American Hospital Association®

Nebraska Hospital Association

Cybersecurity and Risk Update

American Hospital Association™
Advancing Health in America
Cybersecurity and Risk Advisory Services

Presented by:

John Riggi, Senior Advisor for Cybersecurity and Risk

Jeremy Witmer, FBI Special Agent

2/28/2020

American Hospital Association™
Advancing Health in America

AHA CENTER FOR HEALTH INNOVATION

Agenda

- Cyber Threat Landscape
- Ransomware
- Foreign Threats to Medical Research and Intellectual Property
- Questions and Contact Information

The Cyber Threat Landscape

Business E-mail Compromise: From June 2016 to July 2019 the FBI received reports of 166,347 incidents globally, with an exposed loss of **$26 Billion**. In 2019, 23, 775 Complaints received with $1.7 Billion in losses. **Contact your bank and the FBI immediately** at **www.ic3.gov**, ***local FBI office*** **or FBI CyWatch 855-292-3937**. ***79 % recovery rate in 2019 if reported within first 24 – 72 hours***

Verbal payment authentication procedures, *Cyber insurance, BAA, MFA !*

Computer Intrusions: (Foreign Based External Hacking) accounts for **88% of all records breached, *32m records*,** in first half of 2019, **approx. 41 million for 2019.** The average healthcare breach cost is ~3x all industry average or ***$10 + million*** . Average time to identify and contain an attack in healthcare is ***329 days.*** ***Incident Response Team****, Cyber Exercises, Cyber insurance,* ***VRM***

Ransomware + Data Extortion: Recent attacks are more targeted, sophisticated, combined with data extortion and costly as ransom demands are increasing. Email phishing campaigns, remote desktop protocol (RDP) vulnerabilities and software vulnerabilities. ***Backups being targeted***.

Medical device vulnerabilities, incident response plan, cyber insurance, ***backup security and redundancy****, and incident response plan!*

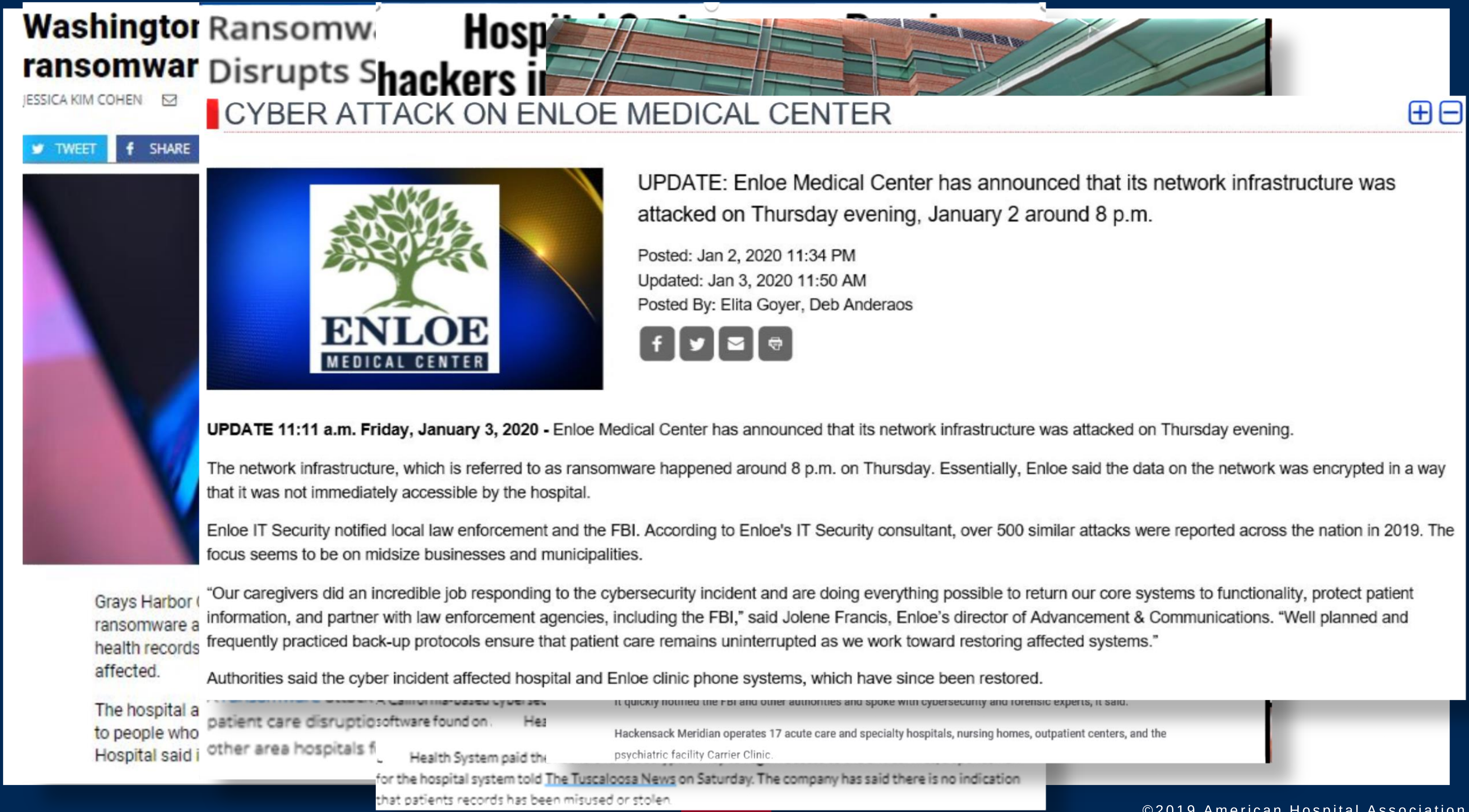
Sources: FBI 2019 Internet Crime Report (2/13/2020) Verizon 2019 Data Breach Report 5/8/2019; 2019 Mid Year Breach Barometer – Protenus 7/31/2019; 2019 Cost of a Data Breach Study: 7/24/2019 US, sponsored by IBM Independently conducted by Ponemon Institute LLC. FBI High Impact Ransomware Report 10/2/2019 I-10022019-PSA

©2019 American Hospital Association

“A ransomware attack on a hospital, is a not just an economic crime, it’s a crime that directly threatens public health and safety …and it should be prioritized, pursued and prosecuted as such ”

John Riggi, AHA Senior for Cybersecurity and Risk

©2019 American Hospital Association



Washingtor

ransomwar

JESSICA KIM COHEN

Ransomw

Disrupts S

Hosp

hackers i

CYBER ATTACK ON ENLOE MEDICAL CENTER

UPDATE: Enloe Medical Center has announced that its network infrastructure was attacked on Thursday evening, January 2 around 8 p.m.

Posted: Jan 2, 2020 11:34 PM
Updated: Jan 3, 2020 11:50 AM
Posted By: Elita Goyer, Deb Anderaos

UPDATE 11:11 a.m. Friday, January 3, 2020 - Enloe Medical Center has announced that its network infrastructure was attacked on Thursday evening.

The network infrastructure, which is referred to as ransomware happened around 8 p.m. on Thursday. Essentially, Enloe said the data on the network was encrypted in a way that it was not immediately accessible by the hospital.

Enloe IT Security notified local law enforcement and the FBI. According to Enloe's IT Security consultant, over 500 similar attacks were reported across the nation in 2019. The focus seems to be on midsize businesses and municipalities.

“Our caregivers did an incredible job responding to the cybersecurity incident and are doing everything possible to return our core systems to functionality, protect patient information, and partner with law enforcement agencies, including the FBI,” said Jolene Francis, Enloe’s director of Advancement & Communications. “Well planned and frequently practiced back-up protocols ensure that patient care remains uninterrupted as we work toward restoring affected systems.”

Authorities said the cyber incident affected hospital and Enloe clinic phone systems, which have since been restored.

Grays Harbor
ransomware a
health records
affected.

The hospital a
to people who
Hospital said i

A California-based cybersec
patient care disruptio software found on Hea
other area hospitals f

It quickly notified the FBI and other authorities and spoke with cybersecurity and forensic experts, it said.

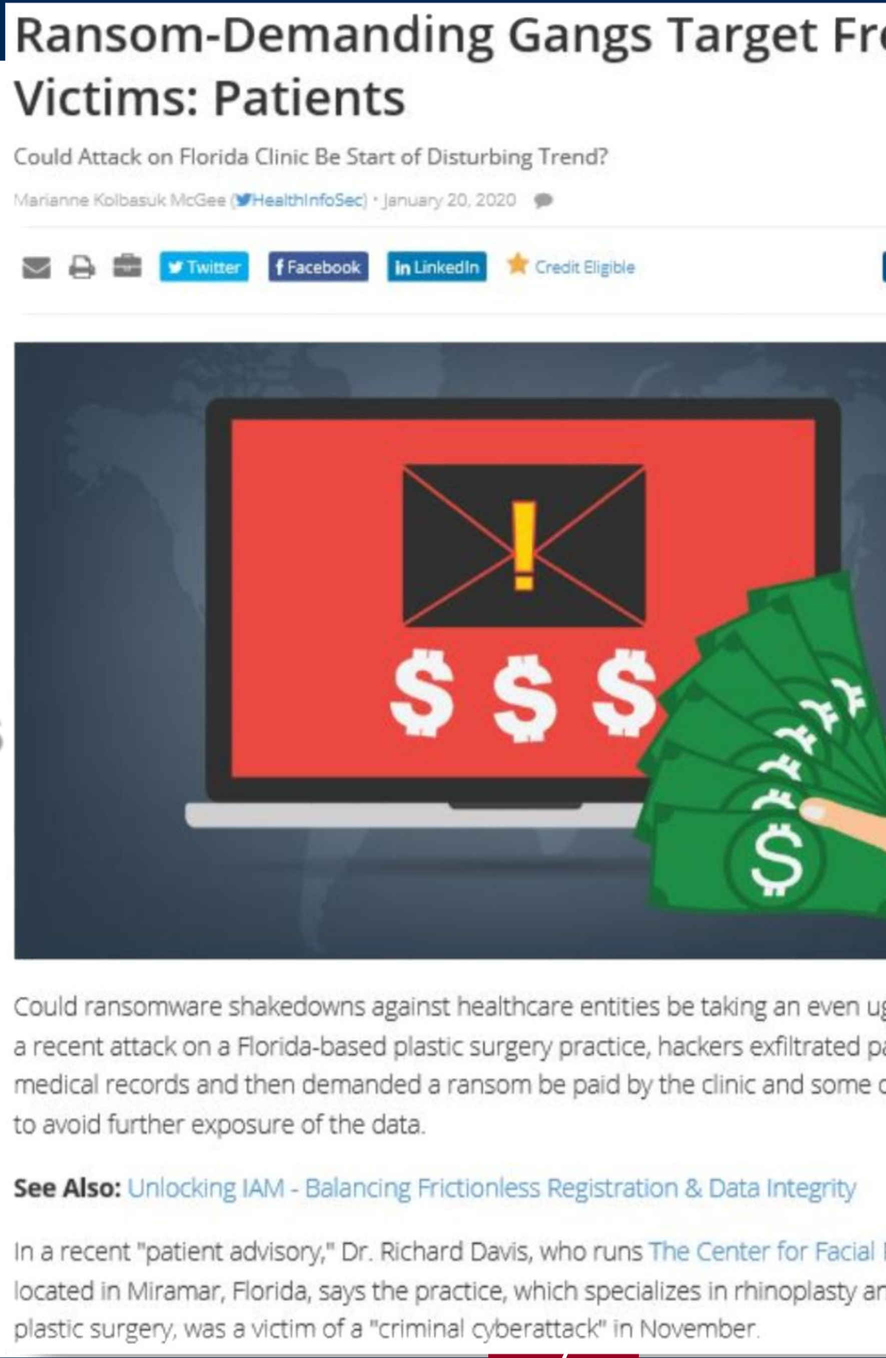
Hackensack Meridian operates 17 acute care and specialty hospitals, nursing homes, outpatient centers, and the psychiatric facility Carrier Clinic.

Health System paid the
for the hospital system told The Tuscaloosa News on Saturday. The company has said there is no indication that patients records has been misused or stolen.

©2019 American Hospital Association

A Disturbing Trend:
Data Extortion

Forcing Hospitals to Make Tough Choices



Ransom-Demanding Gangs Target Fresh Victims: Patients

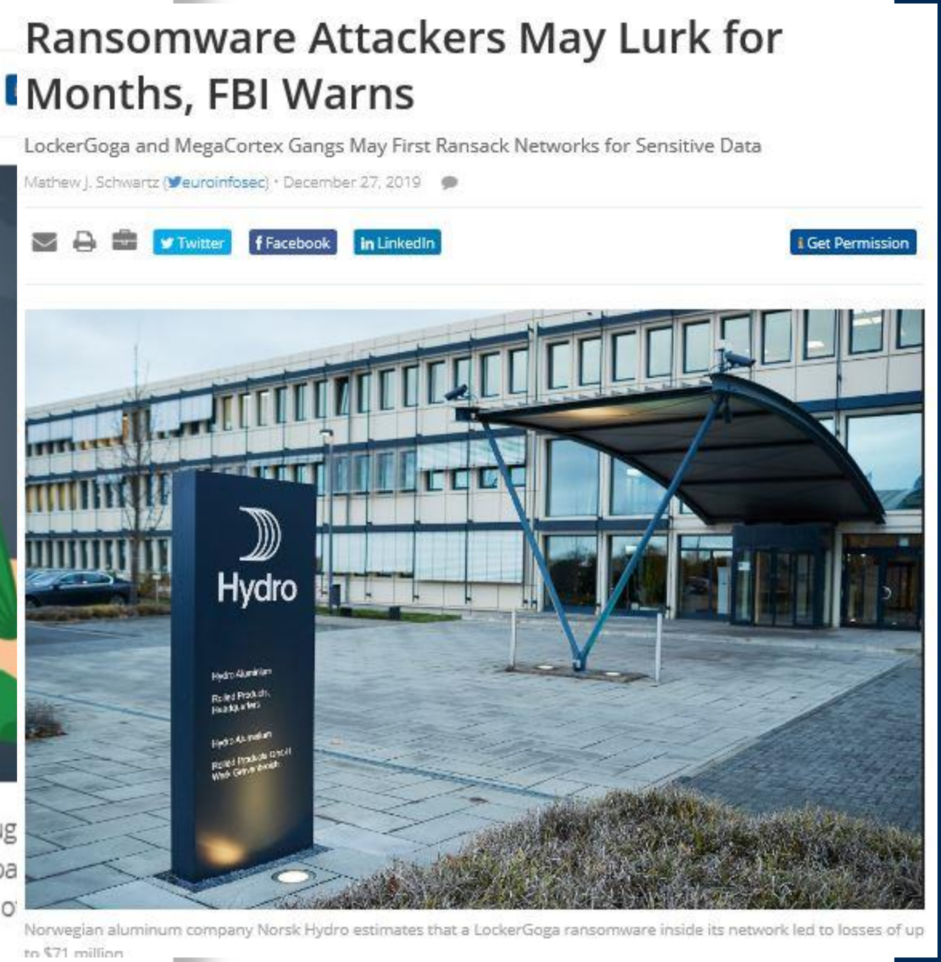
Could Attack on Florida Clinic Be Start of Disturbing Trend?

Marianne Kolbasuk McGee (HealthInfoSec) • January 20, 2020

Could ransomware shakedowns against healthcare entities be taking an even ug
a recent attack on a Florida-based plastic surgery practice, hackers exfiltrated pa
medical records and then demanded a ransom be paid by the clinic and some o
to avoid further exposure of the data.

See Also: Unlocking IAM - Balancing Frictionless Registration & Data Integrity

In a recent "patient advisory," Dr. Richard Davis, who runs The Center for Facial Restoration located in Miramar, Florida, says the practice, which specializes in rhinoplasty and other facial plastic surgery, was a victim of a "criminal cyberattack" in November.

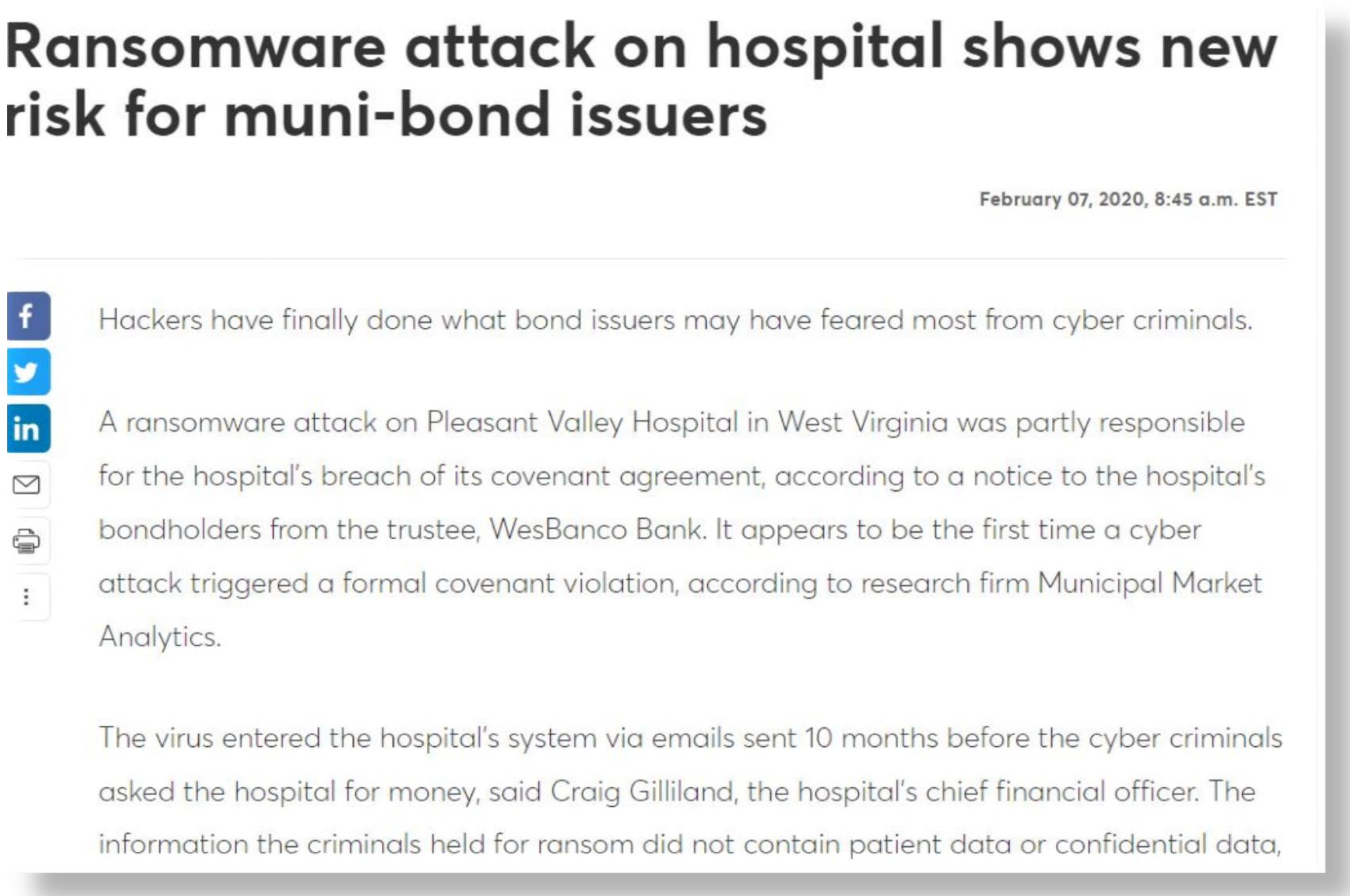


Ransomware Attackers May Lurk for Months, FBI Warns

LockerGoga and MegaCortex Gangs May First Ransack Networks for Sensitive Data

Mathew J. Schwartz (euroinfosec) • December 27, 2019

Norwegian aluminum company Norsk Hydro estimates that a LockerGoga ransomware inside its network led to losses of up to $71 million



Ransomware attack on hospital shows new risk for muni-bond issuers

February 07, 2020, 8:45 a.m. EST

Hackers have finally done what bond issuers may have feared most from cyber criminals.

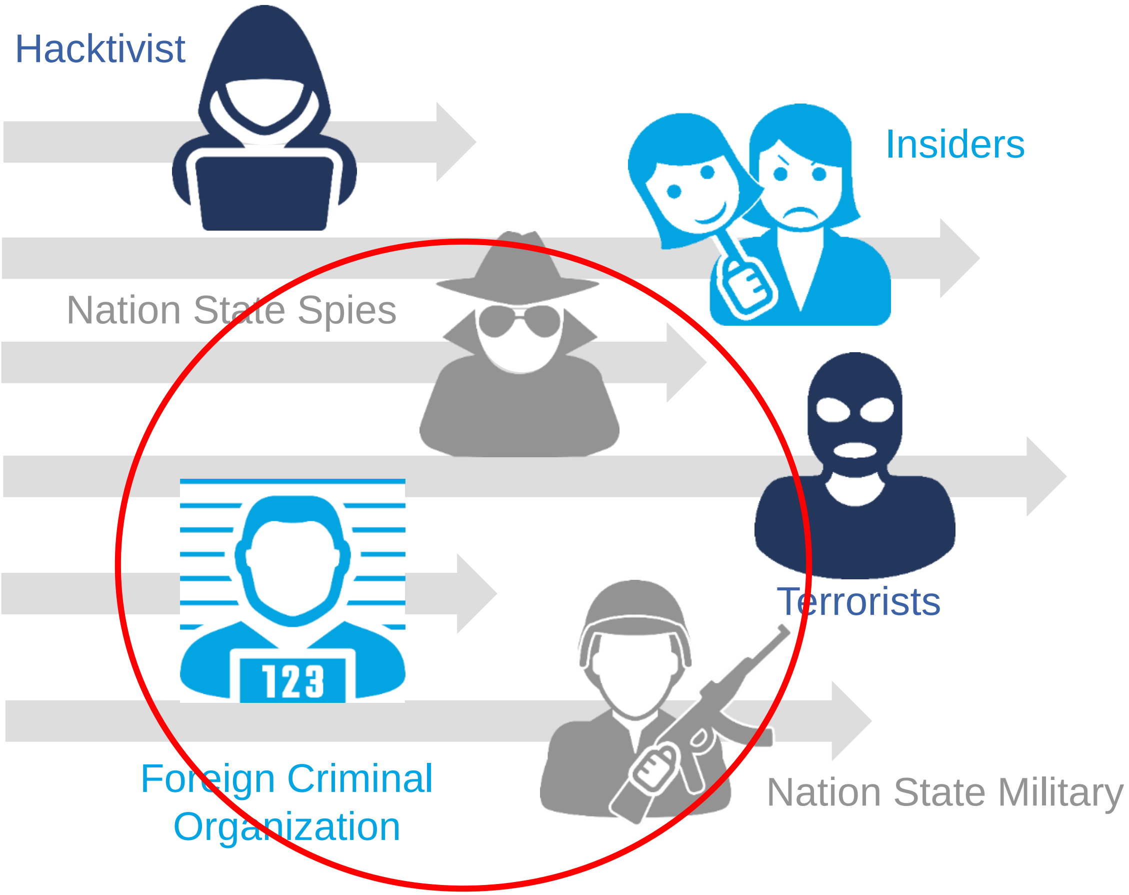
A ransomware attack on Pleasant Valley Hospital in West Virginia was partly responsible for the hospital's breach of its covenant agreement, according to a notice to the hospital's bondholders from the trustee, WesBanco Bank. It appears to be the first time a cyber attack triggered a formal covenant violation, according to research firm Municipal Market Analytics.

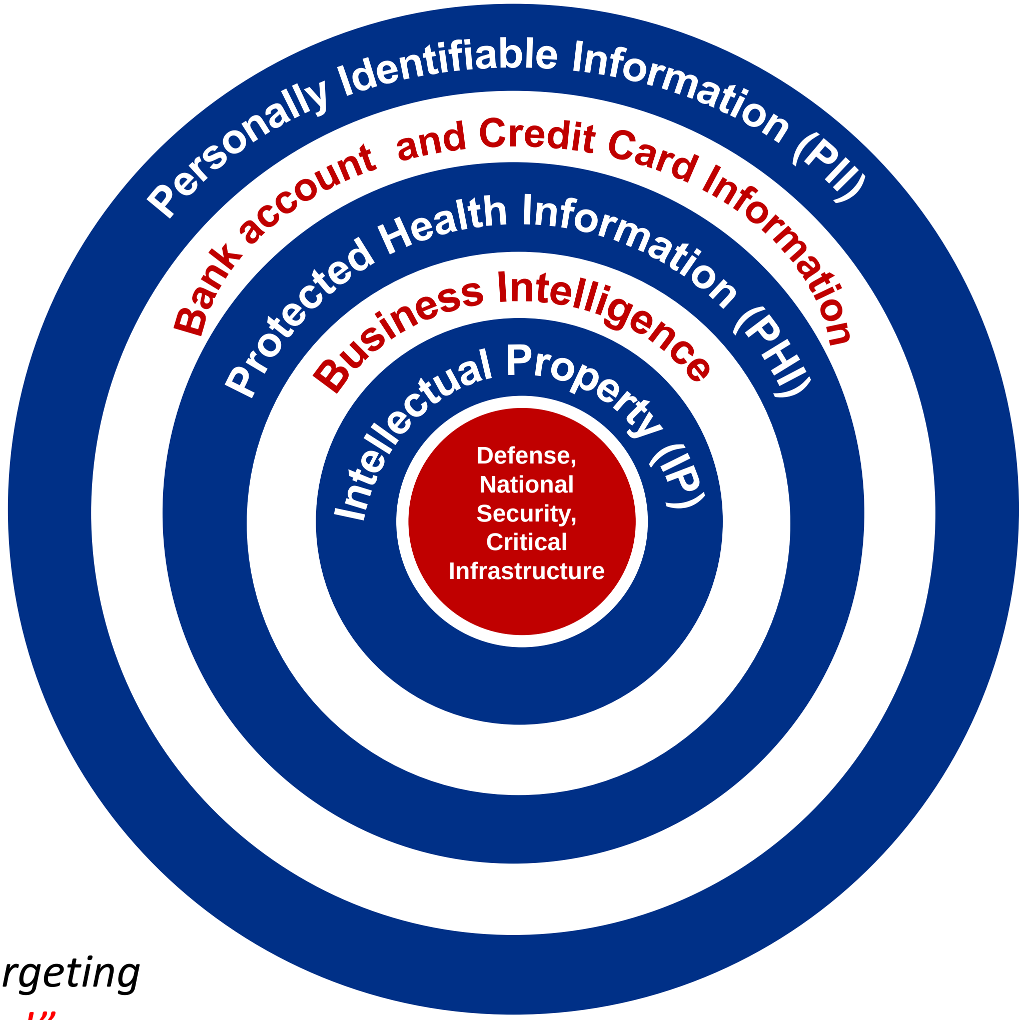
The virus entered the hospital's system via emails sent 10 months before the cyber criminals asked the hospital for money, said Craig Gilliland, the hospital's chief financial officer. The information the criminals held for ransom did not contain patient data or confidential data,

©2019 American Hospital Association

Data Rich Environment = Target Rich Environment

Targeted Data

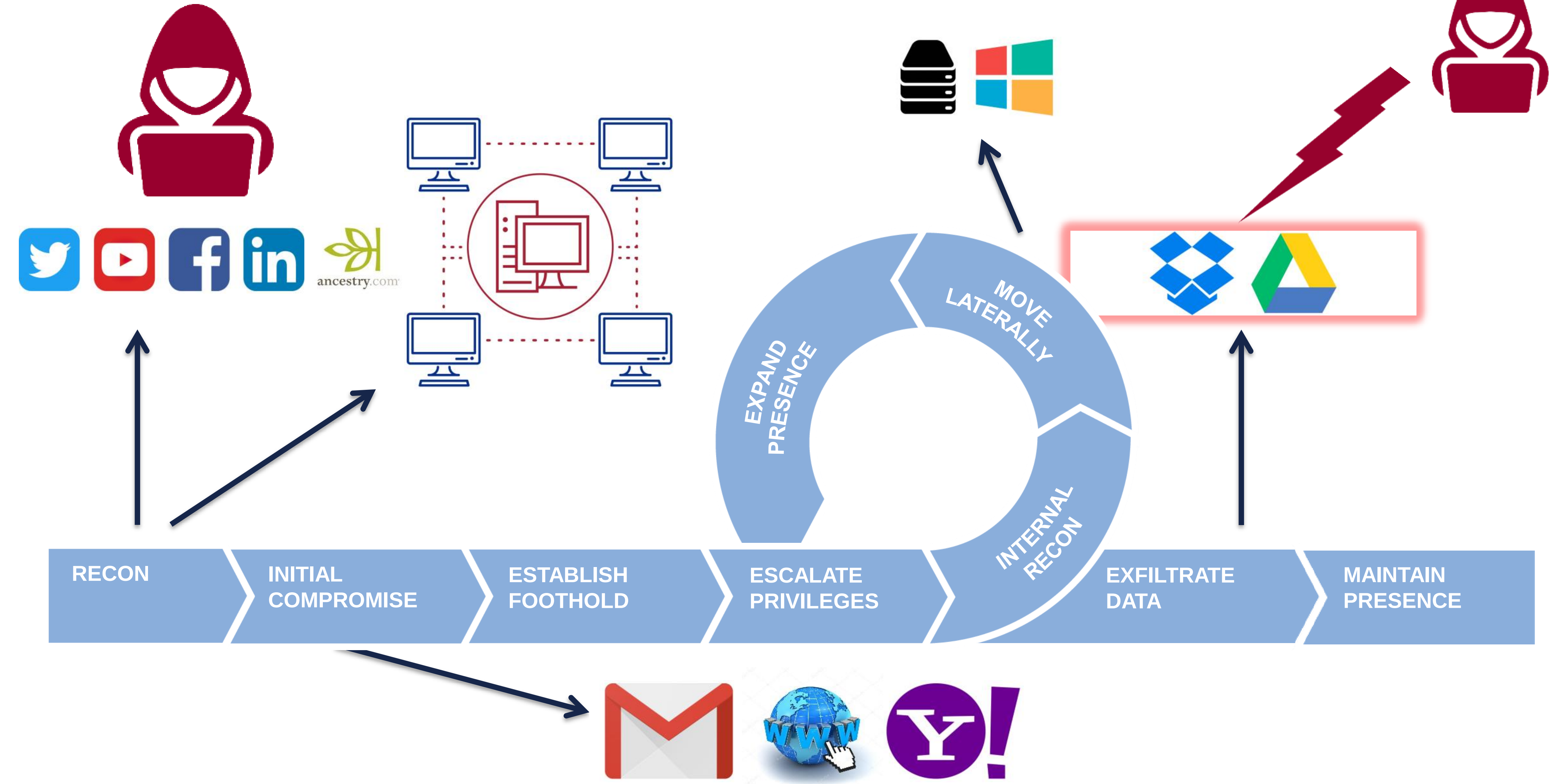



Personally Identifiable Information (PII)
Bank account and Credit Card Information
Protected Health Information (PHI)
Business Intelligence
Intellectual Property (IP)
Defense, National Security, Critical Infrastructure

Nation states, criminals, insiders and hacktivists are aggressively targeting healthcare providers to steal their valuable data. ***"One stop hacking!"***

©2019 American Hospital Association

Anatomy of a Hack

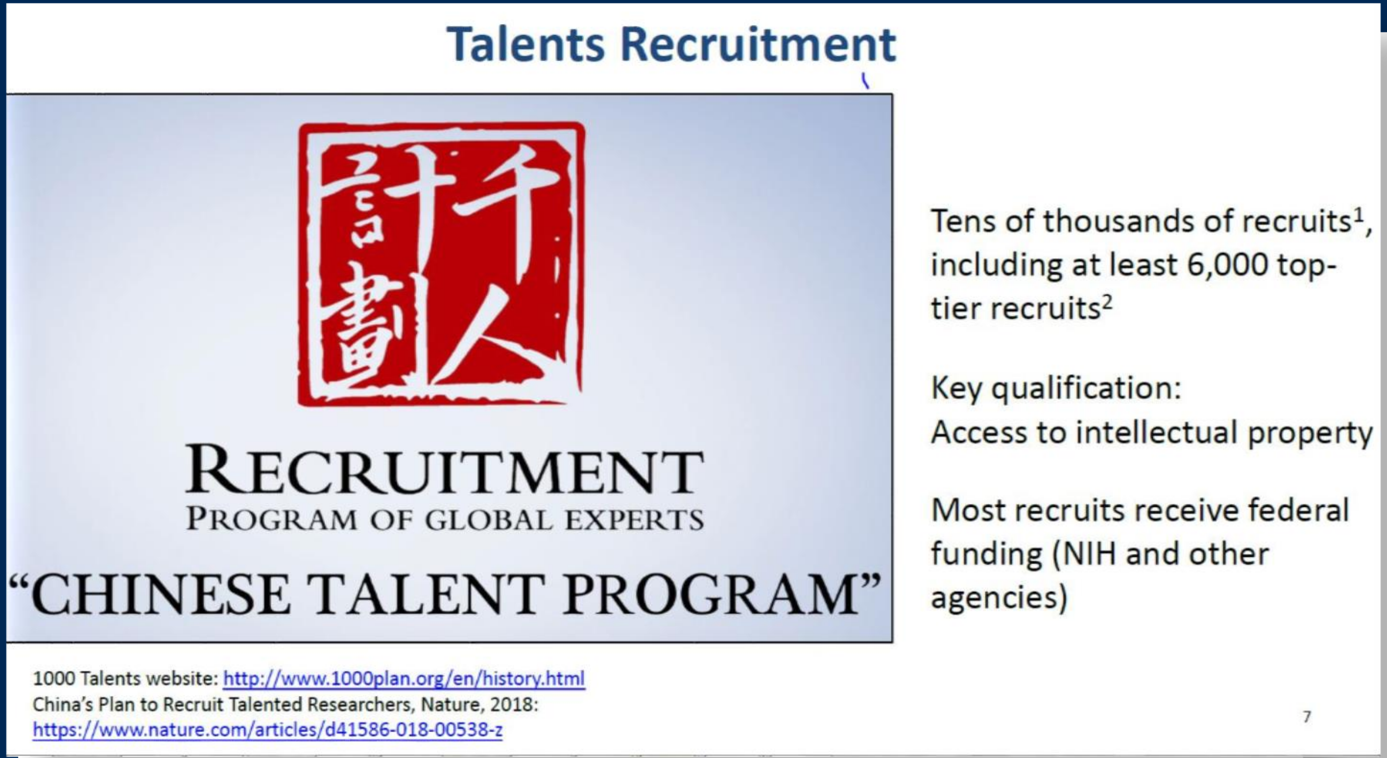


©2019 American Hospital Association

Foreign Threats to Intellectual Property

Medical Research and Innovation under attack

©2019 American Hospital Association



Talents Recruitment

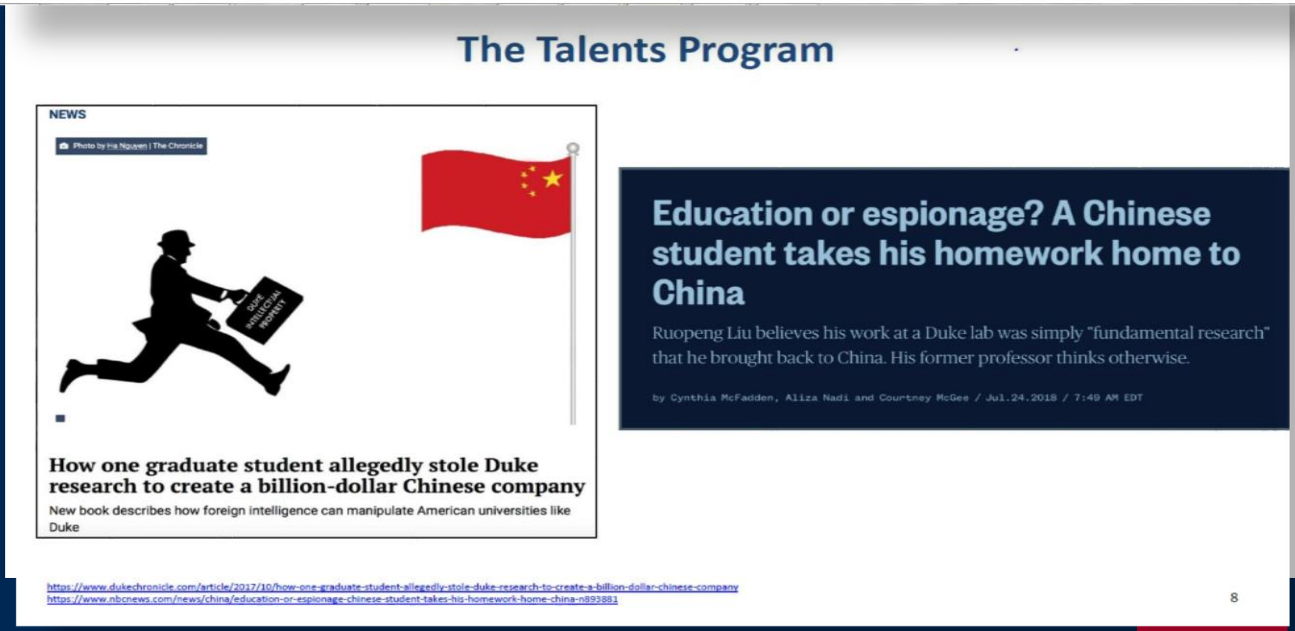
Tens of thousands of recruits[1], including at least 6,000 top-tier recruits[2]

Key qualification:
Access to intellectual property

Most recruits receive federal funding (NIH and other agencies)

1000 Talents website: http://www.1000plan.org/en/history.html
China's Plan to Recruit Talented Researchers, Nature, 2018: https://www.nature.com/articles/d41586-018-00538-z

7



The Talents Program

NEWS

Photo by Ha Nguyen | The Chronicle
DUKE INTELLECTUAL PROPERTY

How one graduate student allegedly stole Duke research to create a billion-dollar Chinese company

New book describes how foreign intelligence can manipulate American universities like Duke

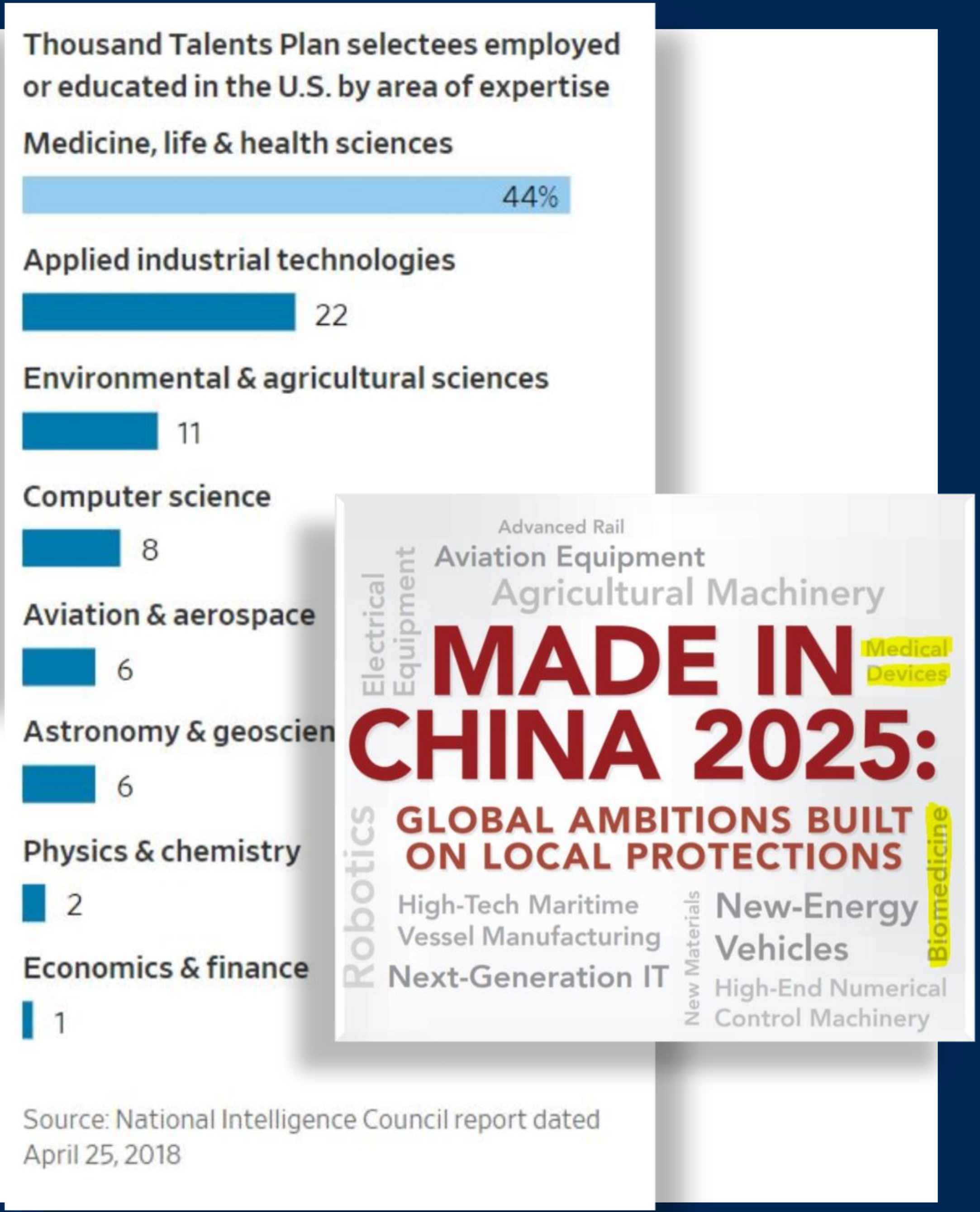
Education or espionage? A Chinese student takes his homework home to China

Ruopeng Liu believes his work at a Duke lab was simply "fundamental research" that he brought back to China. His former professor thinks otherwise.

by Cynthia McFadden, Aliza Nadi and Courtney McGee / Jul.24.2018 / 7:49 AM EDT

https://www.dukechronicle.com/article/2017/10/how-one-graduate-student-allegedly-stole-duke-research-to-create-a-billion-dollar-chinese-company
https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881

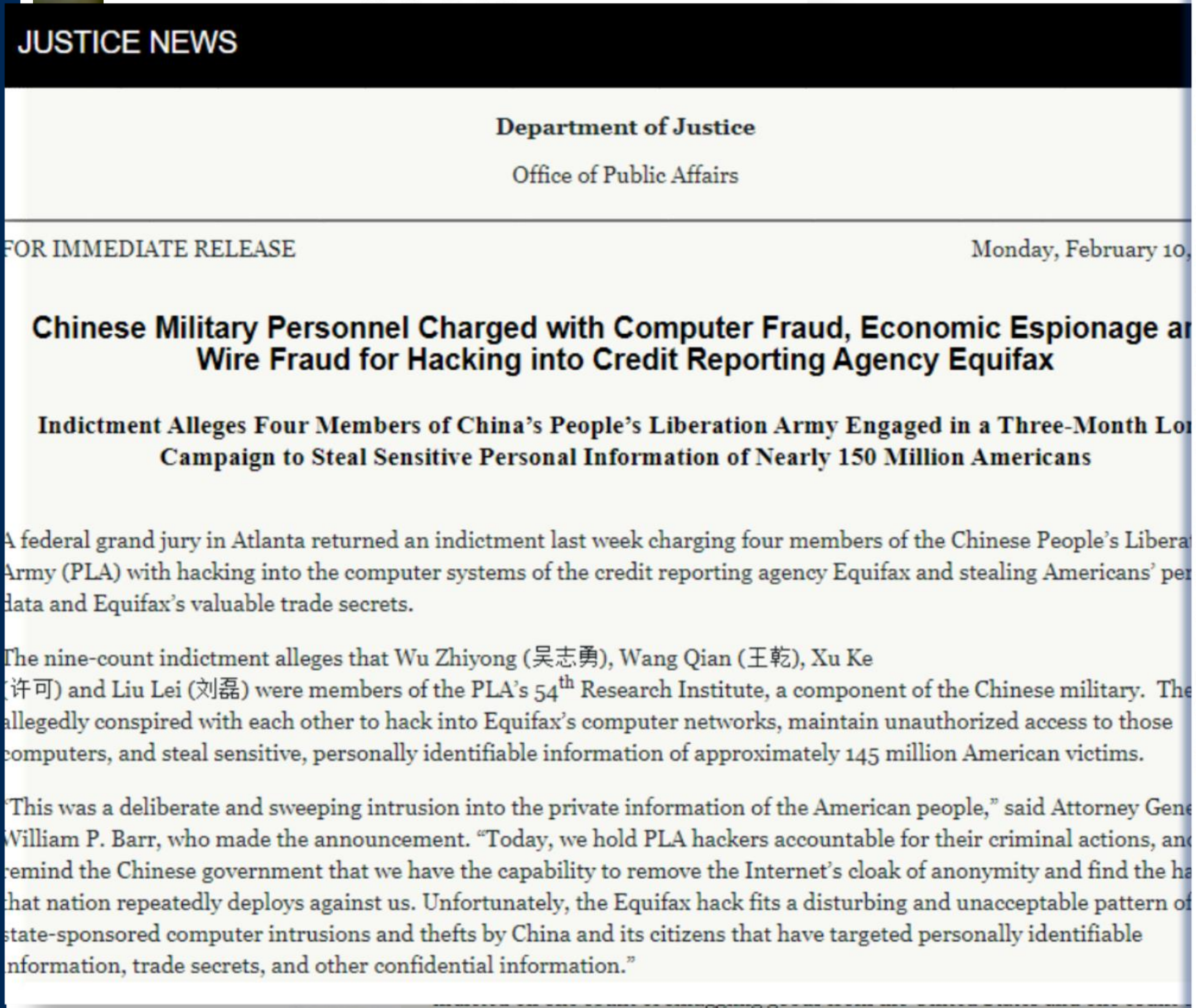
8



Thousand Talents Plan selectees employed or educated in the U.S. by area of expertise

Source: National Intelligence Council report dated April 25, 2018

©2019 American Hospital Association



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Monday, February 10,

Chinese Military Personnel Charged with Computer Fraud, Economic Espionage ar Wire Fraud for Hacking into Credit Reporting Agency Equifax

Indictment Alleges Four Members of China's People's Liberation Army Engaged in a Three-Month Lo Campaign to Steal Sensitive Personal Information of Nearly 150 Million Americans

A federal grand jury in Atlanta returned an indictment last week charging four members of the Chinese People's Libera Army (PLA) with hacking into the computer systems of the credit reporting agency Equifax and stealing Americans' per data and Equifax's valuable trade secrets.

The nine-count indictment alleges that Wu Zhiyong (吴志勇), Wang Qian (王乾), Xu Ke (许可) and Liu Lei (刘磊) were members of the PLA's 54th Research Institute, a component of the Chinese military. The allegedly conspired with each other to hack into Equifax's computer networks, maintain unauthorized access to those computers, and steal sensitive, personally identifiable information of approximately 145 million American victims.

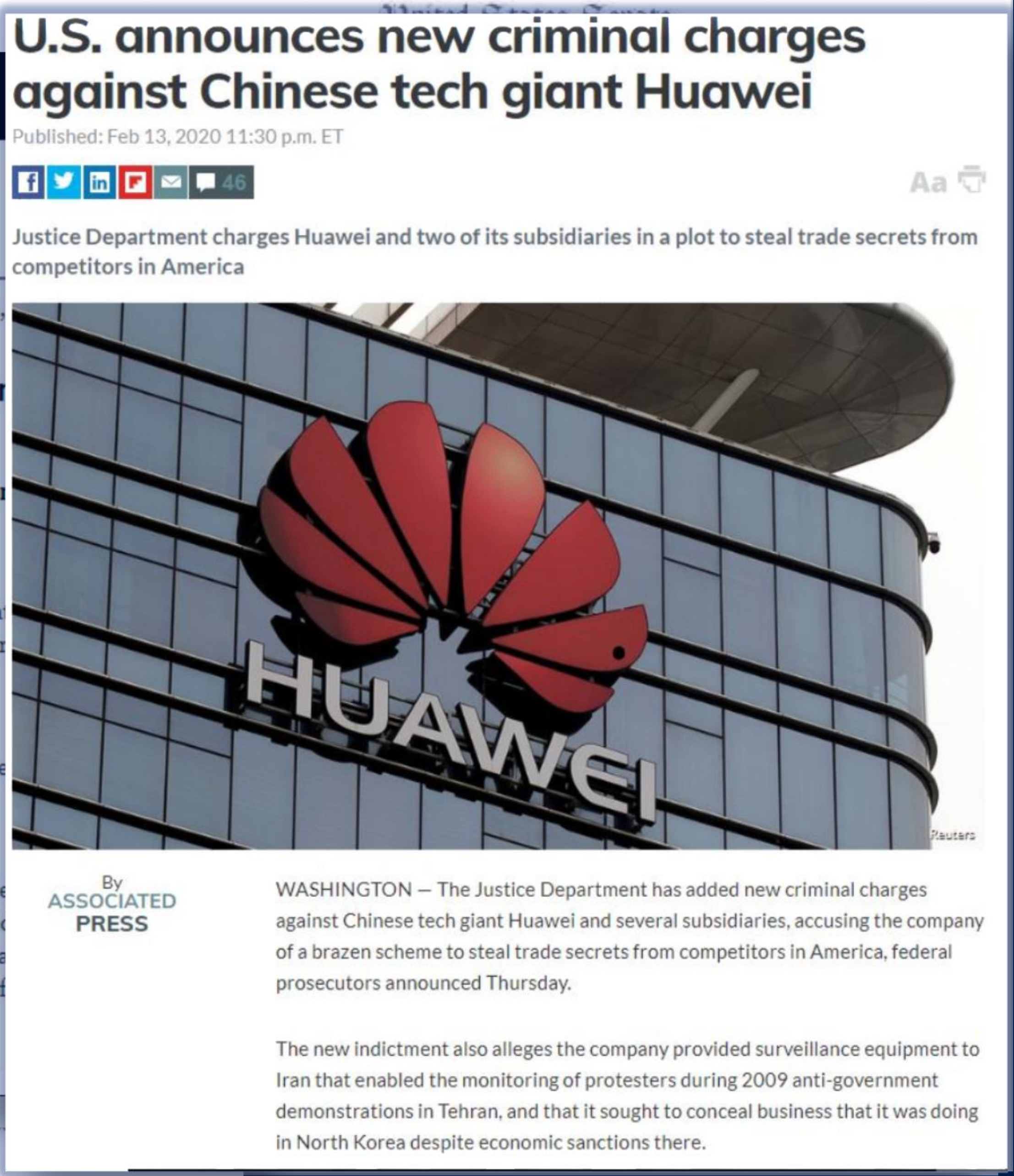
"This was a deliberate and sweeping intrusion into the private information of the American people," said Attorney Gene William P. Barr, who made the announcement. "Today, we hold PLA hackers accountable for their criminal actions, an remind the Chinese government that we have the capability to remove the Internet's cloak of anonymity and find the ha that nation repeatedly deploys against us. Unfortunately, the Equifax hack fits a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."

statements. He has been detained since Dec. 30, 2019.

Jose Oliva a

institutions.

FLORIDA HOUSE OF REPRESENTATIVES



U.S. announces new criminal charges against Chinese tech giant Huawei

Published: Feb 13, 2020 11:30 p.m. ET

Justice Department charges Huawei and two of its subsidiaries in a plot to steal trade secrets from competitors in America

By ASSOCIATED PRESS

WASHINGTON — The Justice Department has added new criminal charges against Chinese tech giant Huawei and several subsidiaries, accusing the company of a brazen scheme to steal trade secrets from competitors in America, federal prosecutors announced Thursday.

The new indictment also alleges the company provided surveillance equipment to Iran that enabled the monitoring of protesters during 2009 anti-government demonstrations in Tehran, and that it sought to conceal business that it was doing in North Korea despite economic sanctions there.

©2019 American Hospital Association

John Riggi, Strategic Advisor for Cybersecurity and Risk

Advisory services uniquely informed by:

- Extensive and varied FBI and CIA experience
- Trusted and confidential access to the nation’s hospital leaders
- Ongoing exchange with federal law enforcement, intelligence and regulatory agencies

jriggi@aha.org (O) 202-626-2272; (M) 24/7 202-640-9159

FBI Contact Information:

Special Agent Jeremy Witmer, jwitmer@fbi.gov

FBI Office, Omaha 402-575-2121,

FBI CyWatch 24/7 - 855-292-3937

www.ic3.gov

AHA Membership Includes:

American Hospital Association®

Cybersecurity and Risk Advisory Services

STRATEGIC CYBERSECURITY AND RISK ADVISORY SERVICES

HOSPITAL LEADERSHIP CYBERSECURITY EDUCATION AND AWARENESS

CYBER AND RISK INCIDENT RESPONSE STRATEGY AND ADVISORY SERVICES

LAW ENFORCEMENT AND NATIONAL SECURITY RELATIONS

Advancing Health in America