Hospital CEO forced to pay hackers in bitcoin now teaches others how to prepare for the worst

Berkeley Lovelace Jr. | Elizabeth Gurdus

Published 8:00 AM ET Sat, 7 April 2018 Updated 48 Mins Ago

CNBC.com

Source: Hancock Regional Hospital

Steve Long, president and CEO of Hancock Regional Hospital.

It was a late Thursday in January when hospital administrator Steve Long was notified that his computer systems had just been hijacked by an unidentified criminal group.

The hackers gave Long seven days to pay a ransom — or else.

It was at the height of flu season, and a winter snowstorm was moving through the Greenfield, Indiana, area where Hancock Regional Hospital is located. As president and CEO of Hancock Health, Long felt an obligation to make sure his patients were safe.

"We were very prepared. We understood that cyberattacks are common," Long told CNBC.

Unfortunately for Long, the criminals had obtained the login credentials of a vendor that provides hardware for one of the information systems used by the hospital, enabling the group to inject malware and encrypt the hospital's data.

Long was eventually forced to pay the hackers in cryptocurrency.

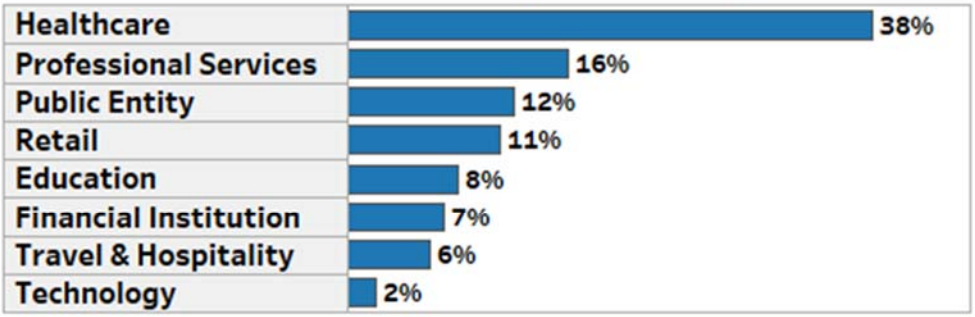
"We never had a choice in hindsight. It's part of a business model. There is a business model behind this," Long said. He now spends his free time traveling around the U.S. teaching other groups what he learned from the experience.

Over the past decade, the health-care field has had far more computer security incidents than any other industry, accounting for 38 percent of incidents versus 16 percent for professional services and 11 percent for retail, according to data from Chubb, the world's largest publicly traded property and casualty insurer.

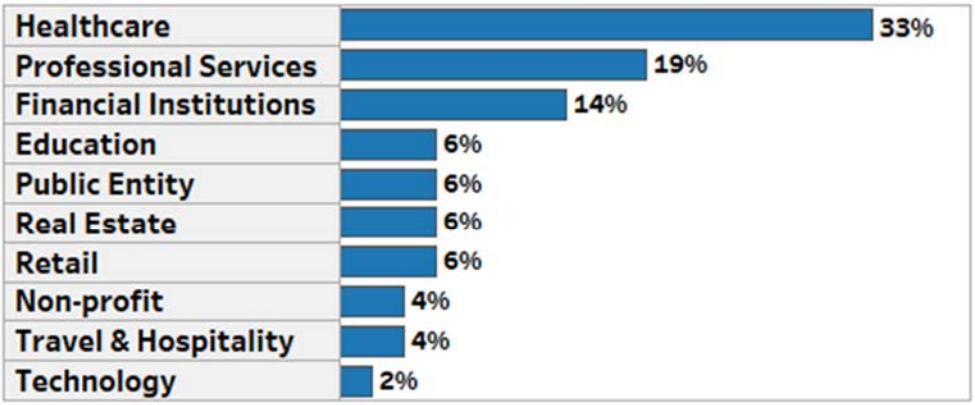
Cyber claims

CNBC
SOURCE: Chubb

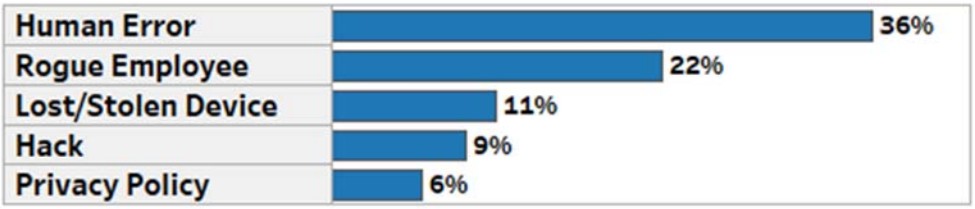
Cyber Incidents (2008-2018)



Ransomware incidents (2016-present)



Cyber triggers in healthcare (2008-2018)



Average cost per incident

Forensics	$231,457
Notification/Call Center	$98,037
Credit Monitoring	$46,412
Legal Costs	$39,036
PR/Crisis Response	$29,116
Total	$444,058

Chubb said personal health information is approximately 10 times more valuable on the black market than data a hacker could obtain from a retailer.

Unlike personal identifiable information —which might include a name, email address and password, credit card numbers or Social Security number — health information offers a wealth of additional data, including medical records. Health insurance ID numbers may also be tied to driver's license numbers or financial information, Chubb experts told CNBC.

They said personal health information hacks can also go on for years. A consumer can shut down her credit card quickly if it has been compromised; she can't cancel her Social Security number or birth date.

As a result, hackers can harvest patient data and hold it for "a larger score down the road," using it for years to open illicit bank accounts or steal additional information, said Mike Tanenbaum, executive vice president of Chubb's North America cyber practice.

The increasing hacks in health care come at a time when U.S. companies have fallen under scrutiny for how they manage consumer data, raising questions about how personal information should be used and protected. Last week, athletic retailer Under Armour told customers that its MyFitnessPal app was compromised, jeopardizing data from approximately 150 million users.

Social media giant Facebook has also came under fire over its privacy practices in the wake of revelations that Cambridge Analytica improperly gained access to data from some 87 million user profiles, then used it to target political ads.

The days following the Hancock attack and beyond

"By 10:30 that night we had shut down every single computer that we had and all our servers," Long recalled about the Thursday night in January. "By midnight we successfully shut off every computer in the organization and started from scratch. It's surreal."

By 4 a.m. on Friday, Long and his team had recruited Indianapolis-based cybersecurity firm Pondurance to identify the cause and scope of the attack and eradicate the imminent threat.

Pondurance co-founder Ron Pelletier said the first priority was to contain the intrusion and evaluate what was affected. Together with the FBI, which was called in to help pinpoint the origin of the attack, Pondurance experts determined that there was no easy way to erase the encrypted data from Hancock's system and replace it with clean data from the backup system.

Taking into consideration the flu outbreak and the snowstorm, Long made the executive decision to buy the decryption keys from the hackers. Late Friday night, Hancock bought the keys by transferring four bitcoin.

Bitcoin's was selling above $13,500 that day, bringing the estimated total Hancock paid to about $55,000.

"Criminal organizations now are treating this like a business," Pelletier said. "They're going to plan, they're going to make sure they understand how they're going to execute and then they're going to set out and see where they can execute."

Cybercriminals typically use the fourth quarter of the year to seek out "low-hanging fruit" and plan their attack, Pelletier said. Then, in the first quarter, particularly between February and April — a time Pelletier has come to refer to as "breach season" due to the uptick of cyber incidents — they put their plan into action.

"Hancock is one organization of many in this period that this happened to," Pelletier said.

While the investigation into Hancock's attack is ongoing, none of the network's patient data appears to have been stolen, which Pelletier said was an indication that this particular group saw ransomware as a more effective way of getting paid.

"If you think about the numbers of breaches that have occurred in general, [it's] millions and millions of records," Pelletier said. "The dark web becomes a supply and demand issue at some point — I can try to monetize PHI [personal health information] by selling it on the dark web, or I can probably make maybe less, but a more expedited payment if I do something like ransomware."

Source: Hancock Regional Hospital

Steve Long, president and CEO of Hancock Regional Hospital.

Since the attack, Long said he has held four or five talks with various health-care groups and IT organizations about some of the best ways to prepare. Long plans to hold four or so more talks over the summer. He said "patient safety and restoration" should guide everything a health organization does in such an event.

"You might do the thing all the people do. But whatever you think is good enough is not. It's worth [it] to get the best stuff out there," Long said. "What we have is the latest, greatest and most expensive, my [chief financial officer] tells me."

Pelletier said his firm prefers AI-enabled software to traditional or legacy antivirus systems because it requires less hands-on management. Traditional antivirus software often requires programming to be able to identify and stop specific threats. But if the system hasn't encountered a particular type of malware, it could fail.

"This next-generation antivirus, narrow AI-type programs, use a math model to be able to understand what it is a program is intending to do" so programmers don't have to anticipate unknown threats, Pelletier said. He also said it can work offline and doesn't have to be updated as frequently as legacy systems.

The best practices for protecting personal health data

Thomas Samson | AFP | Getty Images

In many cases, particularly in health care, cyberattacks "are not a matter of if, but when," said Pelletier.

According to Chubb, 58 percent of cyber incidents happen because of human error or a rogue employee acting out, which could lead to purposefully installed malware, stolen documents or other one-off breaches with potentially larger consequences.

"You can't rely on technology alone to be secure. It just won't work," Pelletier said. "Over time, technology can be circumvented because your adversary is a human being. You need a human to counter another human — thinking like a human would give you a better chance to provide a better and more effective defense."

Here are some of Pelletier's recommendations for how health-care networks and hospitals can best protect their systems from cyberthreats:

1. Set up multifactor authentication for everybody with access to the system. It should include something you know, like a password; something you are, like a biometric scan of a fingerprint; and something you have, like a randomly generated token from an application like Google Authenticator that is linked to your system.

2. Practice vulnerability management. Don't just run tools to scan your environment — actively look for things that could create a risk, like a part of the system that is open to the internet without good cause, and turn them off or make them private.

3. Vet your vendors. Always keep track of who has access to your systems and what they have access to. Vendors should have the minimum level of access necessary to do their jobs. Note how your vendors think about cybersecurity. Do they make sure to change their passwords over time? Do they use multifactor authentication?

4. Install AI-enabled software that can work offline, needs fewer updates and doesn't rely on manual programming to function correctly.

5. Enable some level of system logging so you can track what is done in the case of an attack and provide the best possible outcome in a forensic investigation

"Health care is making strides in terms of security maturity," Pelletier said. "The challenges they continue to face are that they need to make data available for other health-care organizations, other entities that need to use the data, and so there is a level of openness that still needs to be contained and secured."

"So I think health care's making strides, but it's taking some time for more organizations."

—CNBC's John Schoen contributed to this report.