hopefully find ways to mitigate these losses of life.

One of our findings was stunning. We found a strong positive correlation between Adult Intensive Care Unit (ICU) Bed utilization and Excess Deaths two, four, and six weeks later. In the model, if the country hit 75% ICU Bed utilization, you’d expect 18,000 lost Americans in two weeks. If the model hit 100%, it would indicate 80,000 lost Americans in two weeks. Delayed and degraded care affects outcomes for time sensitive conditions. ICU strain significantly added delays. Cyberattacks made them worse.

[59] CISA Insights Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm https://www.cisa.gov/sites/default/files/publications/CISA_Insight_Provide_Medical_Care_Sep2021.pdf.

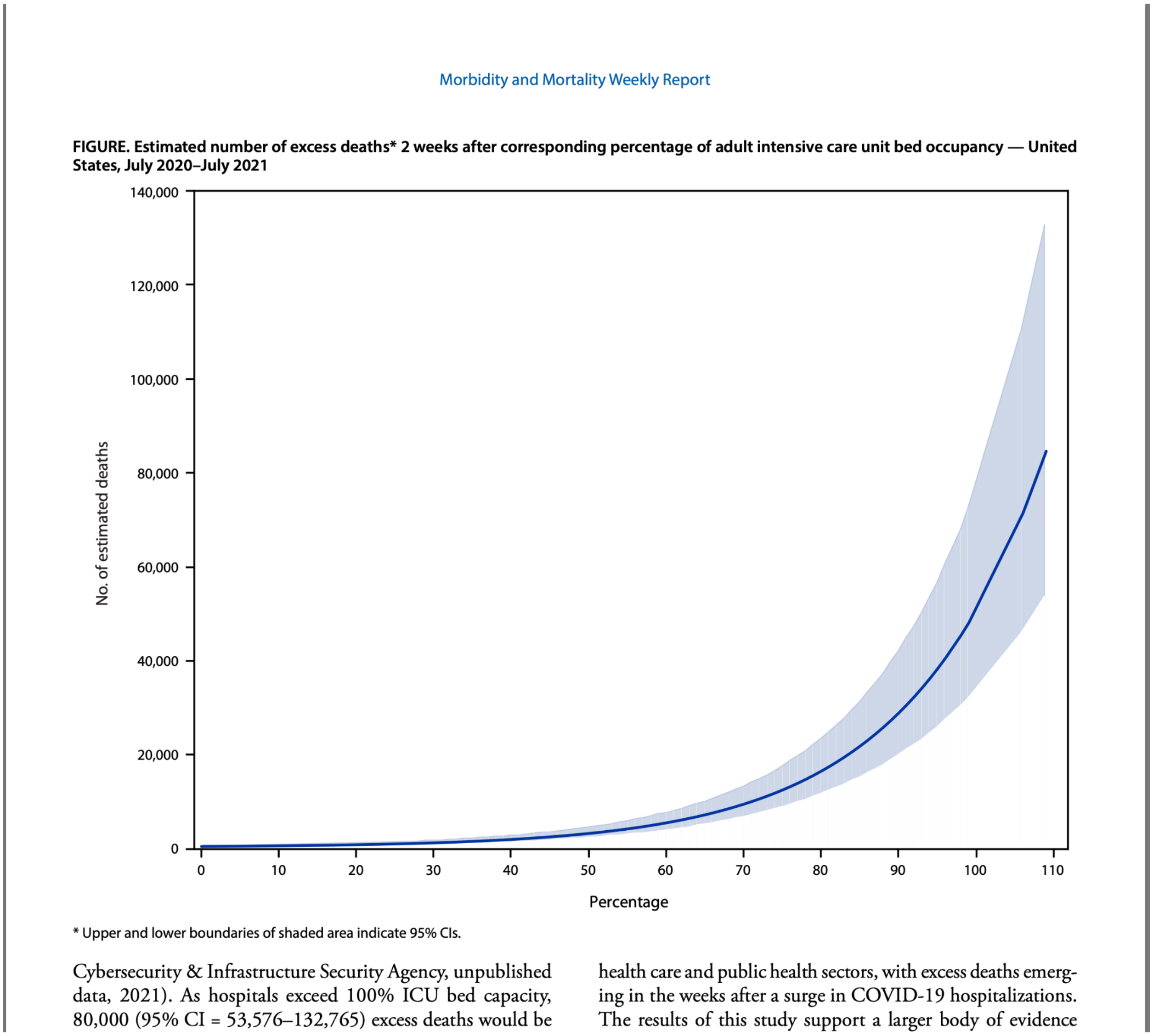
[60] CDC MMWR Impact of Hospital Strain on Excess Deaths During the COVID-19 Pandemic — United States, July 2020–July 2021 https://www.cdc.gov/mmwr/volumes/70/wr/mm7046a5.htm.

[61] CISA COVID Task Force: “Provide Medical Care is in Critical Condition” December 2021 https://www.youtube.com/watch?v=F-uh-lx_KKU&t=6s.

[62] WSJ Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.

[63] Entering uncharted territory, the U.S. counts 500,000 Covid-related deaths. https://www.nytimes.com/2021/02/22/us/us-covid-deaths-half-a-million.html.

[64] Delays in Emergency Care and Mortality during Major U.S. Marathons https://www.nejm.org/doi/full/10.1056/nejmsa1614073.



Morbidity and Mortality Weekly Report

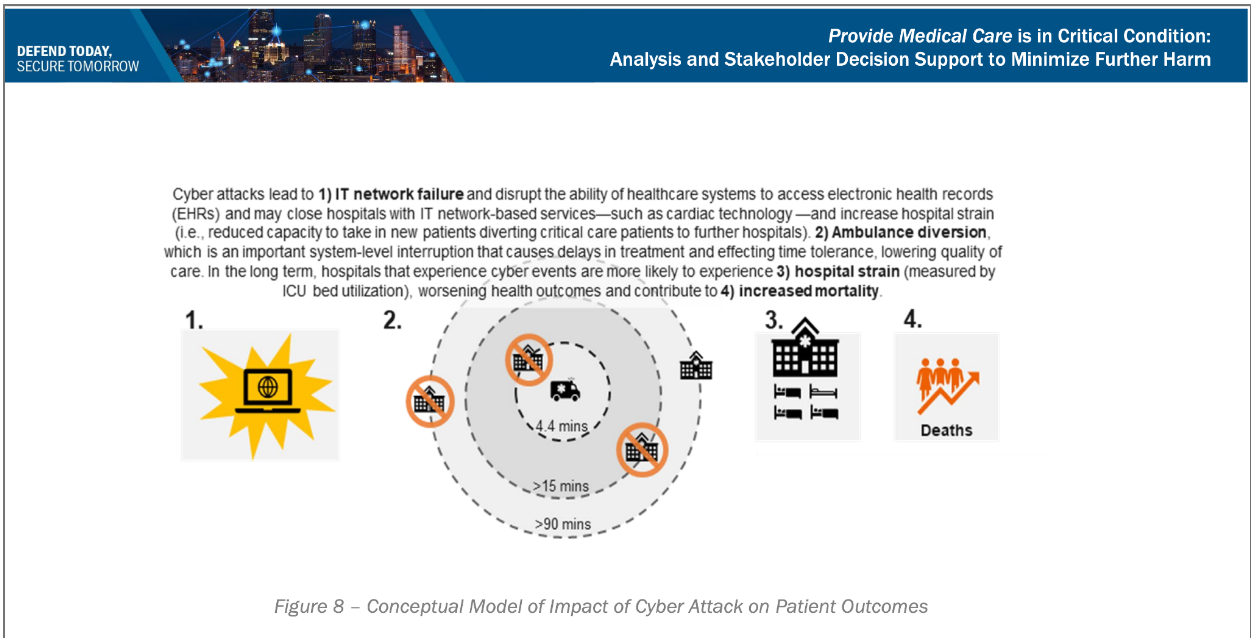
FIGURE. Estimated number of excess deaths* 2 weeks after corresponding percentage of adult intensive care unit bed occupancy — United States, July 2020–July 2021

* Upper and lower boundaries of shaded area indicate 95% CIs.

Cybersecurity & Infrastructure Security Agency, unpublished data, 2021). As hospitals exceed 100% ICU bed capacity, 80,000 (95% CI = 53,576–132,765) excess deaths would be

health care and public health sectors, with excess deaths emerging in the weeks after a surge in COVID-19 hospitalizations. The results of this study support a larger body of evidence

While this Excess Death math is a feature of the pandemic strains, the systems analysis revealed the elevated risk of loss of life when (for example) ambulance diversions are too far away for the time-sensitive conditions. Also, with the financial strains from covid and the substantive losses of skill workers in healthcare, we will not return to safer capacity levels for some time.



DEFEND TODAY, SECURE TOMORROW

Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm

Cyber attacks lead to **1) IT network failure** and disrupt the ability of healthcare systems to access electronic health records (EHRs) and may close hospitals with IT network-based services—such as cardiac technology —and increase hospital strain (i.e., reduced capacity to take in new patients diverting critical care patients to further hospitals). **2) Ambulance diversion**, which is an important system-level interruption that causes delays in treatment and effecting time tolerance, lowering quality of care. In the long term, hospitals that experience cyber events are more likely to experience **3) hospital strain** (measured by ICU bed utilization), worsening health outcomes and contribute to **4) increased mortality**.

Figure 8 – Conceptual Model of Impact of Cyber Attack on Patient Outcomes

Pragmatism for the Target Rich; Cyber Poor:
Years ago, my colleague from industry, Wendy Nather coined: "Living Below the Security Poverty Line."[65] Throughout my emergency Federal Service, and with a focus on Critical Infrastructure, I channeled this into what I've been calling **Target Rich; Cyber Poor.** An entity can be **Cyber Poor** if there is a deficiency in one or more of the following three areas:

- Insufficient Information/Awareness
- Insufficient Incentives (Carrots/Sticks)
- Insufficient Resources

Going back to the 405c Task Force Report, **our estimate was that 85% of the healthcare delivery organizations in the country lack a single, experienced cybersecurity person on staff**. We saw similarly prone targets in the vaccine supply chain ball bearings. We saw similar conditions in Water & Waste Water, in Food Production, etc.

There is a massive split between the *Haves* and the *HaveNots* of critical infrastructure. The *Haves* might attempt "Best Practices" and are likely in or around Sector Coordinating Councils and ISACS and running the race. The *HaveNots* of the Cyber Poor may not even be at the starting line. It became clear to me that we would need to reckon with these *HaveNots* - meet them where they are, and identify and buy down risk… *Crawl, then Walk, then Run*.

[65] Security Ledger Episode 223: CISA Looks To Erase The Security Poverty Line https://securityledger.com/2021/08/episode-223-cisa-looks-to-erase-the-security-poverty-line/.

During the Microsoft Exchange attacks,[66] I watched the Cyber Poor / Resource Poor being encouraged to “Implement Zero Trust” or “Just Do Best Practices”. Many were asking if software updates would be provided for their Unsupported versions of Exchange. The Chief Data Scientist of Rapid7, Bob Rudis, then surveyed the Internet to find that the dominant versions of Exchange were unsupported. This was especially bad in healthcare. I decided that day that we needed to invert the script. I started working on CISA’s “**Bad Practices**” - the most dangerous practices for owners and operators of critical infrastructure.[67] This list currently has three entries including: the first of which, the use of Unsupported and End of Life Software in service of Critical Infrastructure.

Next I shifted to something I teach my CMU students: **S.O.S.** Get your “stuff” off search.[68] See what your adversaries see about your internet facing infrastructure. We wrote CISA’s *Stuff Off Search* program. A free way to see if your assets are showing - and how to reduce that attack surface.

We use **S.O.S.** as a gateway to the free, taxpayer funded CISA **Cyber Hygiene (CyHy)** Scanning Service – which will send daily scan results of known vulnerabilities to you.[69] And since you likely cannot fix all of them, the CISA **KEV** list can tell you the **K**nown **E**xploited **V**ulnerabilities to prioritize first.[70]

Since attacks are likely to be successful, perhaps the best way to know how you might fare is to practice failure with lightweight **table top crisis simulations** (also offered by CISA).[71]

We rolled these together into a collection we informally called the *Pragmatic Security Suite*… a short set of self service webinar videos.[72]

Be under no illusions… these will not make the Cyber Poor immune to attackers. But they may be the difference in opportunistic attacks. This starts their journey… but there will need to be strong incentives and assistance to advance this journey.

Good steps - in need of acceleration:
There are some bright spots, but these efforts need to move more quickly.

[66] The Microsoft Exchange Server hack: A timeline https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html.
[67] CISA Bad Practices https://www.cisa.gov/BadPractices.
[68] CISA Stuff Off Search https://www.cisa.gov/publication/stuff-off-search.
[69] CISA Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services.
[70] CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[71] CISA Tabletop Exercises Packages https://www.cisa.gov/cisa-tabletop-exercises-packages.
[72] The Pragmatic Cyber Security Series https://www.cisa.gov/pragmatic-cyber-security-webinar.

- The FDA CyberSecurity Pre-Market[73] and Post-Market[74] Guidance: Suzanne Schwartz has leaned-in and shown bold leadership. She needs more support and authority to drive these advances more quickly.[75,76] Hospitals are desperate for these fortifications. This is helpful for FDA approved technologies, but EHRs and other non-FDA regulated. healthcare tech require similar levels of care
- SBOM[77] (Software Bill of Materials): This Software Supply Chain foundational enabling artifact/practice is in the FDA Pre-Market Draft,[78] enjoyed an 3.5 voluntary cultivation via NTIA,[79,80] made it into President Biden's CyberSecurity Executive Order,[8182] and is *increasingly* proving its necessity on large scale issues like the most recent Log4j exposures.[83,84] Parts of industry still fear this transparency and want to go more slowly than we can afford. The Healthcare Proof of Concept team developed an open source tool "Daggerboard" to ingest/manage SBOMs to protect hospitals… its full value will grow as SBOMs become more readily available
- Medical/Clinical Hacking Simulations: I am The Cavalry teamed with doctors to start the Cyber Med Summits[85,86,87] - now a formal 501(c)(3) non-profit. ER & OR hacking simulations and table-top exercises show healthcare stakeholders how real medical technology hacks affect patient care. We have hacked insulin

[73] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff https://www.fda.gov/media/119933/download.

[74] Postmarket Management of Cybersecurity in Medical Devices https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices.

[75] H.R.7084 - PATCH Act of 2022 https://www.congress.gov/bill/117th-congress/house-bill/7084/text

[76] S.3983 - PATCH Act https://www.congress.gov/bill/117th-congress/senate-bill/3983/text

[77] NTIA Software Bill of Materials https://www.ntia.gov/sbom.

[78] 115th Congress of the United States Committee on Energy and Commerce Letter from Chairman Walden to Acting Secretary Hargan https://republicans-energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf.

[79] NTIA Launches Initiative to Improve Software Component Transparency https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency

[80] NTIA Software Component Transparency https://www.ntia.gov/SoftwareTransparency.

[81] EO 14028: Improving the Nation's Cybersecurity https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[82] EO 14028: The Minimum Elements For a Software Bill of Materials (SBOM) https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom.

[83] Log4j is why you need an SBoM https://blog.reversinglabs.com/blog/log4j-is-why-you-need-an-sbom.

[84] Nature: Building resilient medical technology supply chains with a software bill of materials https://www.nature.com/articles/s41746-021-00403-w.

[85] CyberMed Summit https://www.cybermedsummit.org/.

[86] ABC Nightline: Fears of hackers targeting US hospitals, medical devices for cyber attacks https://abcnews.go.com/Health/fears-hackers-targeting-us-hospitals-medical-devices-cyber/story?id=48348384.

[87] Mark Albert: Efforts to protect patients from cyberattacks grow https://www.wisn.com/article/efforts-to-protect-patients-from-cyberattacks-grow/27493371#.

pumps, pacemaker defibrillators,[88,89] bedside infusion pumps, imaging systems, blood bank databases, building automation systems, EHRs, and more. Experiential learning forums like these could inform and inspire more awareness - sooner.

- Mandatory Breach Reporting[90] to CISA: I was pleased to see this passed into law, but disappointed to see a multi-year rule making process. With so many attacks and such poor reporting, we need to move as quickly as possible. We cannot shift to studying and preventing attacks without adequate and timely visibility into them
- Bad Practices[91] are declared: Who will help to drive them toward extinction? Sector Specific Regulators? FTC? SEC? The Insurance Industry is talking about their role… I could see arguments around due care and negligence getting traction if encouraged
- SRMAs (Sector Risk Management Agencies) are now in statute: but/and the interagency, shared responsibility model with CISA (and FBI, etc) is *far* from where it needs to be. Our CISA Covid Task Force got a lot of great things accomplished outside of interagency comfort zones… and I fear those positive models have diminished since our task force was ended. **Cybersecurity is a team sport**… the sooner we find the optimal shared responsibility model… the sooner we can do what the country needs us to… Perhaps the newly formed ONCD in the White House can assist here

Failed Markets & Getting Beyond Voluntary:
Congress has acted in directionally-correct ways - plural times.[92,93] Industry prefers voluntary… and yet, we're now seeing more and more devastating attacks to healthcare.[94,95,96] Critical Infrastructure needs to work.

The NIST CYbersecurity Framework is voluntary - and nearly a decade later, OIG reports show we still have poor visibility into if it is being used or not.[97] The

[88] Digital Defenses for Hacked Hearts: Why Software Patching Can Save Lives https://www.jacc.org/doi/10.1016/j.jacc.2018.03.540

[89] FDA Warning Letter - Abbott (St Jude Medical Inc.) https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/abbott-st-jude-medical-inc-519686-04122017

[90] H.R.2471 - Consolidated Appropriations Act, 2022 https://www.congress.gov/bill/117th-congress/house-bill/2471/text

[91] CISA Bad Practices https://www.cisa.gov/BadPractices.

[92] 115th Congress of the United States Committee on Energy and Commerce Letter from Chairman Walden to Acting Secretary Hargan https://republicans-energycommerce.house.gov/wp-content/uploads/2017/11/20171116HHS.pdf

[93] H.R.4611 - DHS Software Supply Chain Risk Management Act of 2021 https://www.congress.gov/bill/117th-congress/house-bill/4611/text.

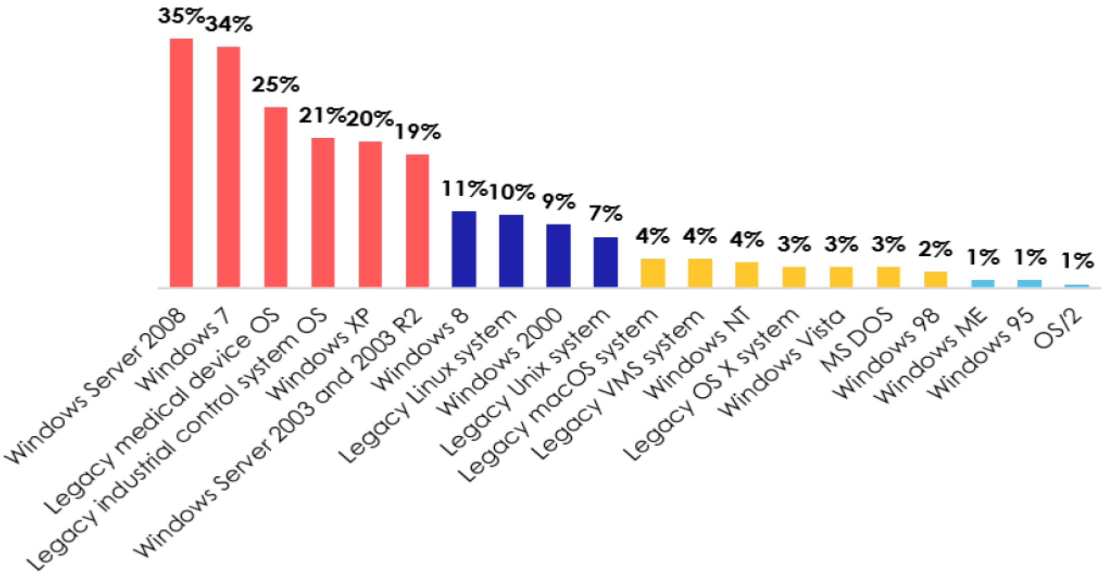
[94] RTF Report: Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force https://securityandtechnology.org/ransomwaretaskforce/report/.

[95] Nine security lessons from the 'Conti cyber attack on the HSE' report https://bhconsulting.ie/nine-security-lessons-from-the-conti-cyber-attack-on-the-hse-report/.

[96] Mark Albert: Efforts to protect patients from cyberattacks grow https://www.wisn.com/article/efforts-to-protect-patients-from-cyberattacks-grow/27493371#.

Cybersecurity Act of 2015 reduced the risk of information sharing and provided some safe harbor for reporting to CISA, yet it isn't being used for more than a tiny fraction of publicly observable attacks. FDA has done a great job raising the bar for the Cybersecurity of new devices and have even issued safety communications and affected recalls.[98,99] Yet hospitals continue to use these recalled devices and unsupported devices - as the norm. Without HHS CMS and/or Joint Commission requirements, we will remain prone. And… With mandatory minimums, there may need to be assistance. Our 405c Task Force had suggestions for Cash-For-Clunkers-like models for technology refresh programs to remove the most dangerous equipment from rotation. HIMSS surveys show legacy & unsupported software remains unaddressed[100]

Figure 12: Legacy (Unsupported) Operating Systems in Place



Seatbelts weren't voluntary. I don't believe fire escapes were voluntary - nor kitchen sanitation codes for commercial restaurants. Public Safety isn't free. The lack of sufficient public safety and public good is also dis-economic. Further crisis of confidence in the public in modern healthcare will drive devastating harms to the public safety, economic, and national security.

[97] Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals https://oig.hhs.gov/oei/reports/OEI-01-20-00220.asp.

[98] LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities https://wayback.archive-it.org/7993/20170112164109/http:/www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm446828.htm.

[99] FDA warns of security flaw in Hospira infusion pumps https://www.reuters.com/article/hospira-fda-cybersecurity-idCNL1N10B2GY20150731.

[100] 2021 HIMSS Healthcare Cybersecurity Survey Report https://www.himss.org/resources/himss-healthcare-cybersecurity-survey.

The Therac-25 radiation delivery machine's software design flaws killed people.[101,102] At the time, they wanted to give it a few more years before we introduced liability to software.[103,104] That was 37 years ago. We're now seeing more brazen adversaries, more nation state use of cyberwarfare, and more frequent and consequential attacks on designated critical infrastructure.

As the world is increasingly depending upon digital infrastructure,[105] that infrastructure needs to be more dependable.

The cybersecurity of healthcare is not trending in the right direction. We can do something about that. We must.

[101] An investigation of the Therac-25 accidents https://ieeexplore.ieee.org/document/274940.
[102] The Therac-25: 30 Years Later https://www.computer.org/csdl/magazine/co/2017/11/mco2017110008/13rRUxAStVR.
[103] 2014 RSAC Webinar - Software Liability?: The Worst Possible Idea (Except for all Others) https://www.rsaconference.com/library/webcast/webcast-software-liability-the-worst-possible-idea-except-for-all-others.
[104] 2017 RSAC Talk: SW Liability? Uncomfortable Truths Require Uncomfortable Response https://youtu.be/yGIAC6zxVnc.
[105] Andrea Matwyshyn - Internet of Bodies https://scholarship.law.wm.edu/wmlr/vol61/iss1/3/.