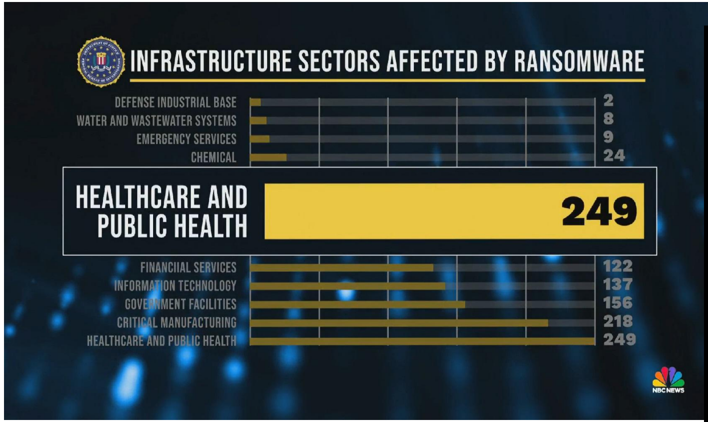
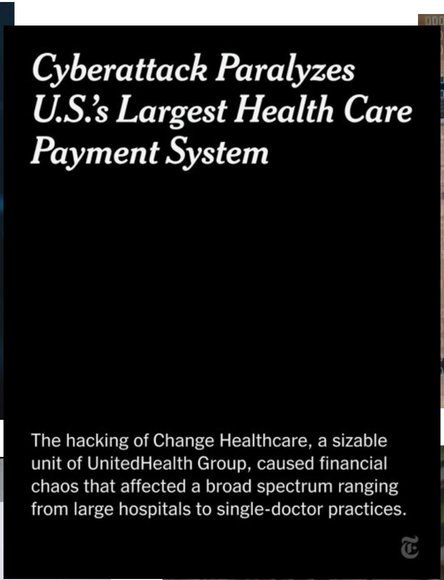
The MIT Cybersecurity Clinic

https://urbancyberdefense.mit.edu/

Speaker: Jungwoo Chun

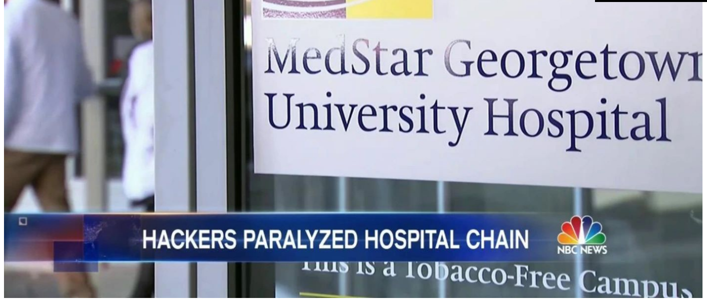




Cyberattack Paralyzes U.S.'s Largest Health Care Payment System

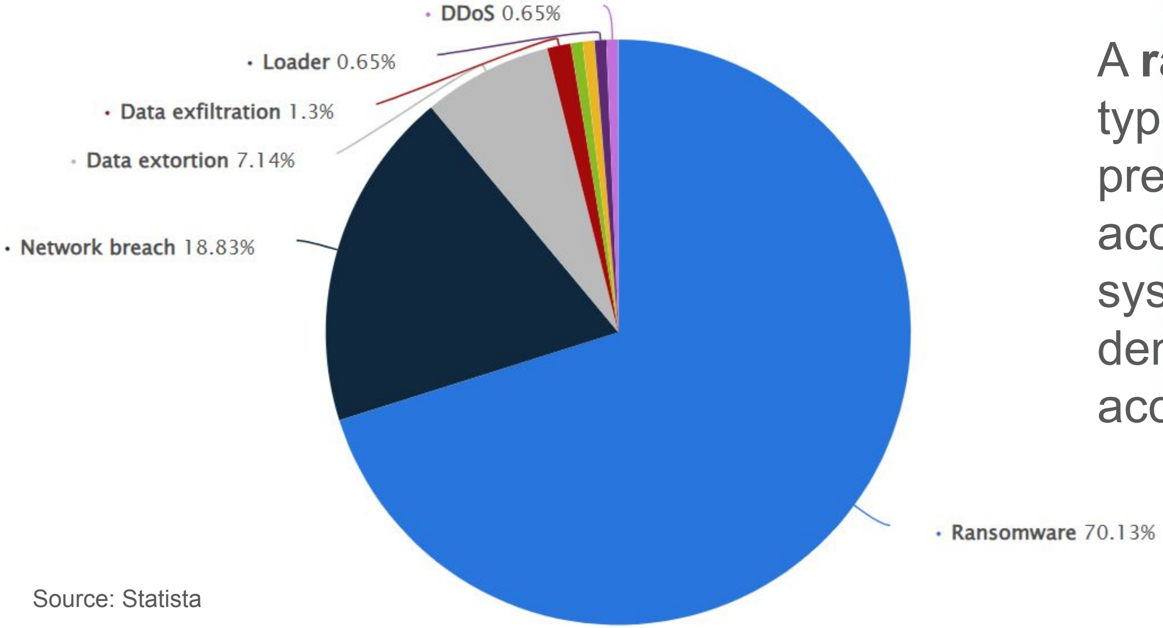
The hacking of Change Healthcare, a sizable unit of UnitedHealth Group, caused financial chaos that affected a broad spectrum ranging from large hospitals to single-doctor practices.

NEARLY THREE WEEKS SINCE ASCENSION RANSOMWARE ATTACK
WORKERS CALL THIS 'LIFE OR DEATH' SITUATION
kxan
85°
6:15


MedStar Georgetown
University Hospital
HACKERS PARALYZED HOSPITAL CHAIN
NBC NEWS
This is a Tobacco-Free Campus

DEVELOPING STORY
CBS NEWS CHICAGO
SYSTEMS STILL OFFLINE AFTER CYBERATTACK
LURIE CHILDREN'S HOSPITAL
36°
HEADLINES
SPITAL CONTINUES FOLLOWING CYBER SECURITY ATTACK
Ann & Robert H. Lurie Children's Hospital of Chicago

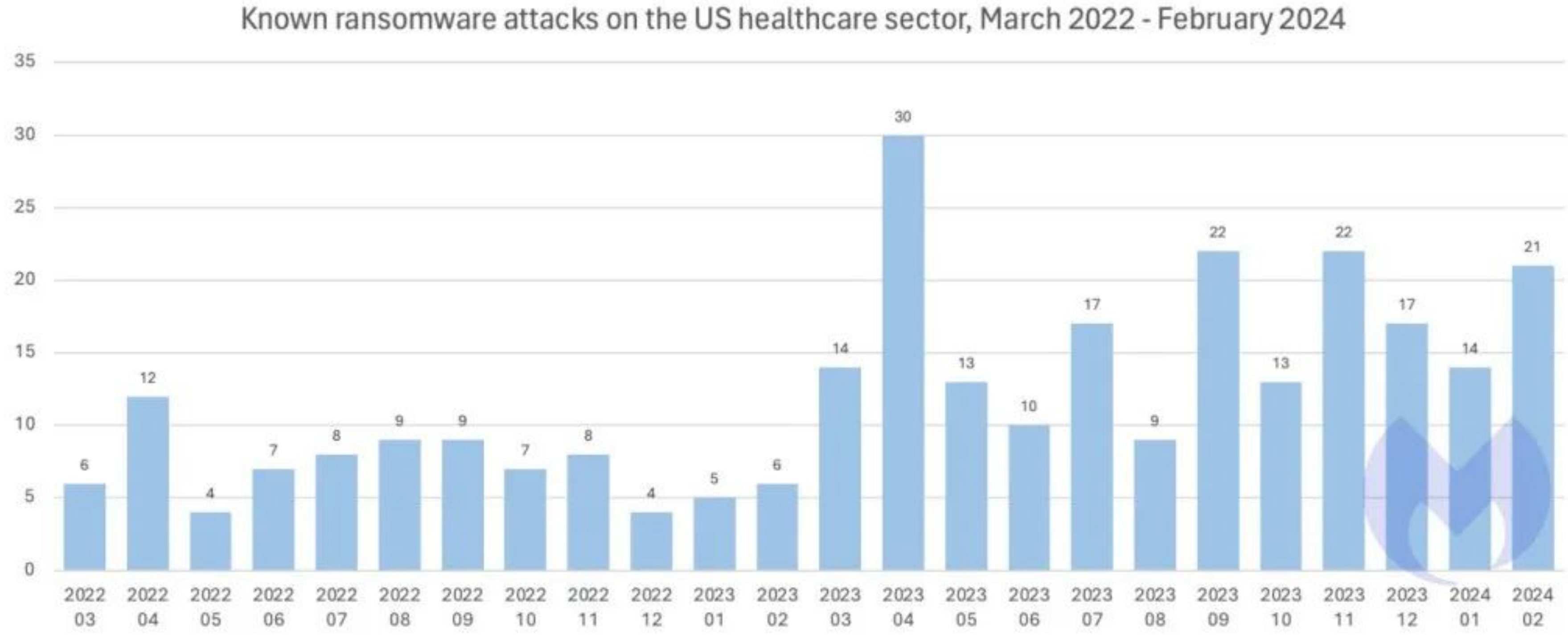
Distribution of detected Cyber Attacks Worldwide in 2023, by Type



Source: Statista

A **ransomware** attack is a type of malware attack that prevents a victim from accessing their files, systems, or networks and demands payment to regain access.

Ransomware attacks have been on the rise in recent years.



In 2023

There were 2,365 cyberattacks in 2023, with 343,338,964 victims.

72% increase in data breaches since 2021, which held the previous all-time record

Around the world, a data breach cost $4.88 million on average in 2024.

Email is the most common vector for malware, with around 35% of malware delivered via email in 2023.

Ninety-four percent of organizations have reported email security incidents.

Business email compromises accounted for over $2.9 billion in losses in 2023.

The average cost of a data breach in the healthcare industry is $9.77 million.

The Healthcare and Public Health (HPH) Sector

With its focus on caring for people, the HPH sector touches each of our lives in powerful ways.

Today, much of the work the HPH sector carries out is based in the digital world, leveraging technology to store patient and medical information, carrying out medical procedures, communicating with patients, and more.

Any disruptions to the HPH digital ecosystem can impact patient safety, create openings for identity theft, and expose intellectual property among other damaging effects.

What is the MIT Cybersecurity Clinic?

We are a group of MIT faculty, students, and researchers helping public agencies defend themselves against cyber attacks by using an approach called Defensive Social Engineering.

We partner with cities, towns and hospitals, particularly in New England, to help them reduce their vulnerability to cyberattacks.

We believe that having an assessment of the status-quo is the first step in figuring out a plan of action that will prevent unwanted incidents.

We work directly with public agencies or elected officials to assess their vulnerabilities and suggest low-cost improvements they can make.

How do conduct the Assessment?

The Clinic provides an opportunity for students to become certified in methods of assessing the vulnerability of public agencies (particularly agencies that manage critical urban infrastructure) and hospitals to the risk of cyber attack.

Certified students will work in teams of 3 or 4 with client agencies and hospitals in various cities and towns around the United States.

Through interactions with client agencies and hospitals, and short on-site visits, student teams will prepare Vulnerability Assessments that client agencies and hospitals can use to secure the technical assistance and financial support they need to manage the risks of cyber attack they are facing.

Defensive Social Engineering

Defensive Social Engineering (DSE) can provide tools to combat the things that occur during the early stages of an attack where technological solutions are less effective. This is especially true in the case of urban cyber terrorism where attackers spend considerable upfront time preparing.

Vulnerability Assessment Framework

We have created a framework based on the NIST Cybersecurity Framework and with the consultation of cybersecurity experts, specifically to aid public institutions and hospitals.

- Pre-Attack
  - Responsibilities and Collaboration
  - Resources
  - Technology and Systems Management
  - Incident Response Planning
- During Attack
  - Coordination and Plan Execution
- Post Attack
  - Incident Review and Plan Refinement

How do we protect privacy?

We DO NOT collect individuals' medical records or any other individually identifiable health information.

We DO NOT collect employee salary or financial information.

The work product is confidential and reserved only for your own use.

What value does it have for your organization?

Your organization will be served by a team of trained student assessors under faculty supervision at no charge to you.

Quality of reporting that summarizes both positive information security achievements, and areas for future improvement with pointed recommendations

An assessment that leaders can use to communicate a 'case for enhancement,' further focus, or investment.

Working with an experienced team that has served over 20 municipalities and hospitals and has certified over 400 students.

Why should hospitals undergo our assessment?

Cyberattacks impede hospital operations and place the health and well-being of patients at risk, and have long-term detrimental effects on the reputation and revenue of hospitals and health facilities.

Personally identifiable information (PII) and protected health information (PHI) are handled by almost every department in a hospital, in one or more health information systems. It is not possible to restore privacy or to reverse psychosocial harm when private data is compromised.

Better assess risks relating to the **Internet of Medical Things**, the collection of medical devices and applications that connect to healthcare information technology systems through online computer networks.

Partner Organization Testimonials

“The clinic reminded us of things we know are lacking (policies) as well as things we are not aware of.”

“The Assessment made recommendations regarding job descriptions and physical security that we have taken steps to immediately address.”

“More in depth than I thought we were going to see as far as reaching out to us regarding inventory, as far as software, hardware. Nobody's ever asked us for that which is which is kind of nice and the interviews were more in depth from what we would normally see from a kind of a third party vendor.”

Common Q&A

What is the exercise and output?

A cybersecurity assessment culminating in a short report that includes insights and recommendations.

How is it done?

Information collection is done via questionnaire and interviews. We can work in-person or remotely – whichever you prefer. Our process respects privacy and confidentiality as mandated by Health Insurance Portability and Accountability Act (HIPAA).

What is the time commitment?

We engage several roles to span infosec domains, but each interviewee would typically spend 1.5-3 hours end-to-end over the period.

Contacts

Larry Susskind
susskind@mit.edu

Jungwoo Chun
jwchun@mit.edu

cyberclinic@mit.edu