

MANAGING THROUGH GETTING HACKED – INSIDE THE WILD 18 HOURS FROM FIRST INTRUSION THROUGH PAYING THEM OFF

Seth Jeremy Katz, MPH, RHIA, FAHIMA

Vice President of Revenue Cycle and HIM, University Health

This All Would've Been Gibberish Just A Few Years Ago..

Los Angeles hospital paid \$17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had **lost access** to its computer systems since 5 February after hackers installed a virus that encrypted their files

US hospital pays \$55,000 to hackers after ransomware attack

Hancock Health paid up despite having backups available.

Inside the New York hospital hackers took down for 6 weeks

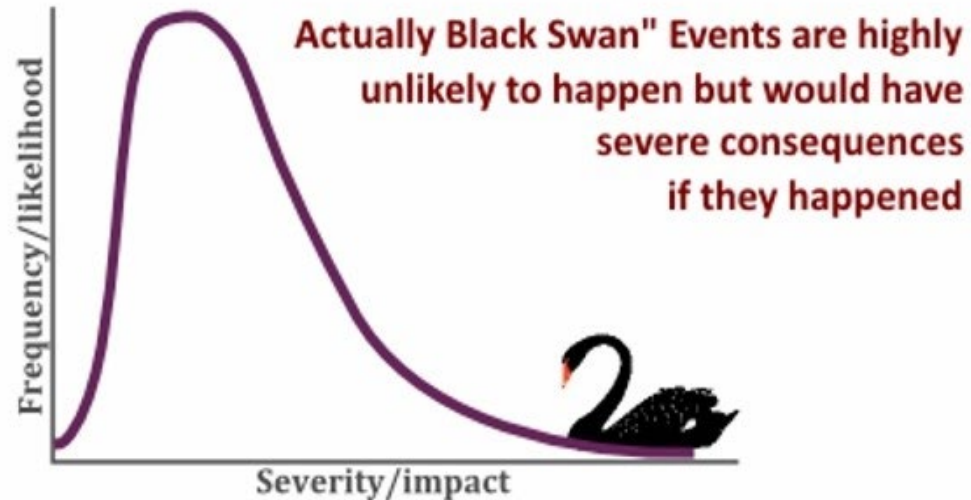
Pugh runs the medical center's emergency room. She was on duty the morning hackers sent a ransomware message demanding \$44,000 in the cyber currency bitcoin to unlock hospital data being held hostage.

Why Do Disasters Feel Like They Come Out of Nowhere?



“People hate to think about bad things
so they always underestimate their
likelihood.”

The Black Swan Event



Recognizing
'Black Swan'
Events

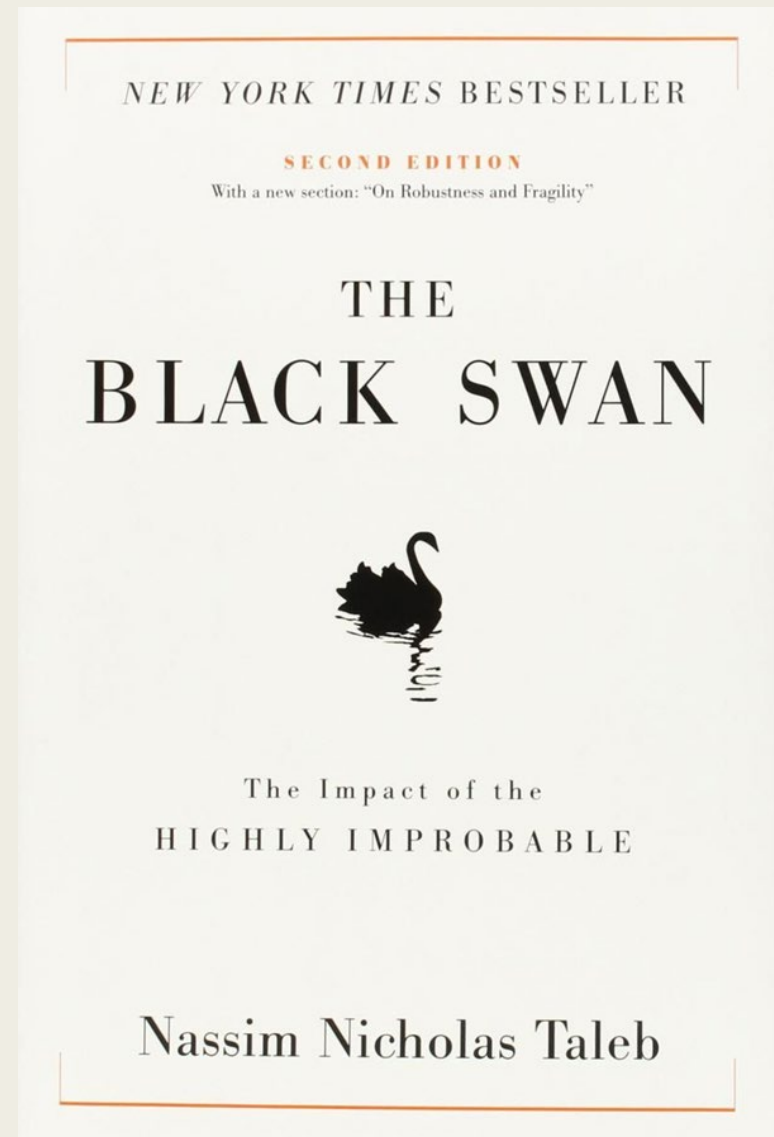
Black Swan Events

Criteria:

1. *Rare*
2. *Extreme (and likely immediate) impact*
3. *Retrospective predictability (though prospective predictability may not be possible)*

The idea of a 'black swan' being used as a metaphor for a disaster comes from the 16th century when there was a belief that no black swans existed

- *Past experience automatically predicts future behavior*
- *Impossible to prove; easy to disprove*



Notable Black Swan Events

See also:

- *Brexit*
- *3 mile island*
- *Challenger explosion*
- *Fukushima power plant meltdown*
- *COVID19*



RMS Titanic Sinks
1912
“Unsinkable”



9/11 Terrorist Attacks
2001
No one can attack us at home



Housing/Global Recession
2008
Belief that the housing market would never go down

Common Themes

Past experience
provided a false
sense of security

Lack of imagination

Massive impact in a
short amount of
time

After each event, the
pieces that lined up
to the event seem
eerily obvious

The Last Message You Ever Want To See

What happened to your files?

Your network targeted by **RobbinHood** ransomware.

We've been watching you for days and we've worked on your systems to gain full access to your company and bypass all of your protections.

You must pay us in **4 days**, if you don't pay in the specified duration, the price increases **\$10,000** each day after the period. After 10 days your keys and your panel will be removed automatically and you won't be able to get your files, just ask Google, don't upload your files to VirusTotal or services like that, don't call FBI or other security organizations. For security reasons **don't shutdown your systems**, don't recover your computer, don't rename your files, it will damage your files. All procedures are automated so don't ask for more times or somethings like that we won't talk more, all we know is MONEY. If you don't care about yourself we won't too. So do not waste your time and **hurry up!** Tik Tak, Tik Tak, Tik Tak

What happened to your files?

All of your files locked and protected by a strong encryption with **RSA-4096** ciphers.

More information about the RSA can be found here:

[https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

In summary you can't read or work with your files, but with our help you can recover them.

It's **impossible** to recover your files without private key and our unlocking software. (You can Google: Baltimore city, Greenville city and RobbinHood)

Just pay the ransomware and end the suffering then get better cybersecurity

How to get private key or unlocking software?



YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!

If you want to restore them, follow this link:

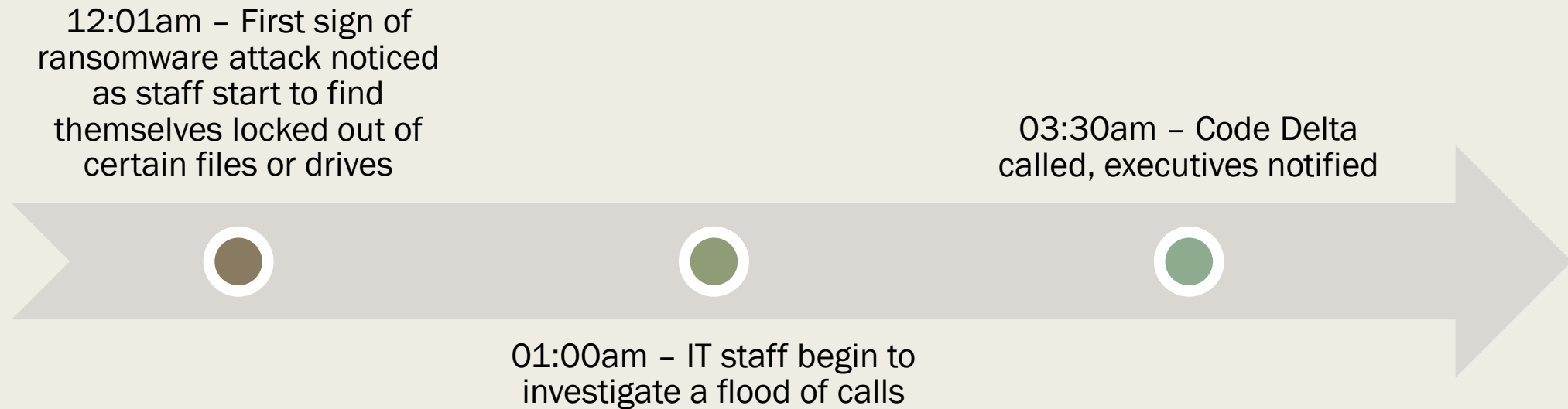
Use [Tor Browser](#) to access this address.

If you have not been answered via the link within 12 hours, write to us by e-mail:

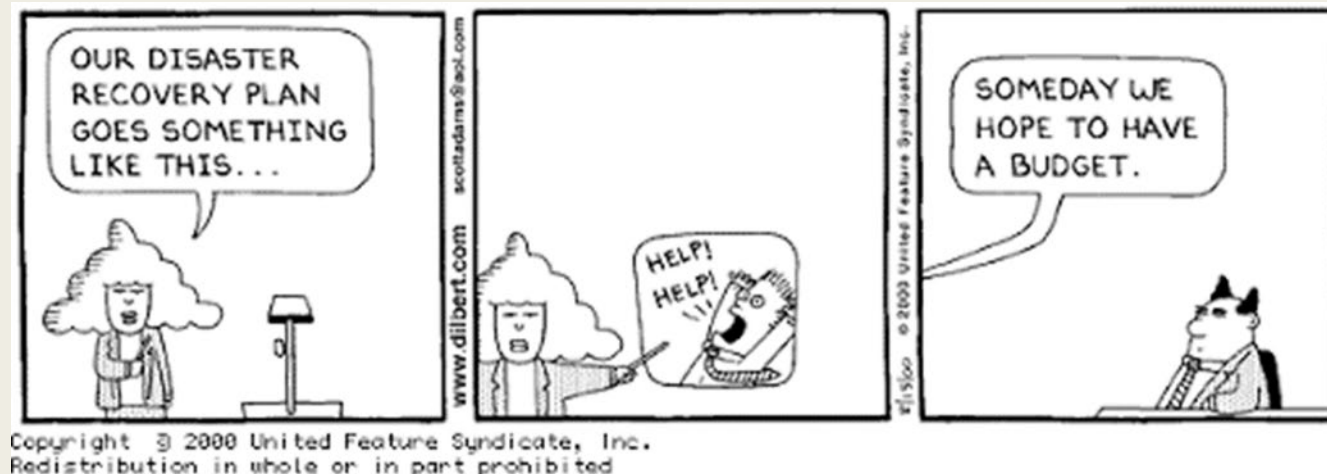
Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.

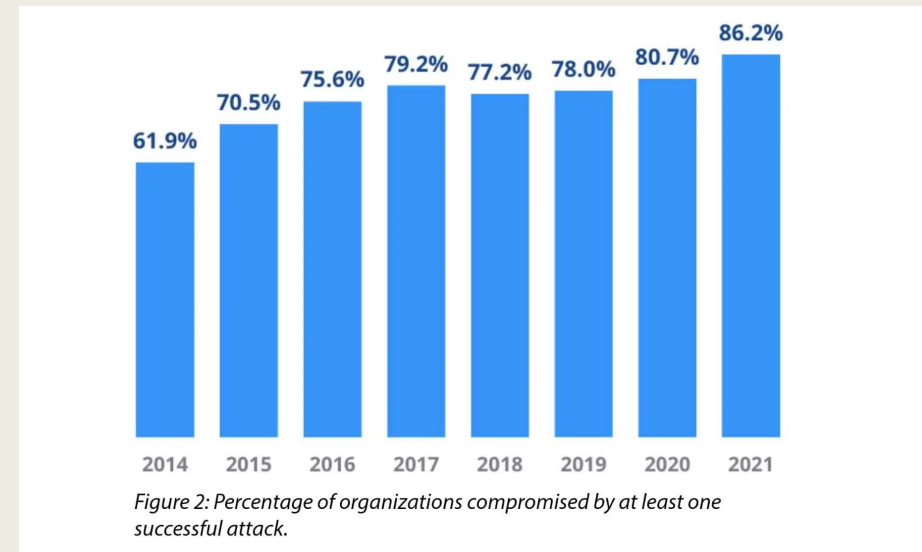
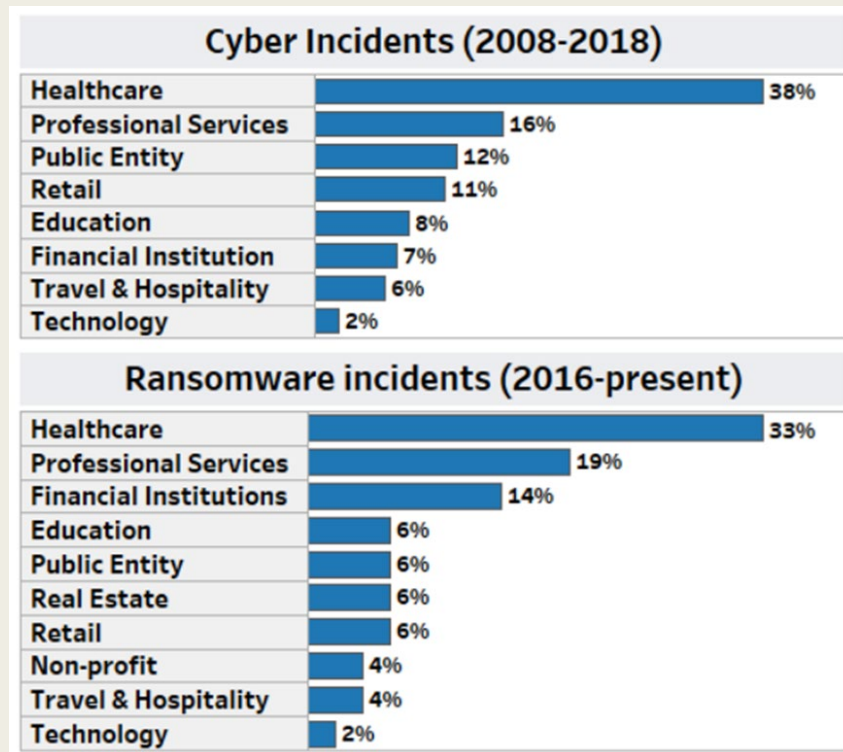
Nothing Good Happens After Midnight



Crisis Management 101



Why Us?



Why Healthcare is a Top Target

- The data is highly valuable
- Lack of investment/training in security
- Highly interconnected systems with a lot of entry points
- Illegal to conduct “Information Blocking”
- Fast moving parts, pieces, regulations and rules
- COVID19

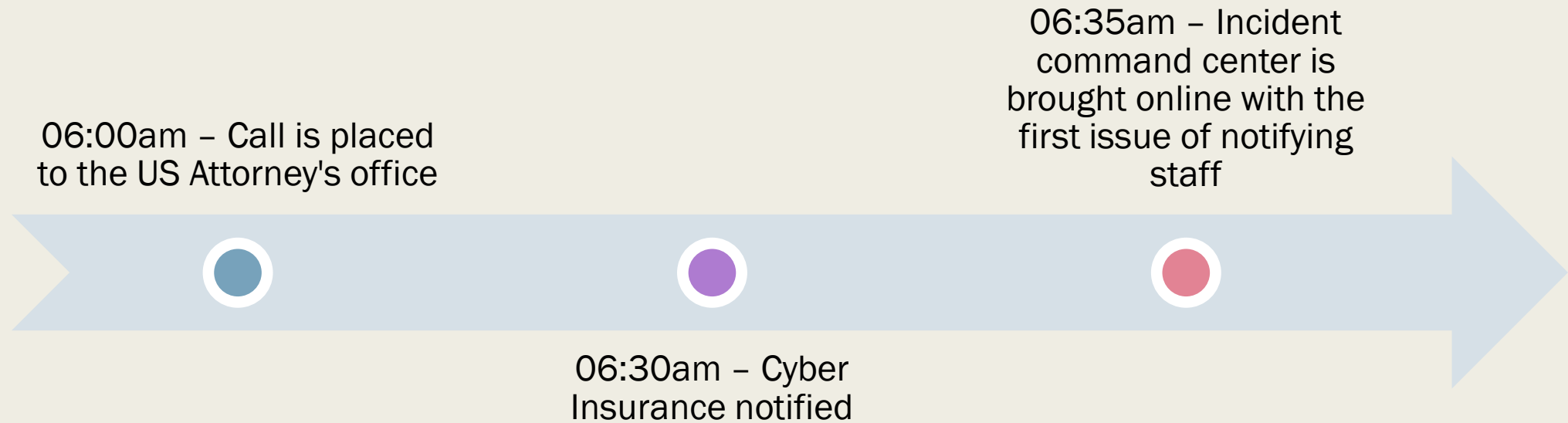
And It's Getting Expensive

Healthcare Organizations Struggle to Obtain Cyber Insurance Policies, Report Shows

As cyber attacks on health care soar, so does the cost of cyber insurance

Rising premiums, more restricted cyber insurance coverage poses big risk for companies

Off To The Races



Impact Statement

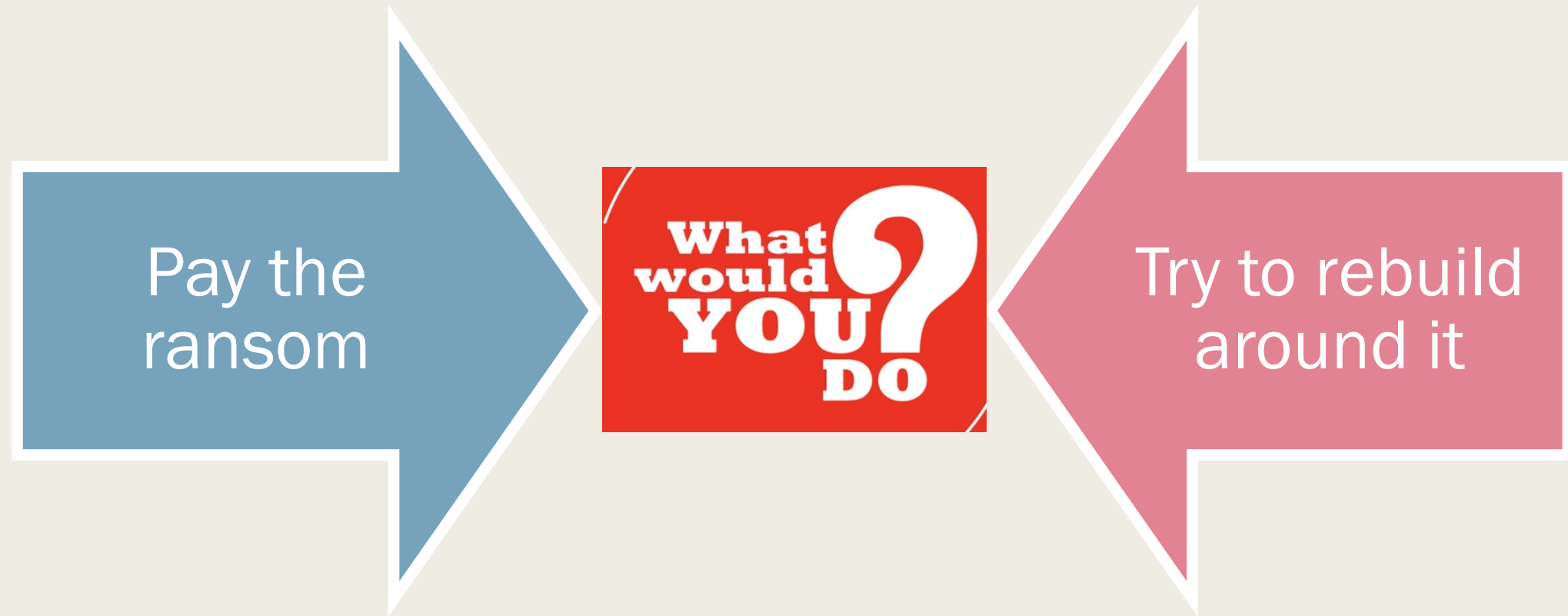
Impacted

- UH Data Center
- Microsoft, payroll, time keeping, faxes, shared file storage, etc.
- ~70% of servers; ~400 PC's

Not Impacted

- Electronic medical record
- Third party applications remote or cloud hosted

The BIG Question



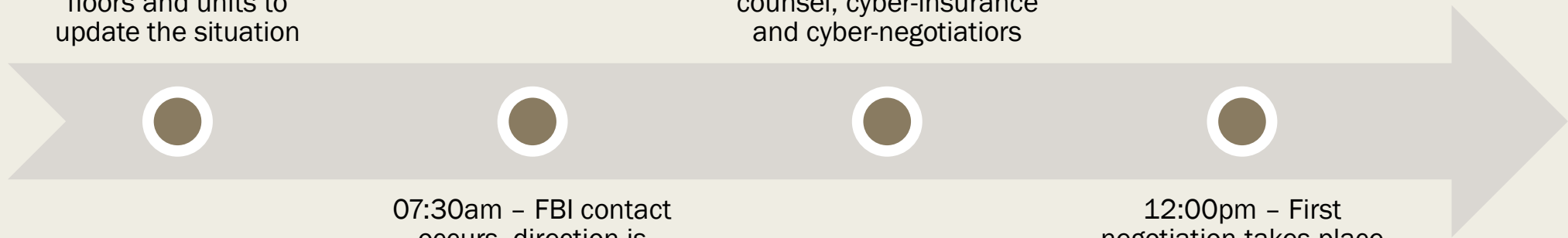
Day Shift Begins

06:45am – Staff are identified to call outlying clinics and run updates manually to different floors and units to update the situation

10:15am – Call with executives, outside counsel, cyber-insurance and cyber-negotiators

07:30am – FBI contact occurs, direction is provided to external cyber-negotiators

12:00pm – First negotiation takes place



A New Industry...



How Most Of Us Feel



While All That's Happening...

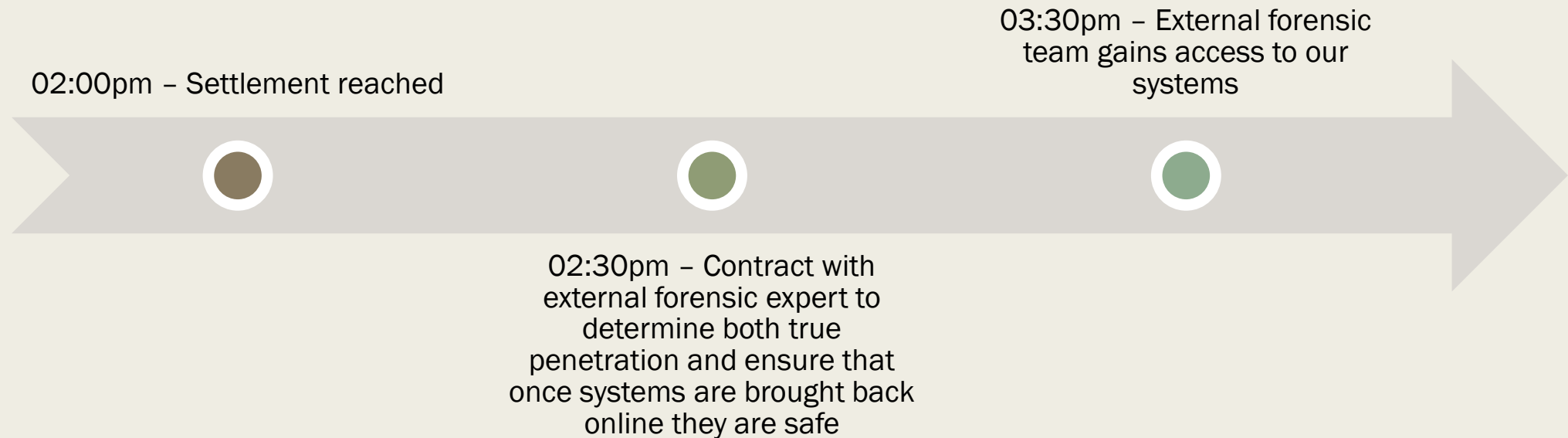
Clinical Staff

- Still seeing patients as EMR was not impacted
- Did not go on diversion
- Paging system still worked for codes or rapid responses

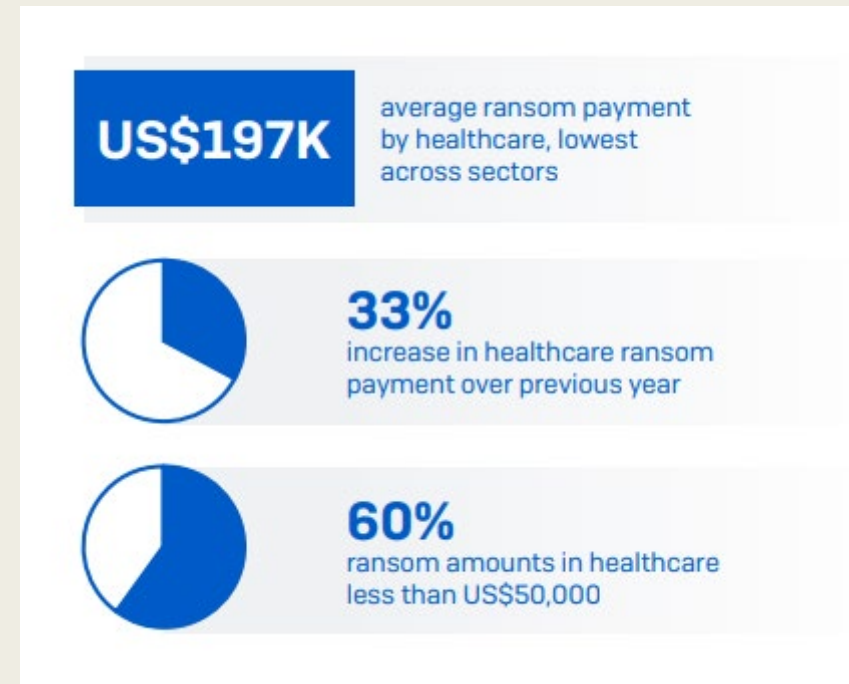
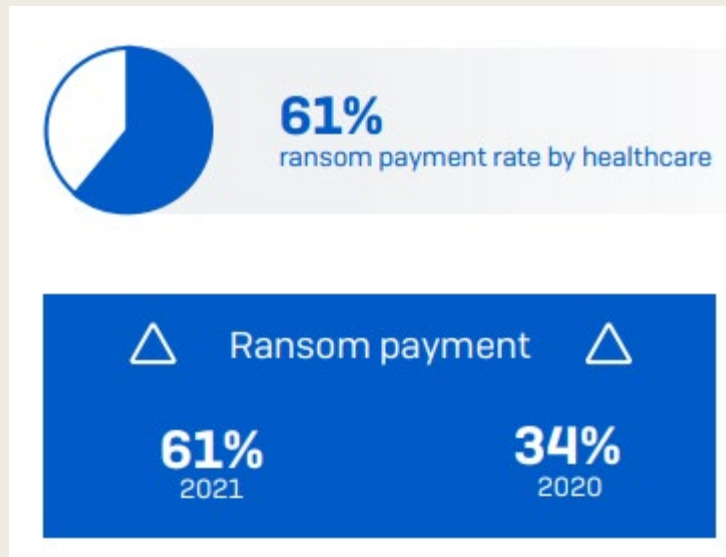
In the ICC

- How to handle communications?
- Planning for what happens if this drags out for days/weeks
- How to handle payroll as it was a pay week


Things Start to Fall Into Place




To Pay or Not to Pay?



What If's....

A large yellow circle with a white border, containing white text.

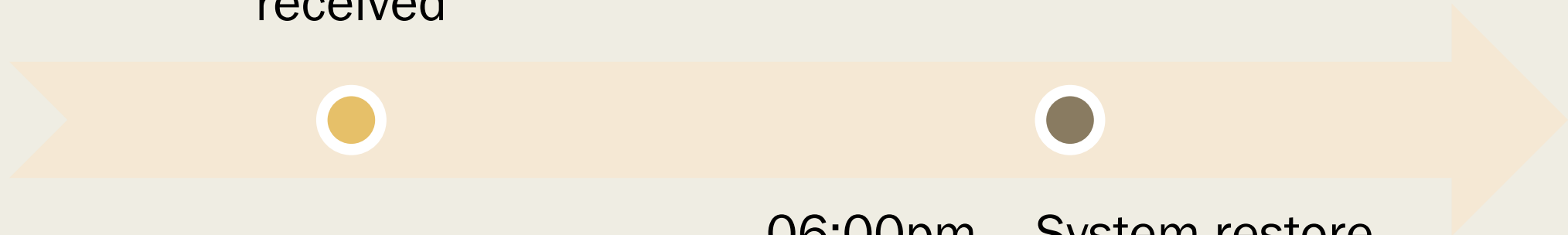
What if they
don't provide
us the
decryption key
once we pay?

A large grey circle with a white border, containing white text.

What if they
come back
a month
later and do
this again?

18 Hours Later...

05:00pm – Ransom paid
and decryption key
received



06:00pm – System restore
begins

Long Tail...

- Rolled out multi-factor authentication within 16 days of incident
- Forensic report found no further or lingering evidence of malicious code
- Staff mass texting software rolled out within a month of the incident
- ICC work plan was key to ensuring smooth operations
- Impact to third parties who may have shut off access during the incident

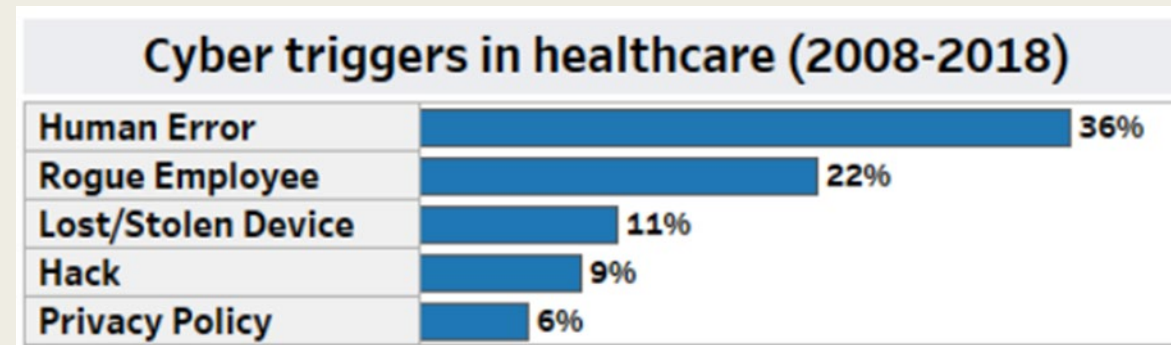
Can We Prevent This?



Rule Number 1 – You Can't Protect Against Dumb



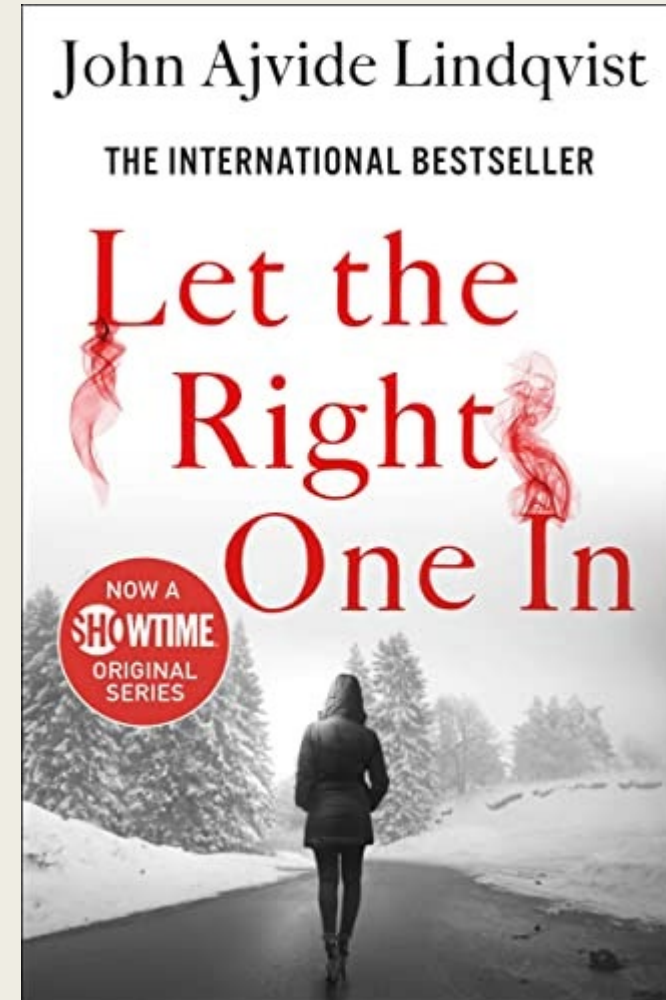
Rule Number 2 – You Can't Protect Against Dumb



So How Did This Even Happen?

A patient had downloaded an app from the app store with the code embedded in it and when the phone connected to our guest network, it released the ransomware

The phone was confiscated and provided to the authorities (no malicious intent by the patient)



All's Well That Ends Well?

