```
d=function(){var a,c,d,f,g,h,i
f(i===f)continue;
.,readyWait:1,holdReady
&e(c).trigger("ready").
achEvent){c.attachEvent(
n(a){return e.type(a)
on(a){if(!a||e.type(a)
b.in.a)return!1;return
"]").replace(r,"")))return(
oadXML(c))}catch(g){d=b}
a.replace(x,"ms-").replace
pply(a[g++],d)===!1)break
a,b){var c=b||[];if(a
```

Managing Through Getting Hacked:

Inside the Wild 18 Hours From First Intrusion Through Paying Them Off

Seth Jeremy Katz, MPH, RHIA, FAHIMA

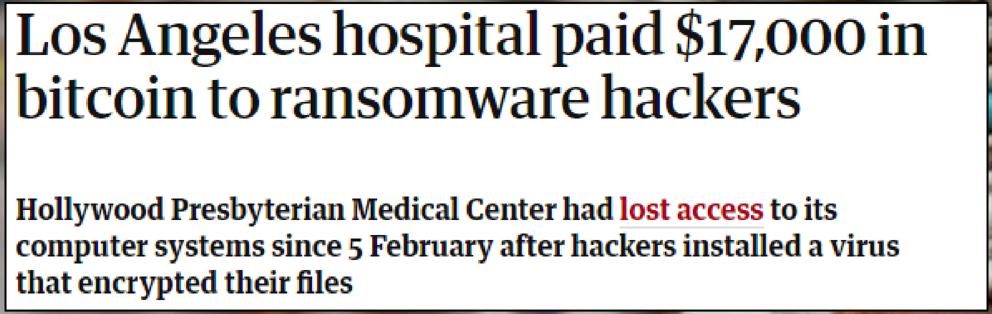
Vice President of Revenue Cycle and HIM

University Health

Learning Objectives

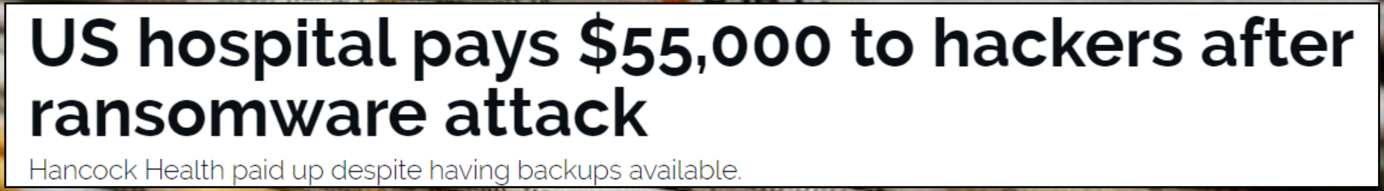
- Understanding how manage through a significant cybersecurity event
- What the industry can do going forward to prepare for these types of events
- Statistics about the growing number of cyber security incidents impacting the healthcare sector

Would've Been Gibberish Headlines Just A Few Years Ago



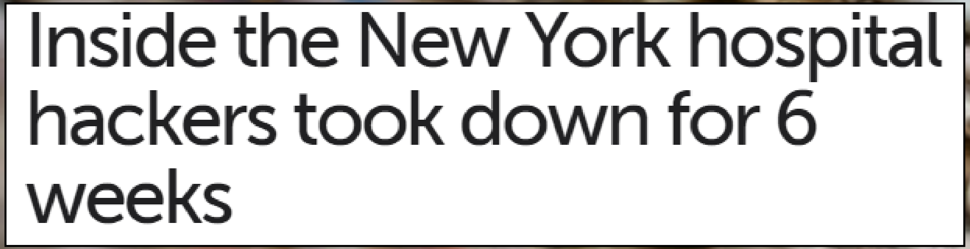
Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

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

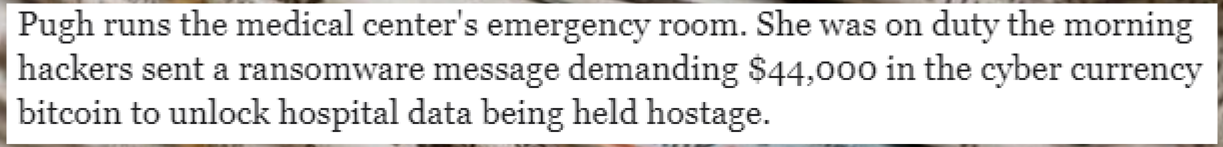


US hospital pays $55,000 to hackers after ransomware attack

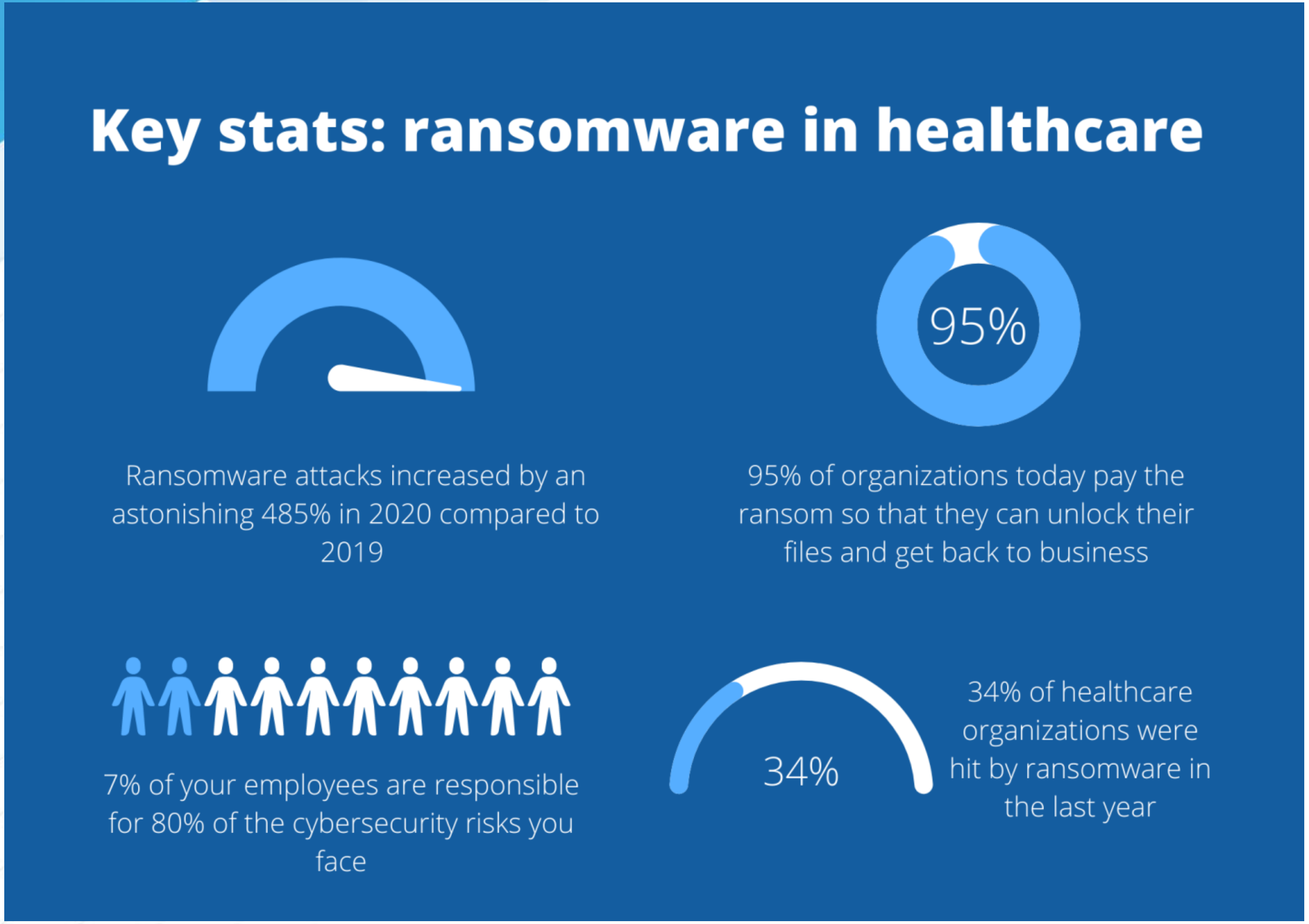
Hancock Health paid up despite having backups available.



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.



Key stats: ransomware in healthcare

Ransomware attacks increased by an astonishing 485% in 2020 compared to 2019

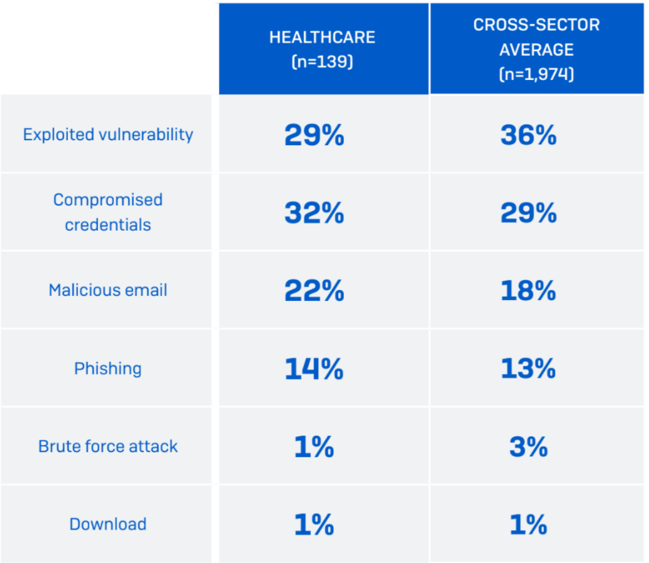
95%

95% of organizations today pay the ransom so that they can unlock their files and get back to business

7% of your employees are responsible for 80% of the cybersecurity risks you face

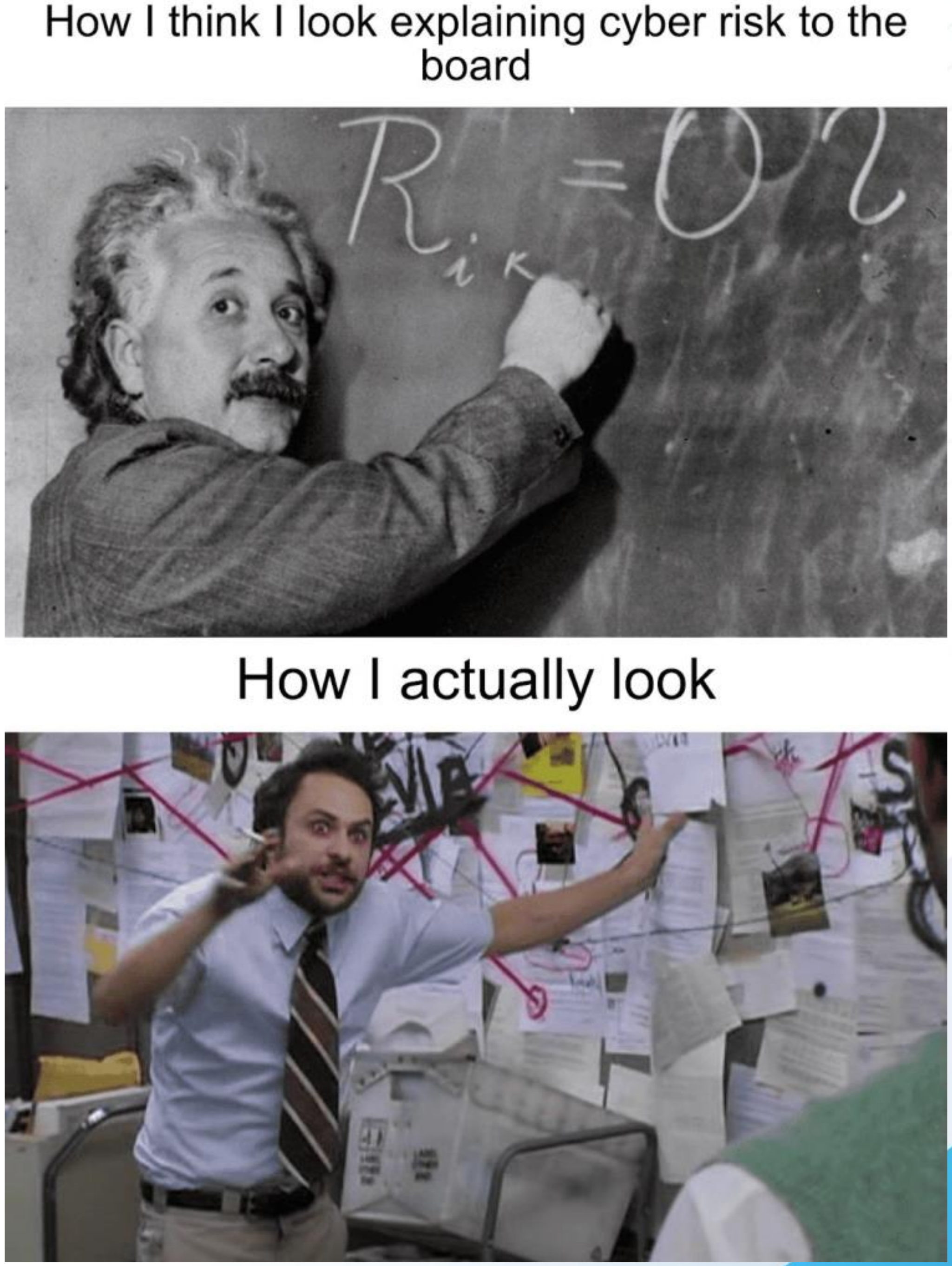
34%

34% of healthcare organizations were hit by ransomware in the last year



	HEALTHCARE (n=139)	CROSS-SECTOR AVERAGE (n=1,974)
Exploited vulnerability	29%	36%
Compromised credentials	32%	29%
Malicious email	22%	18%
Phishing	14%	13%
Brute force attack	1%	3%
Download	1%	1%

There’s a large gap in understanding risks and preparing for them



3 of the Big Ones…

NUANCE®

2018 Attack; $92M in losses

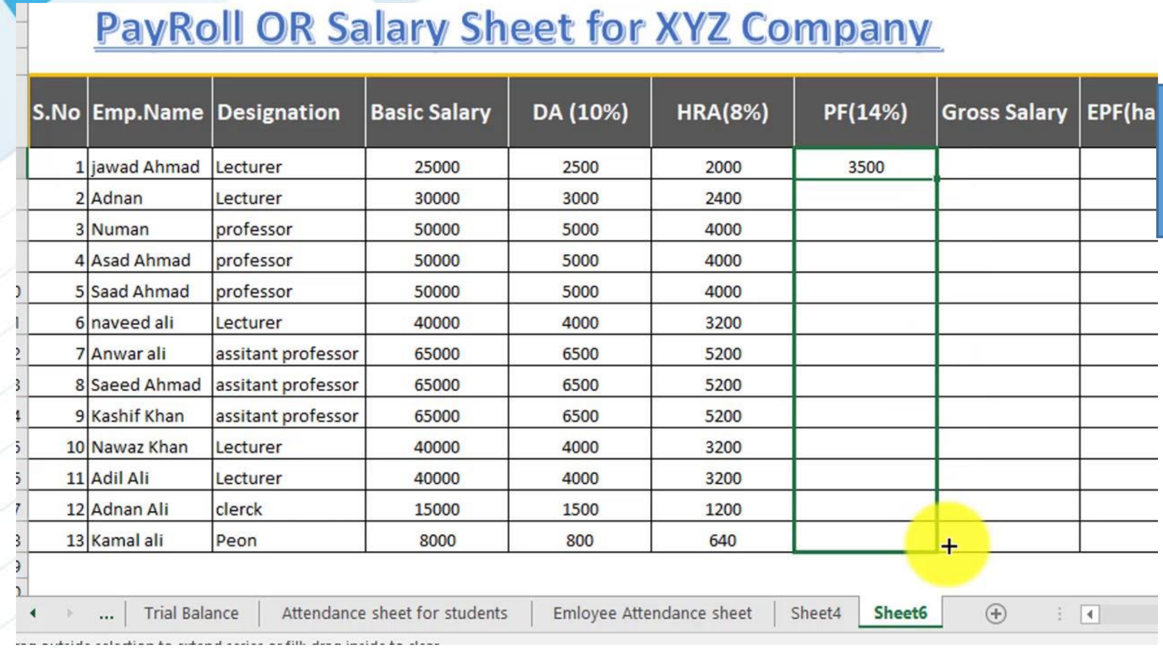
KRONOS®

2021 Attack; Impacted over 8K businesses

CHANGE HEALTHCARE

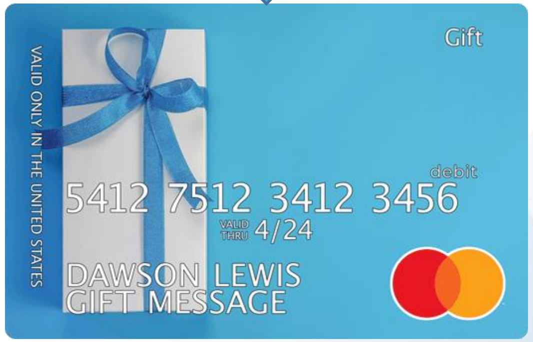
2024 Attack; over 4TB of data stolen, millions in losses

A Preview of Things To Come…?



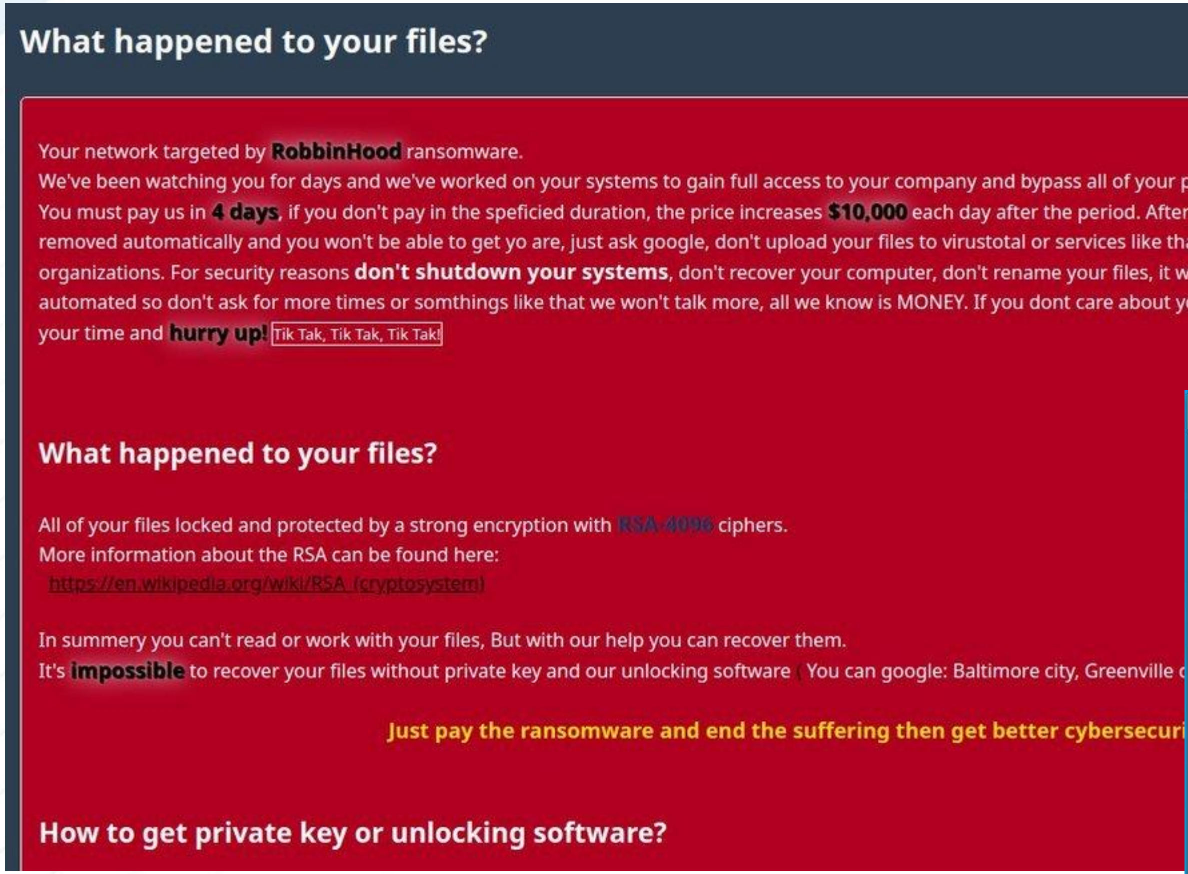
PayRoll OR Salary Sheet for XYZ Company

S.No	Emp.Name	Designation	Basic Salary	DA (10%)	HRA(8%)	PF(14%)	Gross Salary	EPF(ha
1	jawad Ahmad	Lecturer	25000	2500	2000	3500		
2	Adnan	Lecturer	30000	3000	2400			
3	Numan	professor	50000	5000	4000			
4	Asad Ahmad	professor	50000	5000	4000			
5	Saad Ahmad	professor	50000	5000	4000			
6	naveed ali	Lecturer	40000	4000	3200			
7	Anwar ali	assitant professor	65000	6500	5200			
8	Saeed Ahmad	assitant professor	65000	6500	5200			
9	Kashif Khan	assitant professor	65000	6500	5200			
10	Nawaz Khan	Lecturer	40000	4000	3200			
11	Adil Ali	Lecturer	40000	4000	3200			
12	Adnan Ali	clerck	15000	1500	1200			
13	Kamal ali	Peon	8000	800	640			



Nothing Good Happens After Midnight

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 speficied 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 yo are, 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 somthings like that we won't talk more, all we know is MONEY. If you dont care about yourself we won't too. So do not waste your time and **hurry up!** Tik Tak, Tik Tak, Tik Tak!

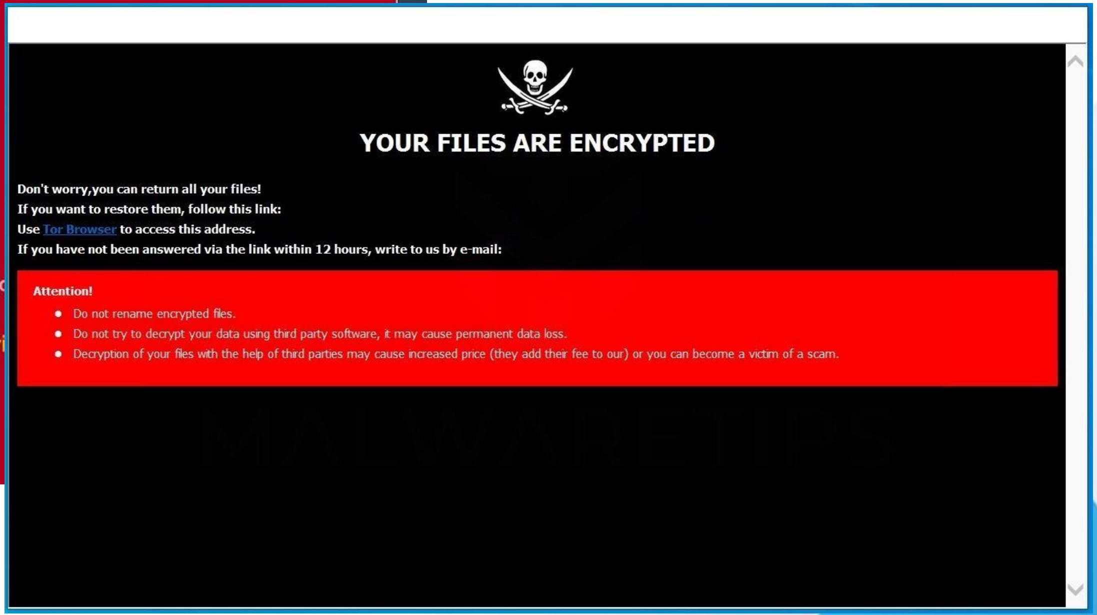
What happened to your files?

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)

In summery 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 c

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

How to get private key or unlocking software?



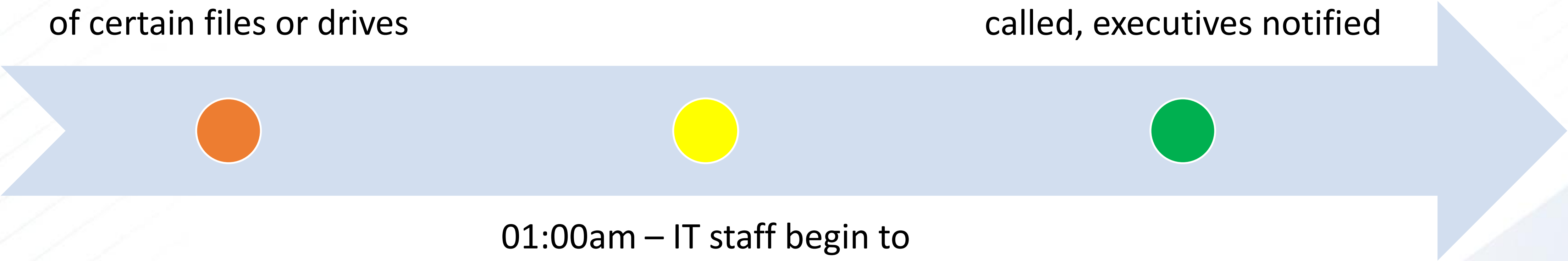
YOUR FILES ARE ENCRYPTED

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 our) or you can become a victim of a scam.

So It Begins…



12:01am – First sign of ransomware attack noticed as staff start to find themselves locked out of certain files or drives

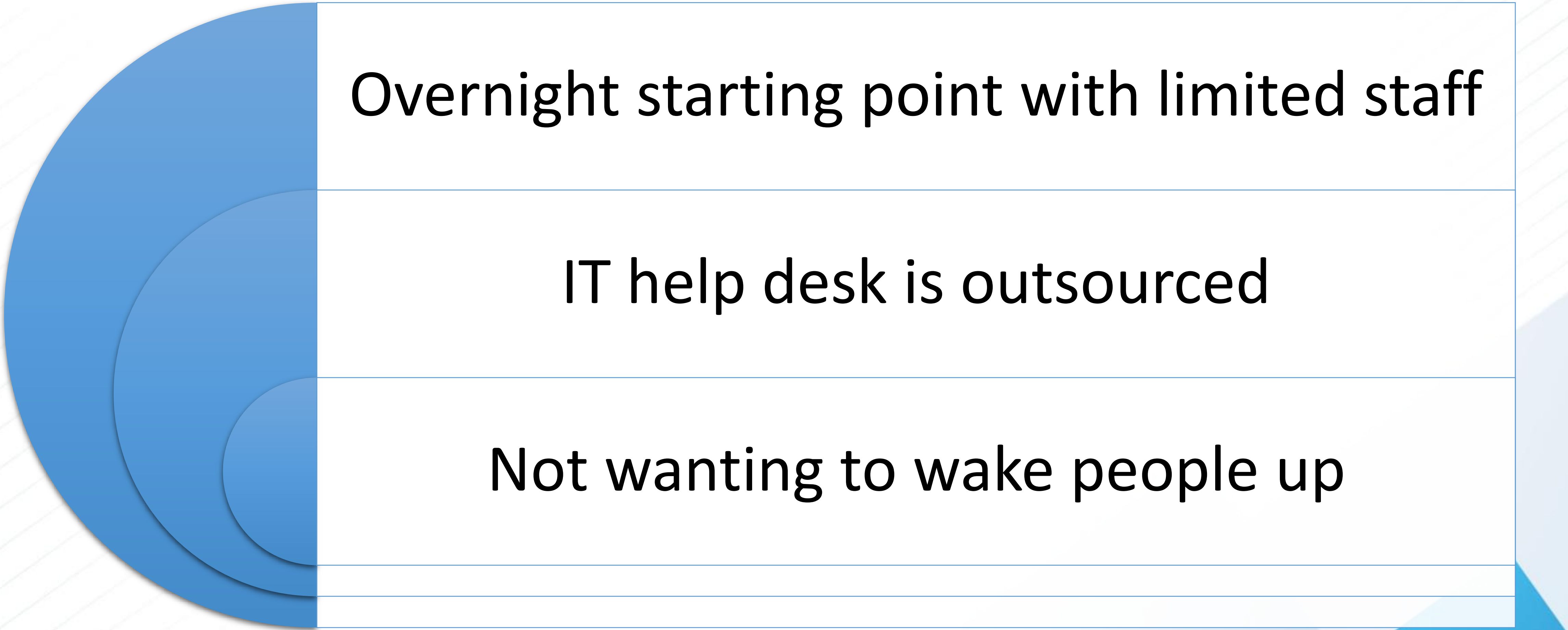
01:00am – IT staff begin to investigate a flood of calls

03:30am – Code Delta called, executives notified

Crisis Management 101

OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...
scottadams@aol.com
www.dilbert.com
HELP! HELP!
© 2000 United Feature Syndicate, Inc.
SOMEDAY WE HOPE TO HAVE A BUDGET.

First Set of Challenges

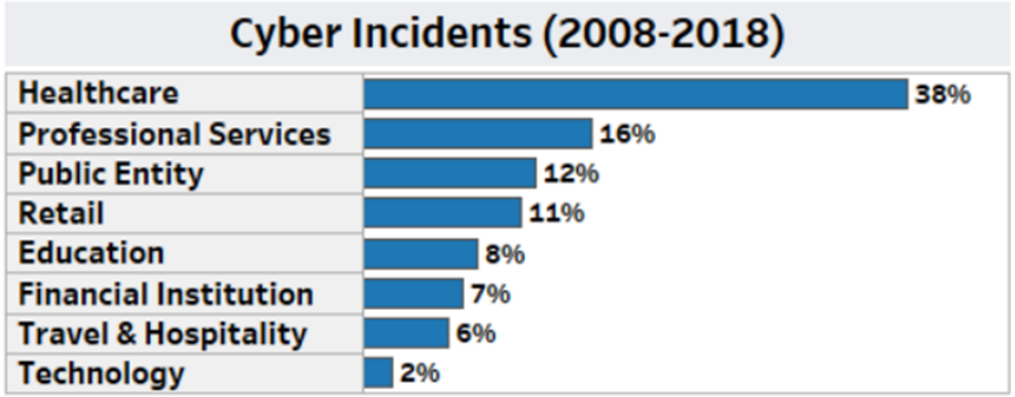


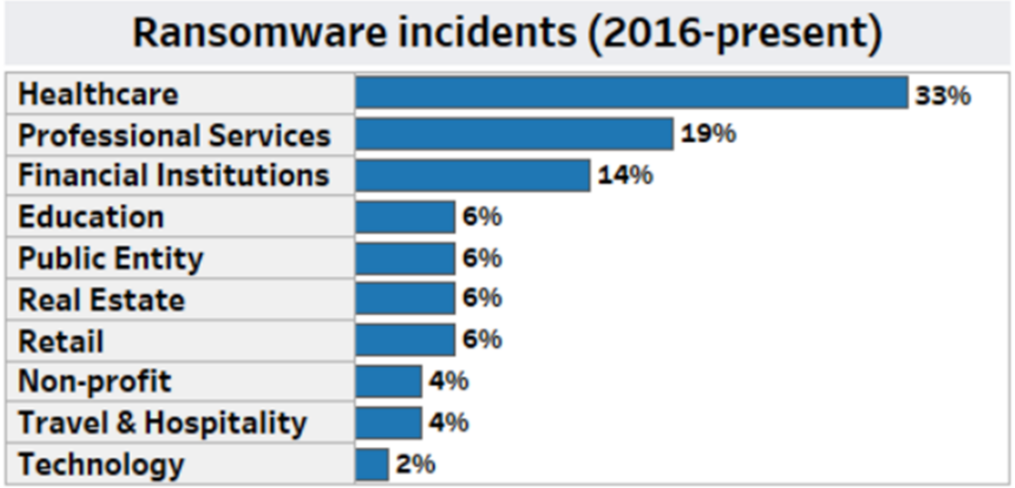
Overnight starting point with limited staff

IT help desk is outsourced

Not wanting to wake people up

Why Us?


Cyber Incidents (2008-2018)


Ransomware incidents (2016-present)

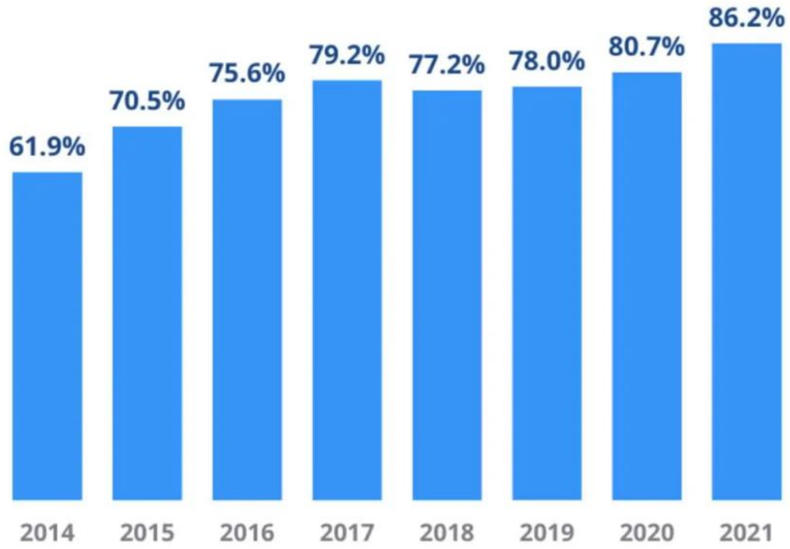
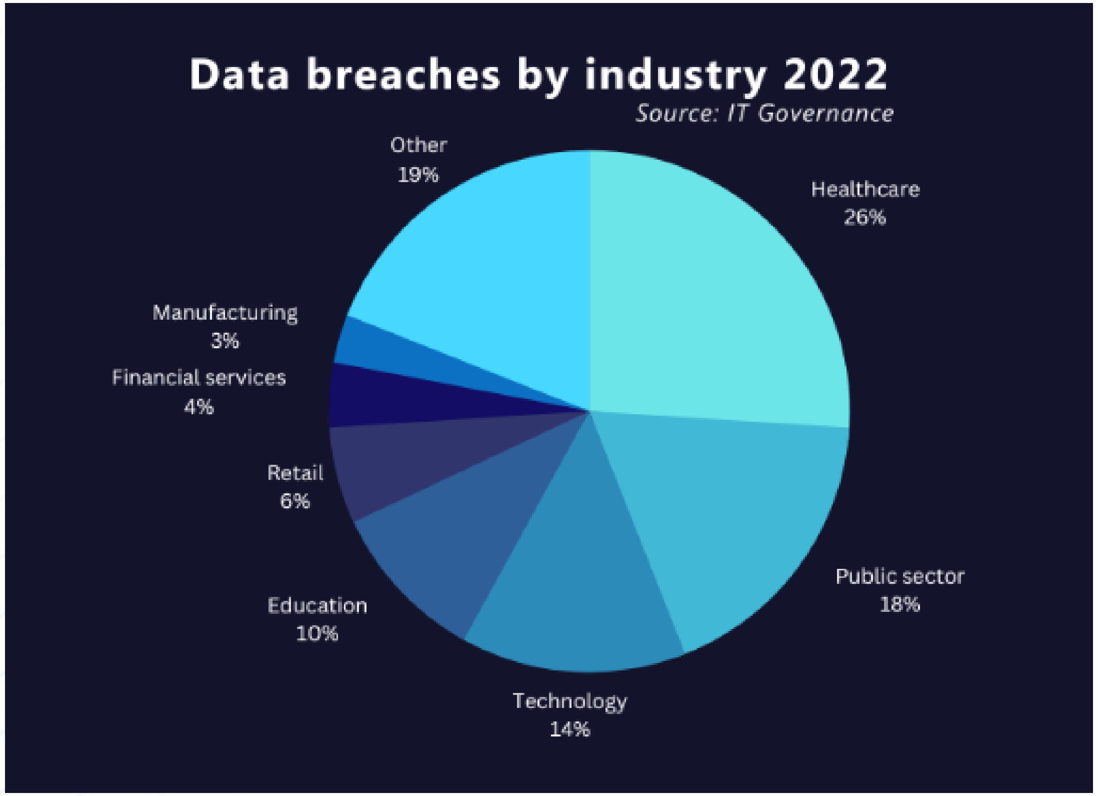
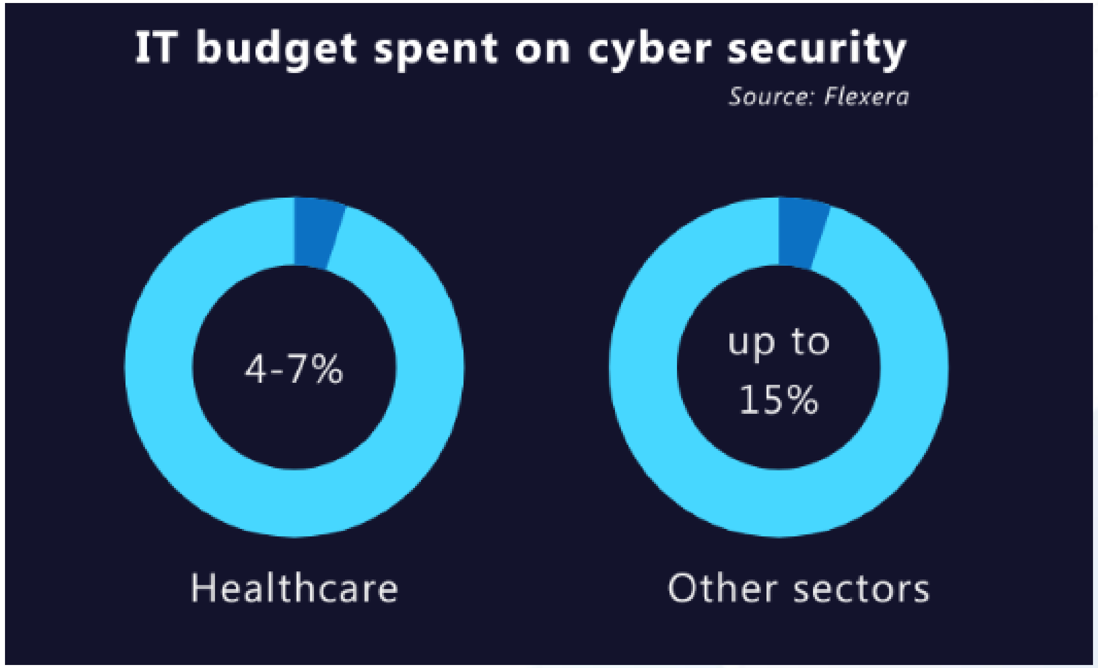


Figure 2: Percentage of organizations compromised by at least one successful attack.

Why Us?

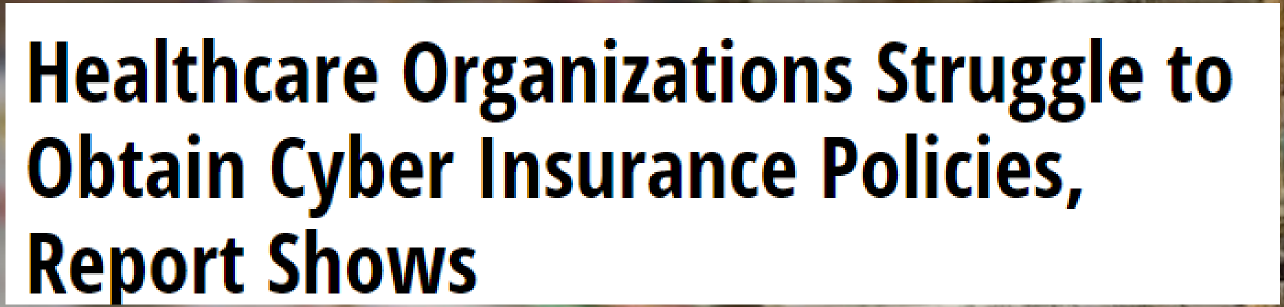

Data breaches by industry 2022
Source: IT Governance
Other 19%
Healthcare 26%
Manufacturing 3%
Financial services 4%
Retail 6%
Education 10%
Technology 14%
Public sector 18%


IT budget spent on cyber security
Source: Flexera
4-7%
Healthcare
up to 15%
Other sectors

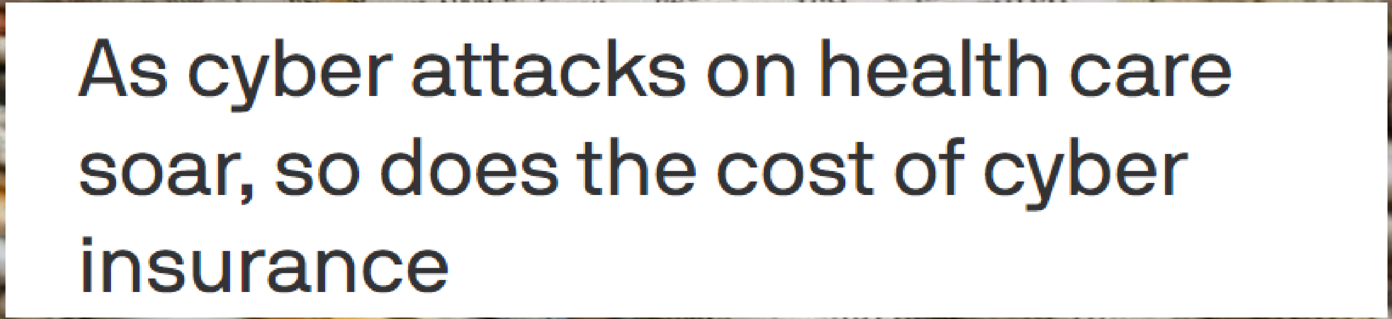
Why Healthcare is a Top Target

- 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

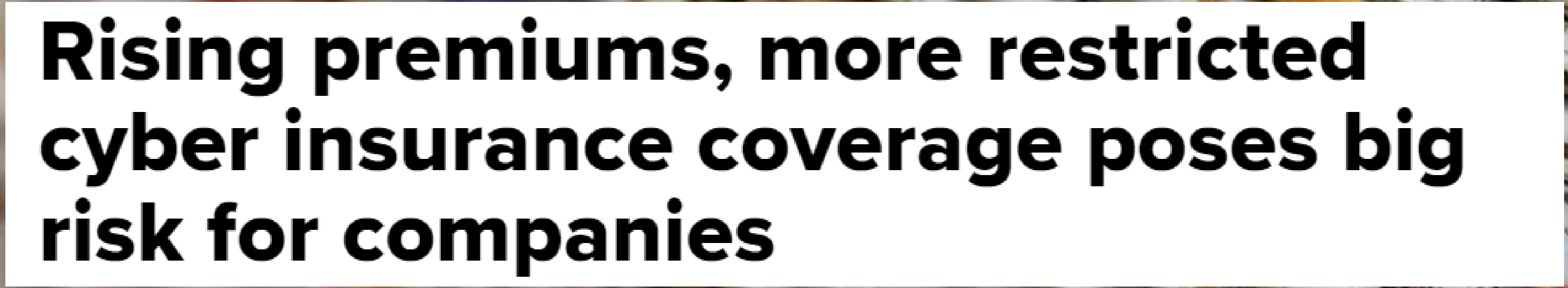
...And It's Getting Expensive



Healthcare Organizations Struggle to Obtain Cyber Insurance Policies, Report Shows

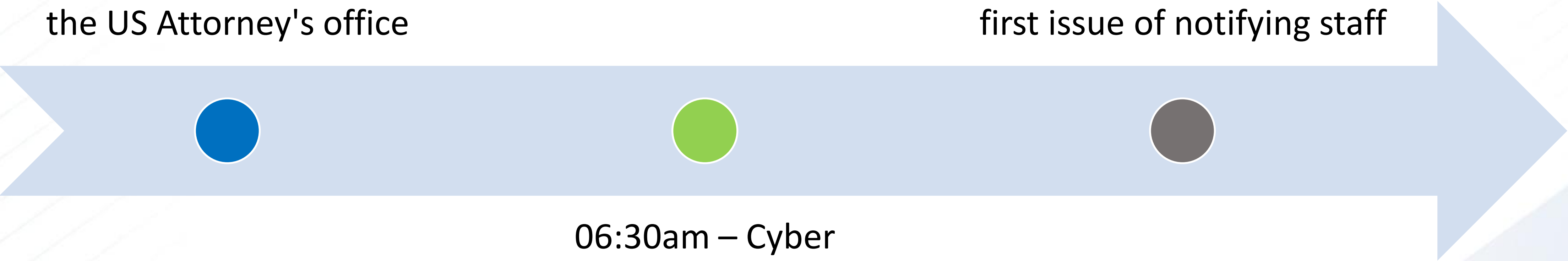


As cyber attacks on health care soar, so does the cost of cyber insurance



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

And We’re Off To The Races…

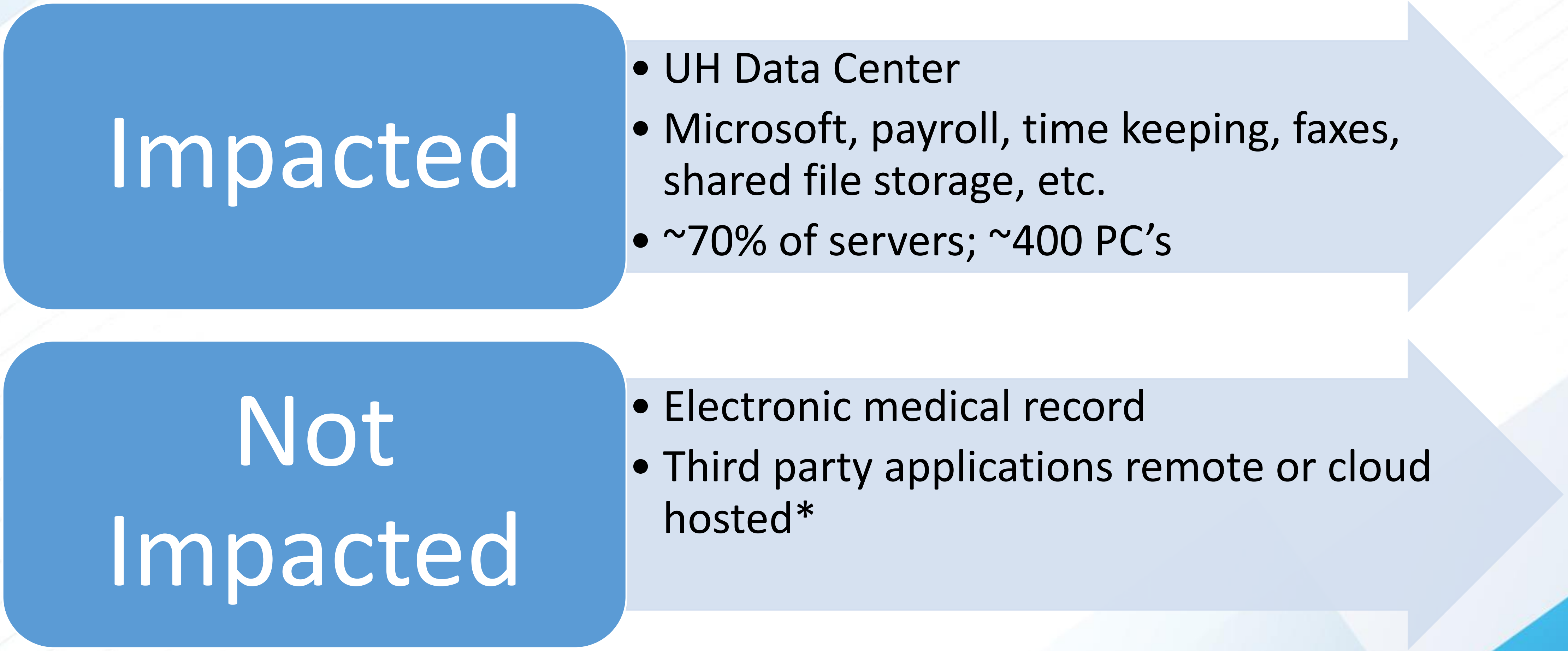


06:00am – Call is placed to the US Attorney's office

06:30am – Cyber Insurance notified

06:35am – Incident command center is brought online with the first issue of notifying staff

What’s in Scope?



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*

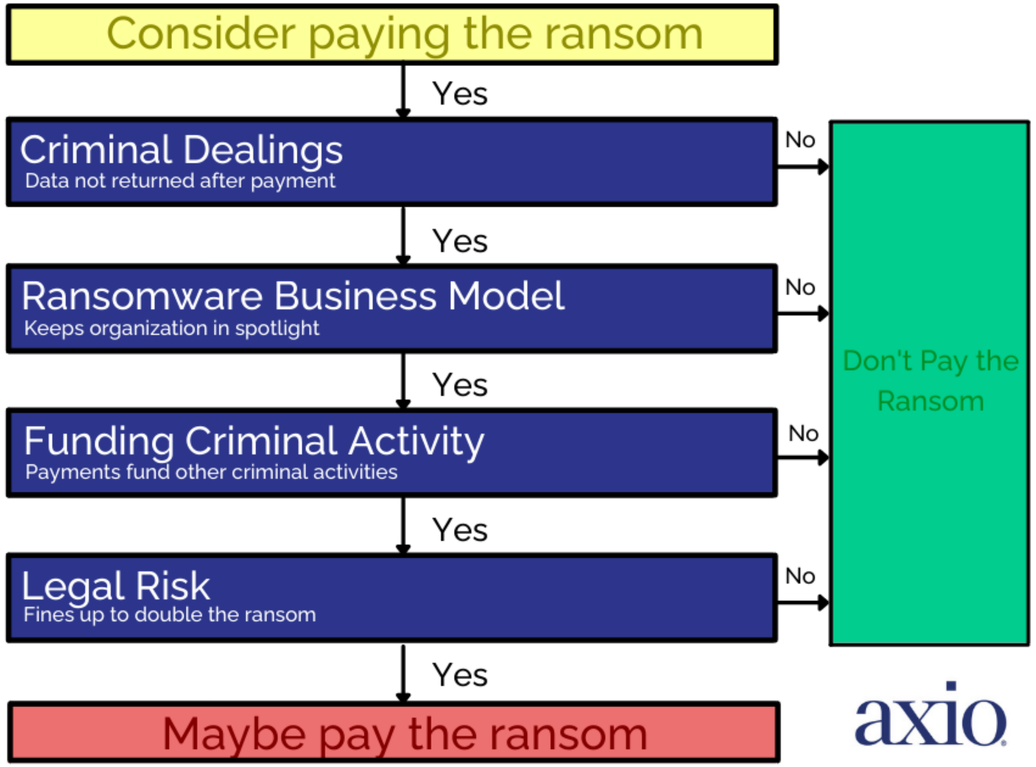
A Word About Third Party Vendors

The Question of the Day

Do you intend to pay the ransom or try to rebuild around the locked servers?

Risks of Paying the Ransom

Always consider the secondary risks when faced with a ransomware attack



Consider paying the ransom

Yes

Criminal Dealings

Data not returned after payment

No

Yes

Ransomware Business Model

Keeps organization in spotlight

No

Yes

Funding Criminal Activity

Payments fund other criminal activities

No

Yes

Legal Risk

Fines up to double the ransom

No

Yes

Maybe pay the ransom

Don't Pay the Ransom

axio

New Industry Is Born

PROVEN DATA

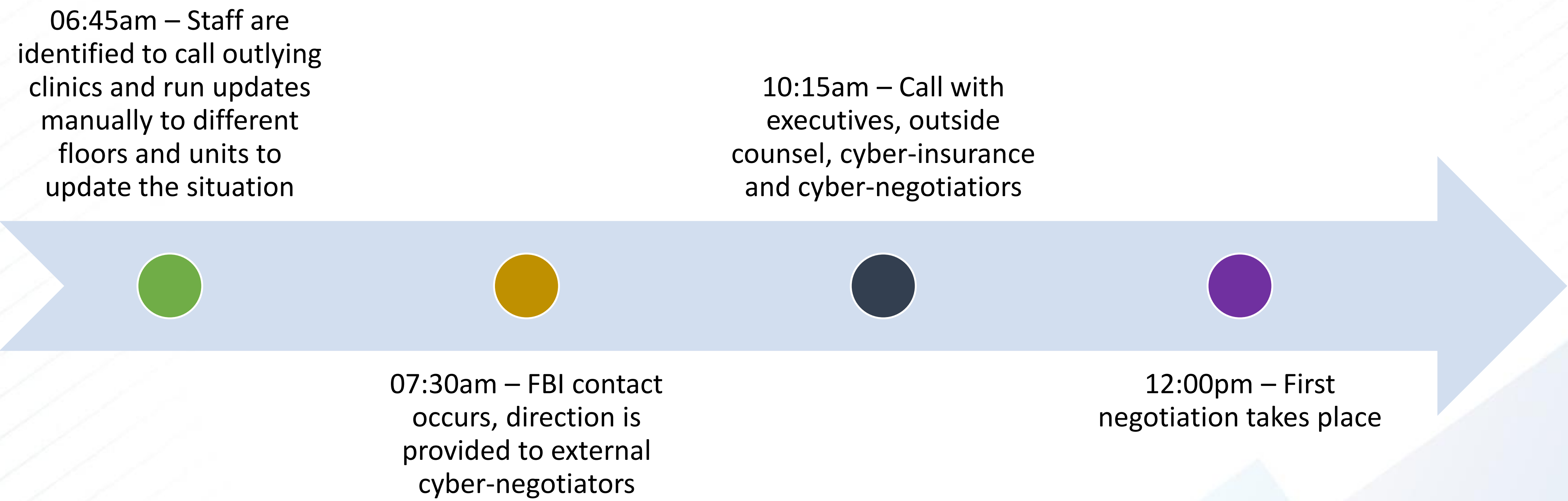
Atlant Security

CyberSecOp

AGIO

groupsense

Day Shift Is Coming On…



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

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

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

12:00pm – First negotiation takes place

I DON'T KNOW
HOW BITCOIN WORKS
AND AT THIS POINT
I'M TOO AFRAID TO ASK
imgflip.com

In The Meantime…

Clinical Staff

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

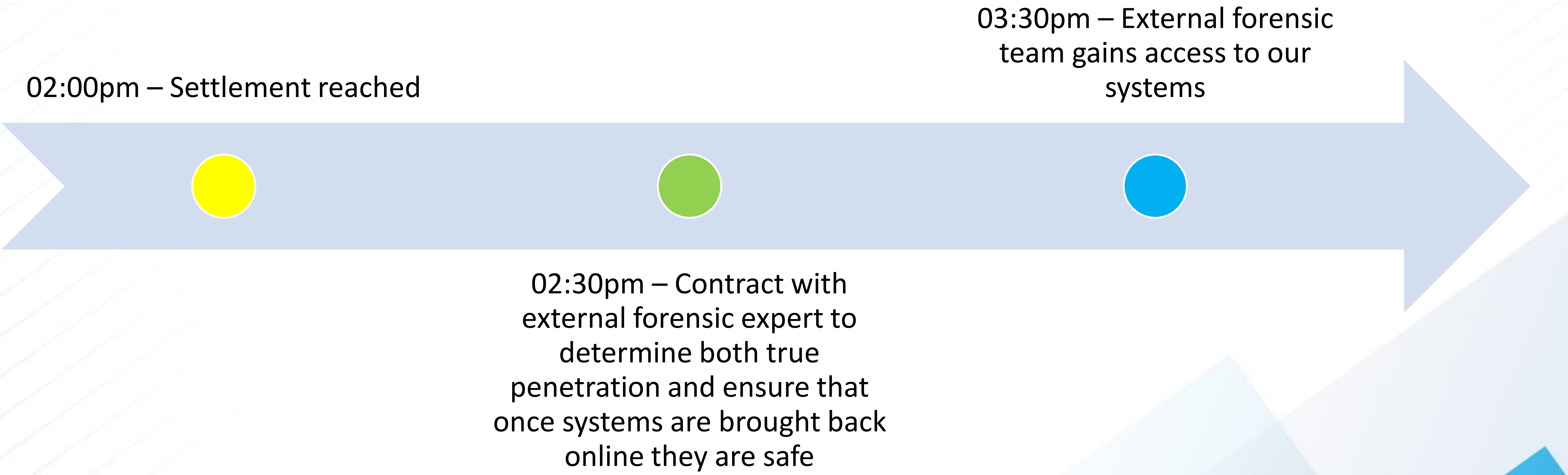
Non-Clinical Staff

- Notifying CMS and Joint Commission
- Planning for news coverage
- Supporting the ICC if their job is impacted

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
- Tracking costs

Things Are Falling Into Place…

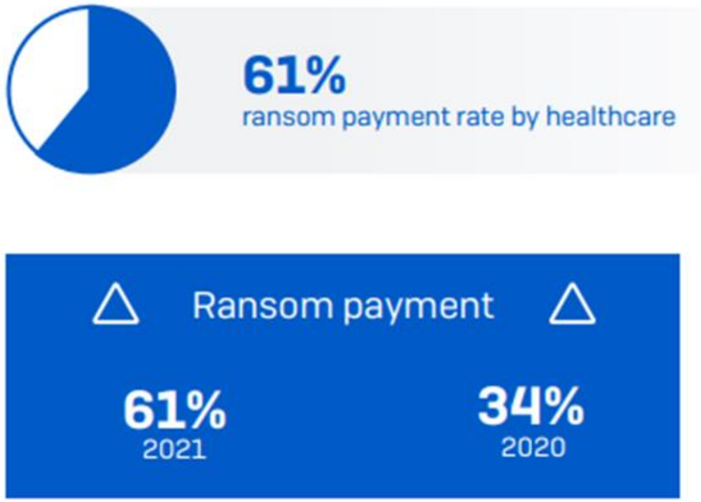


02:00pm – Settlement reached

02:30pm – Contract with external forensic expert to determine both true penetration and ensure that once systems are brought back online they are safe

03:30pm – External forensic team gains access to our systems

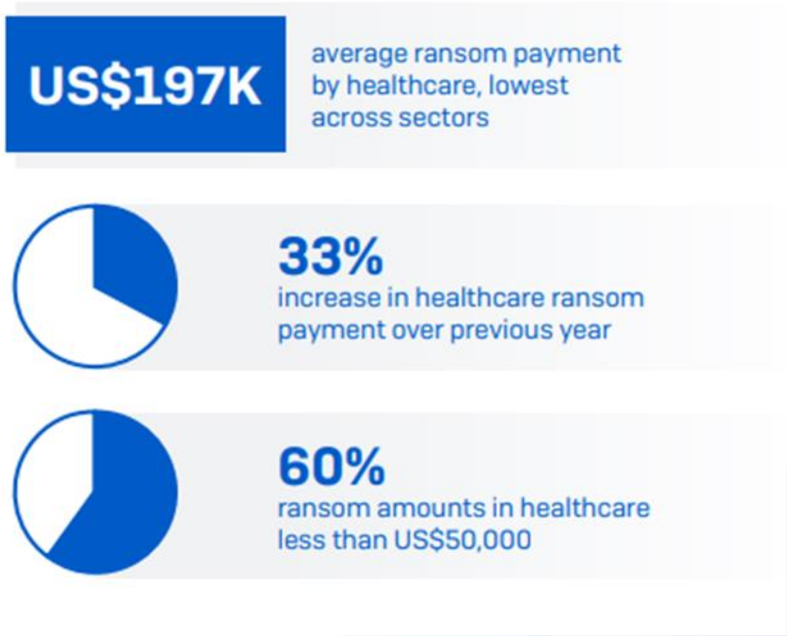
To Pay Or Not To Pay



61%
ransom payment rate by healthcare

△ Ransom payment △

61%	34%
2021	2020



US$197K average ransom payment by healthcare, lowest across sectors

33%
increase in healthcare ransom payment over previous year

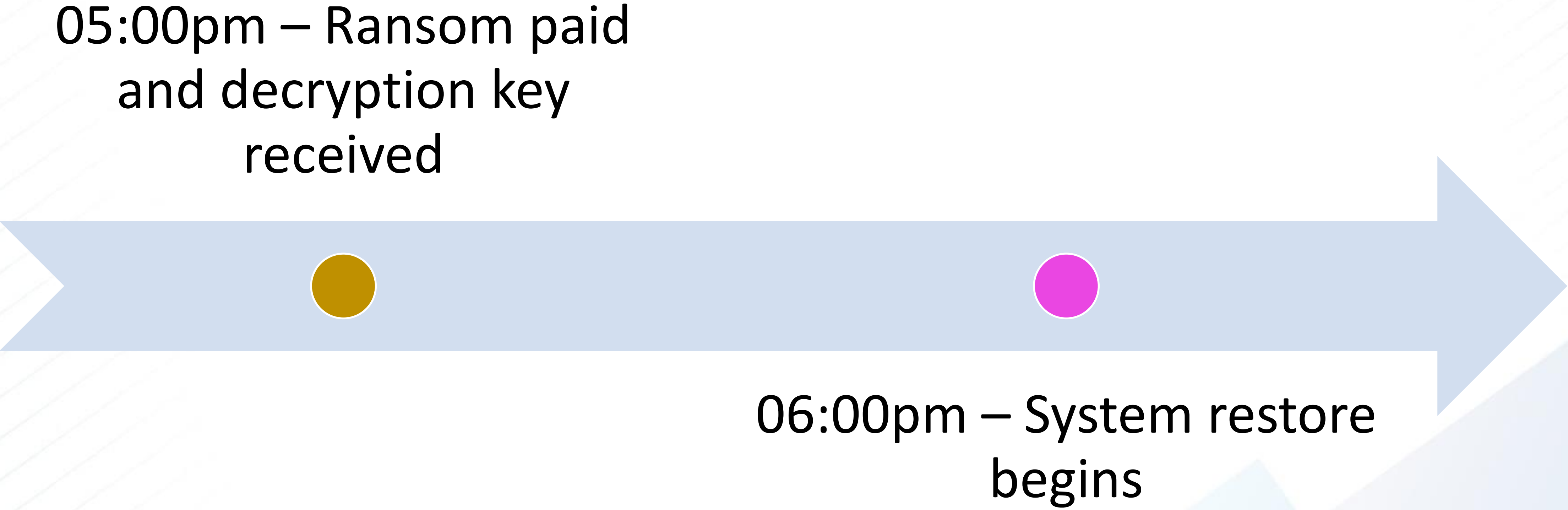
60%
ransom amounts in healthcare less than US$50,000

The What If's…

1. **<u>What If</u>** they don't provide us the decryption key once we pay?

2. **<u>What If</u>** they come back a month later and do this again?

And Eighteen Hours Later…



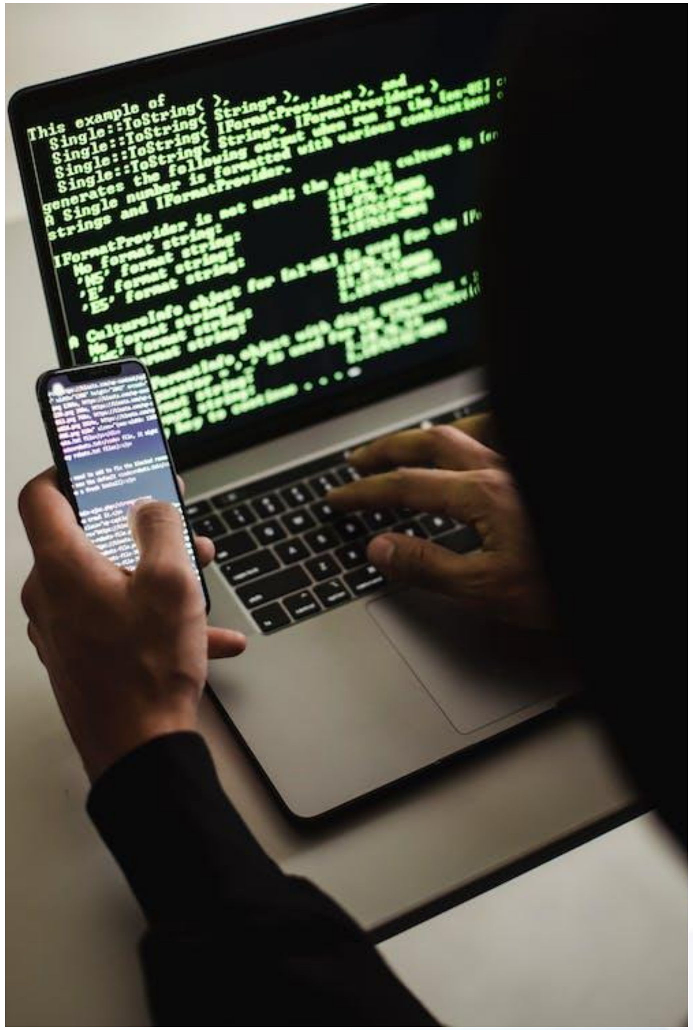
05:00pm – Ransom paid and decryption key received

06:00pm – System restore begins

A Long Tail

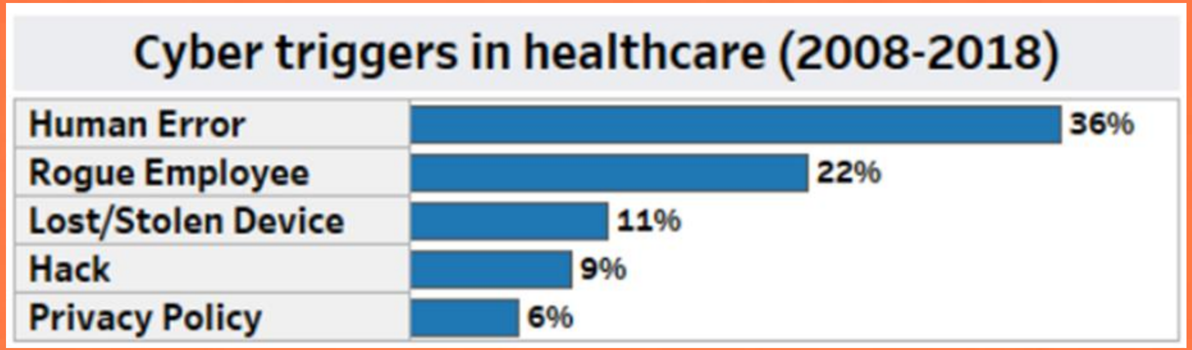
- Rolled out multi-factor authentication within 16 days of incident
- Forensic report found no further or lingering evidence of malicious code
- Staff mass texting software rolled out within a month of the incident
- ICC work plan was key to ensuring smooth operations
- Impact to third parties who may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

Could This Have Been Prevented?



Rule # 1: You Can’t Protect Against Dumb

DANGER
DO NOT TOUCH
NOT ONLY WILL THIS KILL YOU, IT WILL HURT THE WHOLE TIME YOU ARE DYING



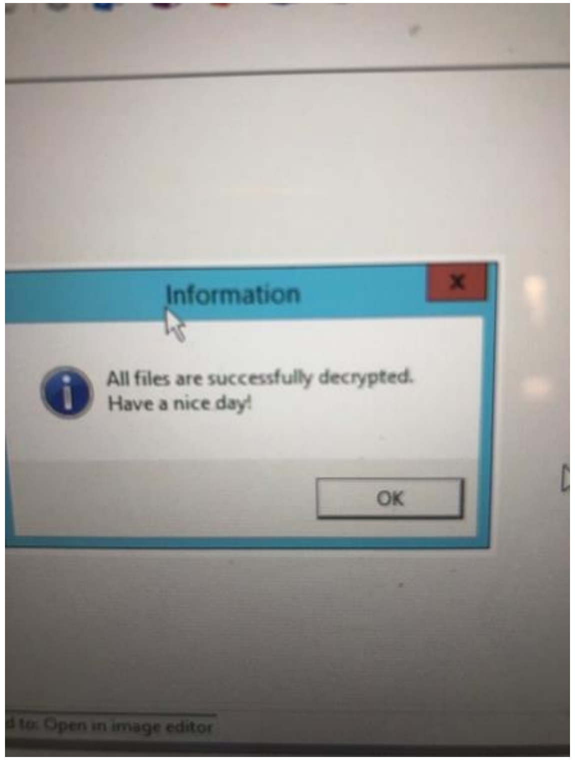
Rule # : You Can’t Protect Against Dumb

So How Did This 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?



All files are successfully decrypted.
Have a nice day!

Seth.katz@uhkc.org
816-404-3355