THE RANSOMWARE PANDEMIC IN HEALTHCARE

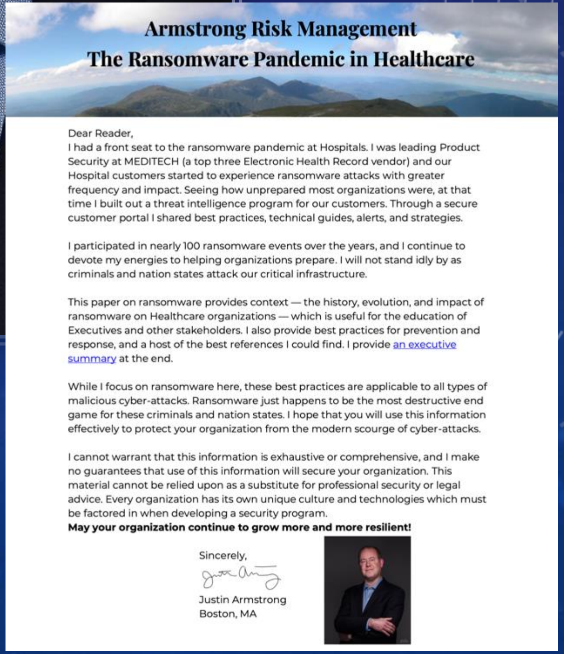
JUSTIN ARMSTRONG, CISSP, HCISPP, CCSP, MS

JUSTIN ARMSTRONG

- MEDITECH – EHR vendor, 22 years
- Tausight – Healthcare Cybersecurity Startup
- Armstrong Risk Management

Recently released e-book on

www.ArmstrongRisk.com



Armstrong Risk Management

The Ransomware Pandemic in Healthcare

Dear Reader,
I had a front seat to the ransomware pandemic at Hospitals. I was leading Product Security at MEDITECH (a top three Electronic Health Record vendor) and our Hospital customers started to experience ransomware attacks with greater frequency and impact. Seeing how unprepared most organizations were, at that time I built out a threat intelligence program for our customers. Through a secure customer portal I shared best practices, technical guides, alerts, and strategies.

I participated in nearly 100 ransomware events over the years, and I continue to devote my energies to helping organizations prepare. I will not stand idly by as criminals and nation states attack our critical infrastructure.

This paper on ransomware provides context — the history, evolution, and impact of ransomware on Healthcare organizations — which is useful for the education of Executives and other stakeholders. I also provide best practices for prevention and response, and a host of the best references I could find. I provide an executive summary at the end.

While I focus on ransomware here, these best practices are applicable to all types of malicious cyber-attacks. Ransomware just happens to be the most destructive end game for these criminals and nation states. I hope that you will use this information effectively to protect your organization from the modern scourge of cyber-attacks.

I cannot warrant that this information is exhaustive or comprehensive, and I make no guarantees that use of this information will secure your organization. This material cannot be relied upon as a substitute for professional security or legal advice. Every organization has its own unique culture and technologies which must be factored in when developing a security program.
May your organization continue to grow more and more resilient!

Sincerely,

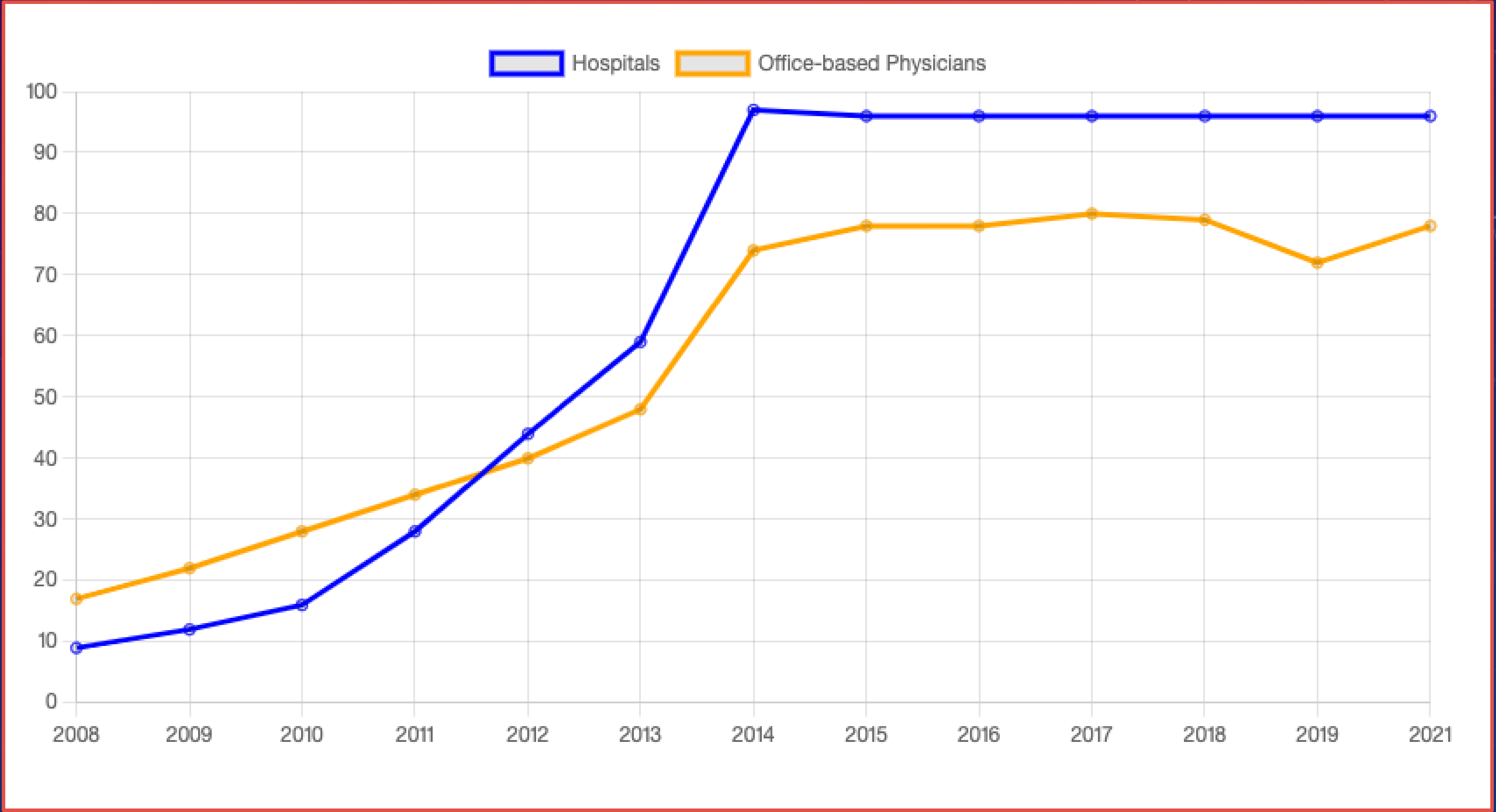
Justin Armstrong
Boston, MA

HISTORY

HOW DID WE GET HERE?

ADOPTION OF ELECTRONIC HEALTH RECORDS (EHR)

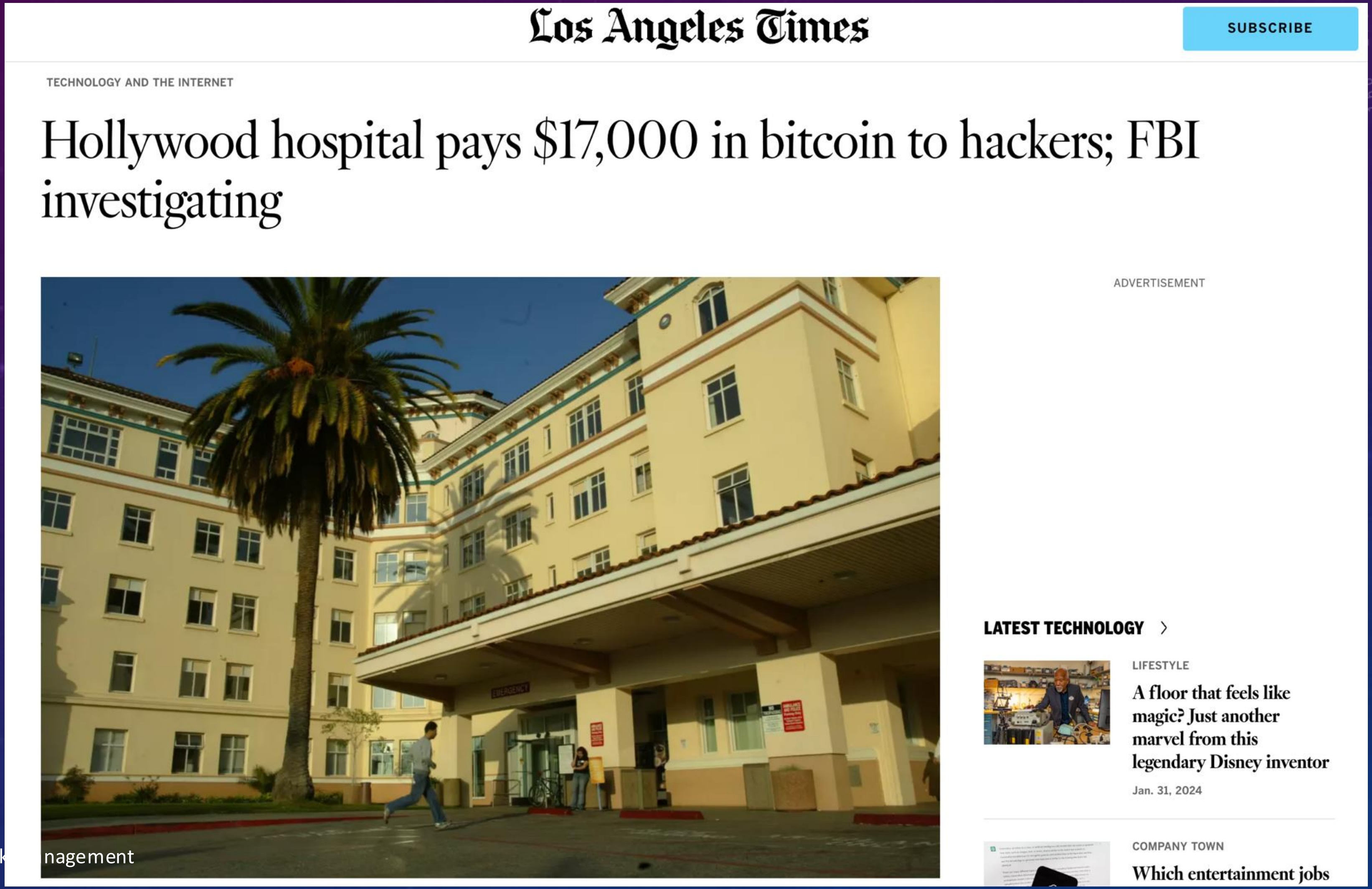
Photos by National Cancer Institute on Unsplash



https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records

2016 - RANSOMWARE IN HEALTHCARE BEGINS

2016: HOLLYWOOD PRESBYTERIAN HOSPITAL



Los Angeles Times

TECHNOLOGY AND THE INTERNET

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

LIFESTYLE

A floor that feels like magic? Just another marvel from this legendary Disney inventor

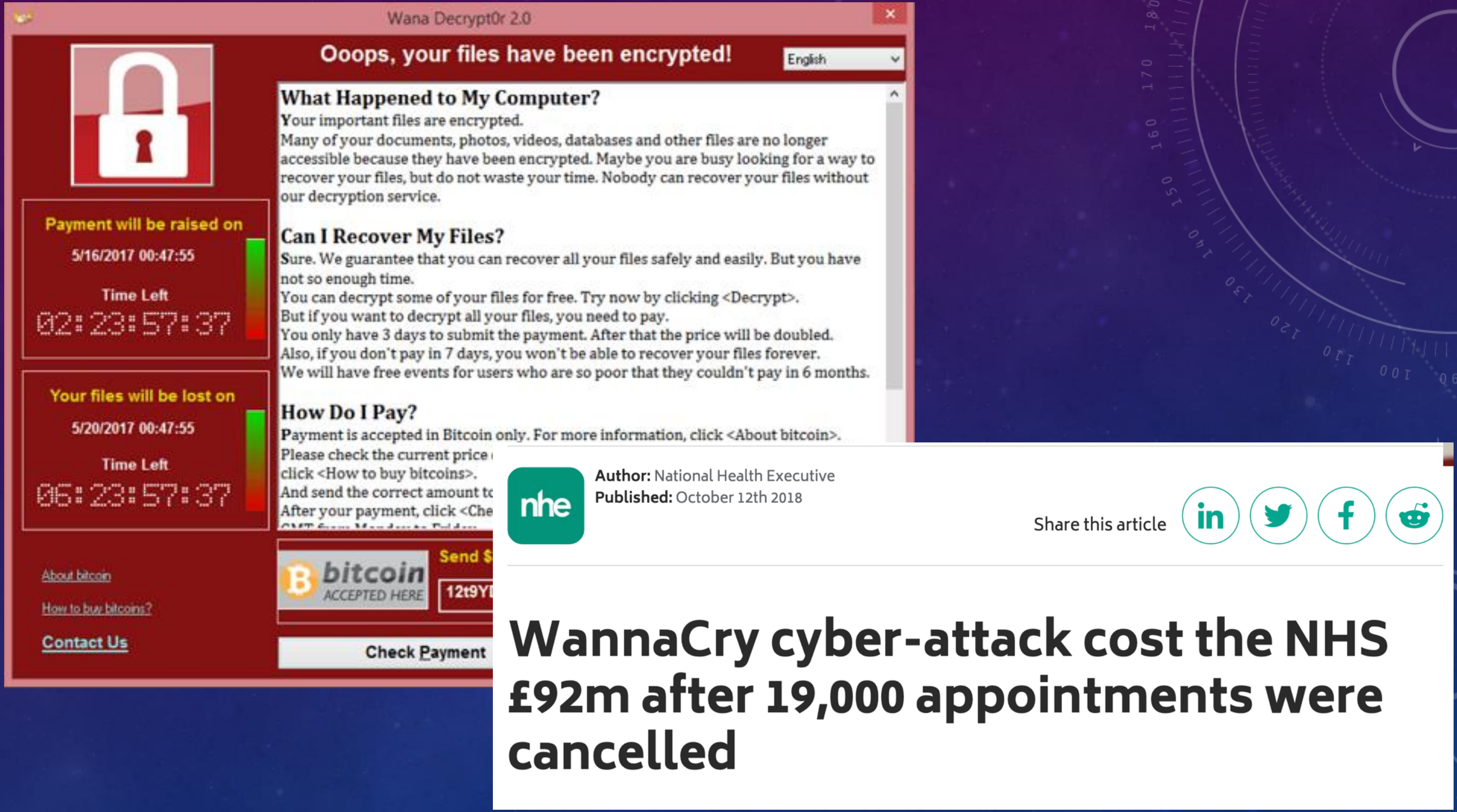
Jan. 31, 2024

COMPANY TOWN

Which entertainment jobs

https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

MAY 2017: WANNACRY - WORLDWIDE



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price
click <How to buy bitcoins>.
And send the correct amount to
After your payment, click <Che

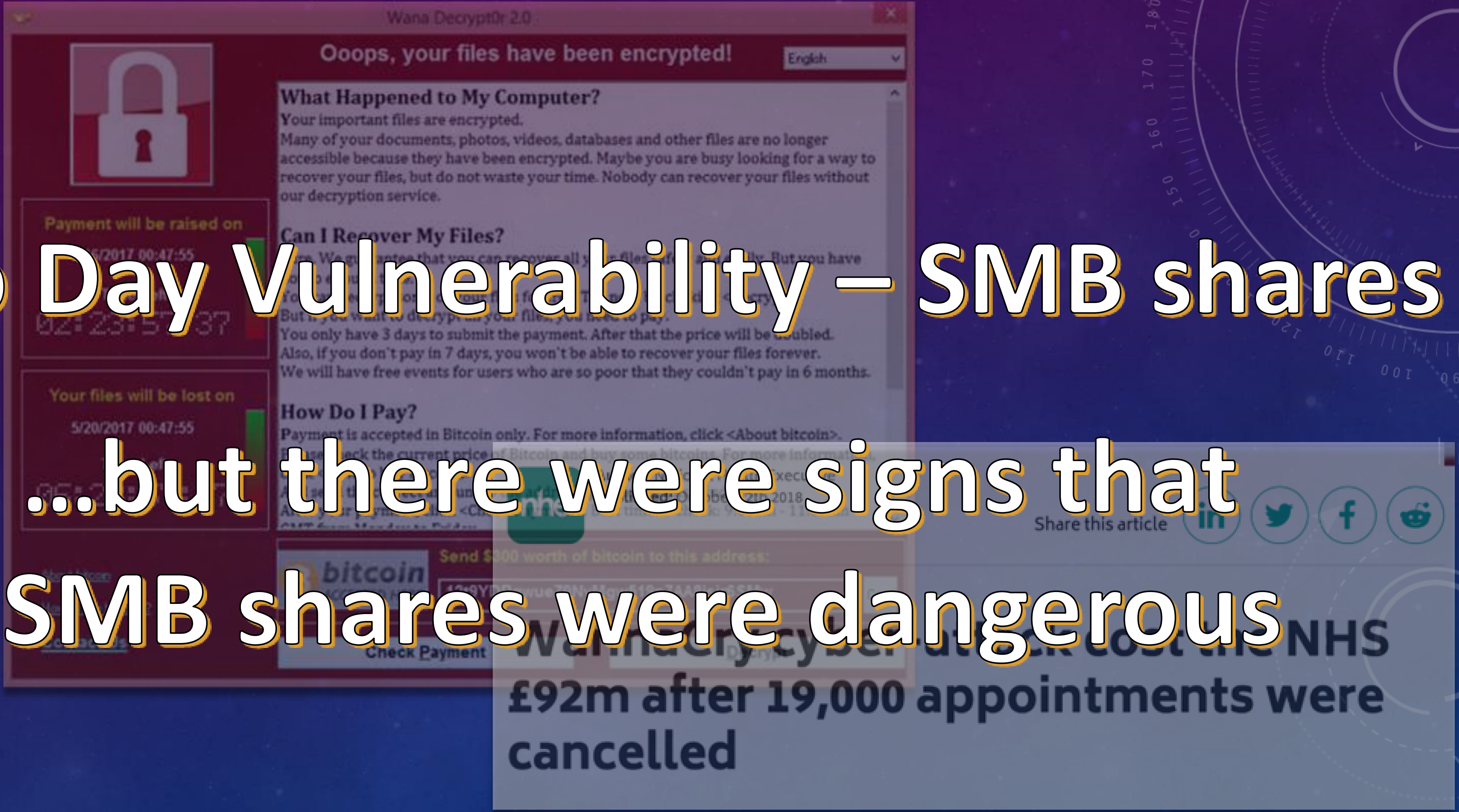
Author: National Health Executive
Published: October 12th 2018

WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled

(c) 2024 Armstrong Risk Management

By https://cdn.securelist.com/files/2017/05/wannacry_05.png Downloaded from :https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/, Fair use, https://en.wikipedia.org/w/index.php?curid=54032765

MAY 2017: WANNACRY - WORLDWIDE



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Payment will be raised on

Your files will be lost on

5/20/2017 00:47:55

Send $300 worth of bitcoin to this address:

Check Payment

WannaCry cyber attack cost the NHS £92m after 19,000 appointments were cancelled

Zero Day Vulnerability – SMB shares

…but there were signs that SMB shares were dangerous

(c) 2024 Armstrong Risk Management

By https://cdn.securelist.com/files/2017/05/wannacry_05.png Downloaded from :https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/, Fair use, https://en.wikipedia.org/w/index.php?curid=54032765

WANNACRY – NORTH KOREA (ANIMATION)

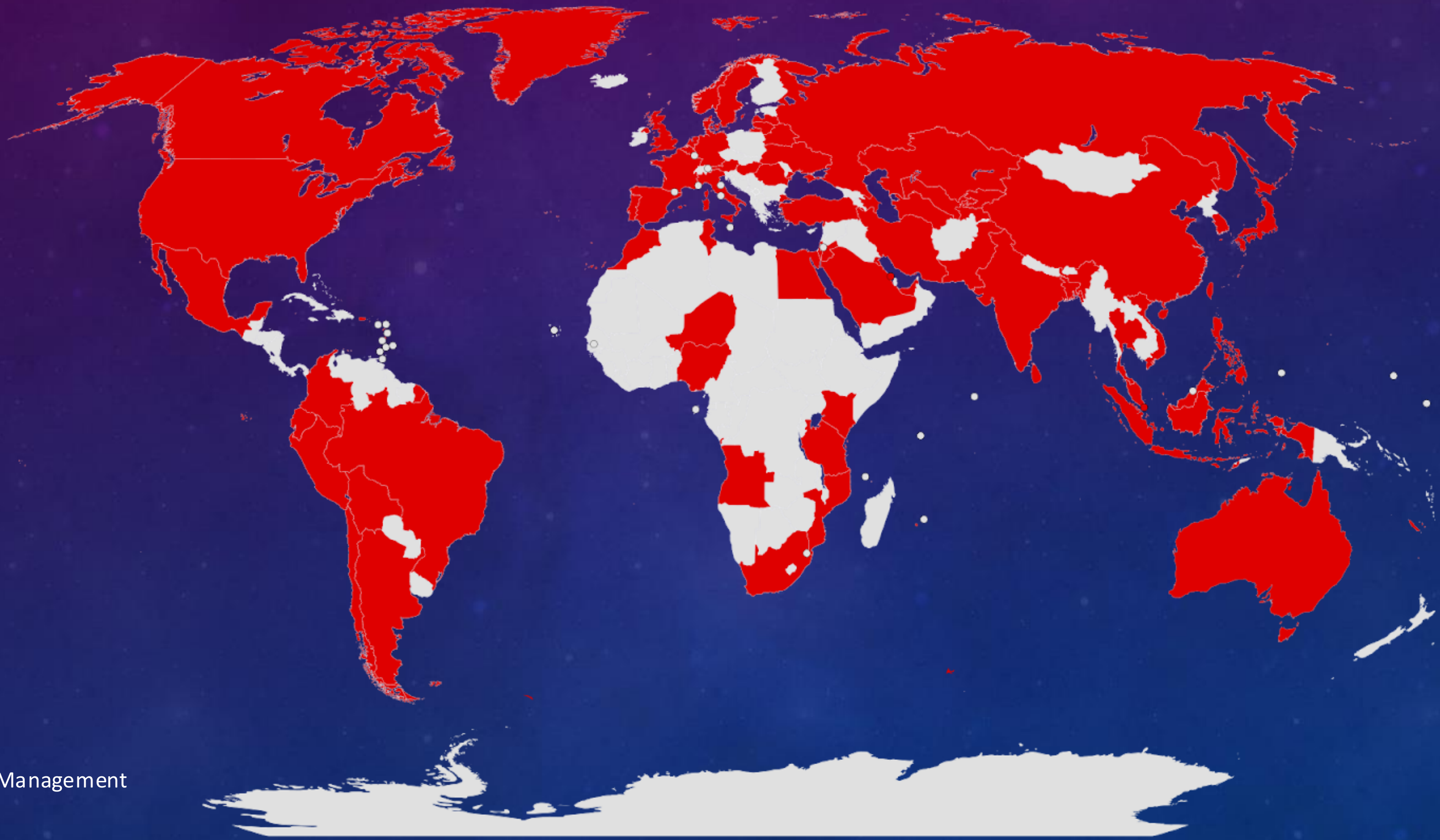
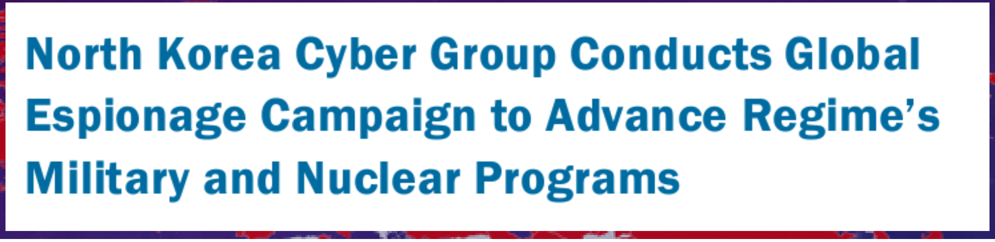
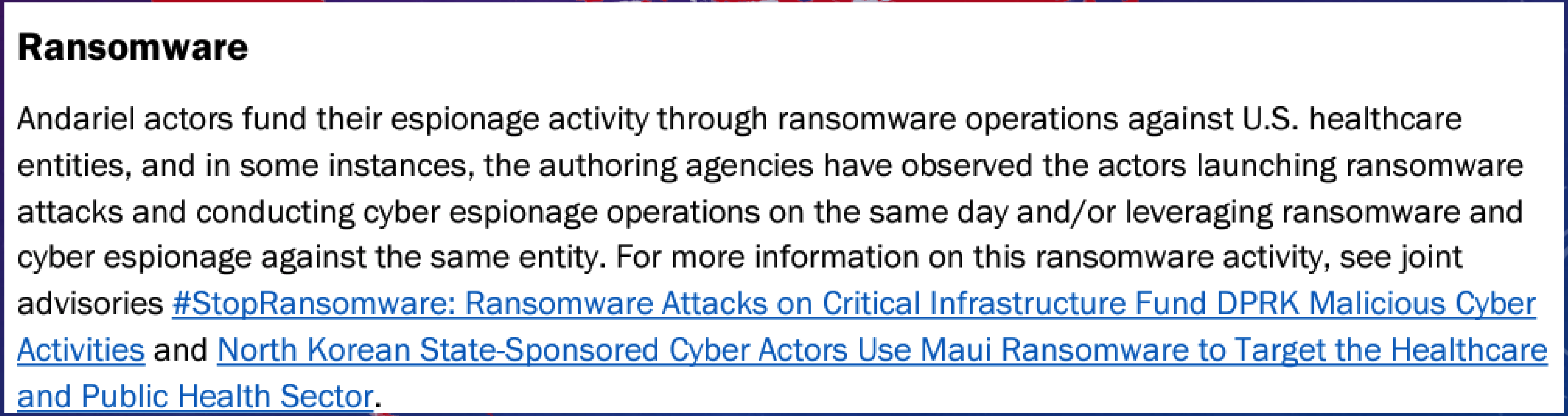


Image Courtesy of Wikimedia Commons, created by user Roke

NORTH KOREAN ACTIVITY *NOW!*



North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs

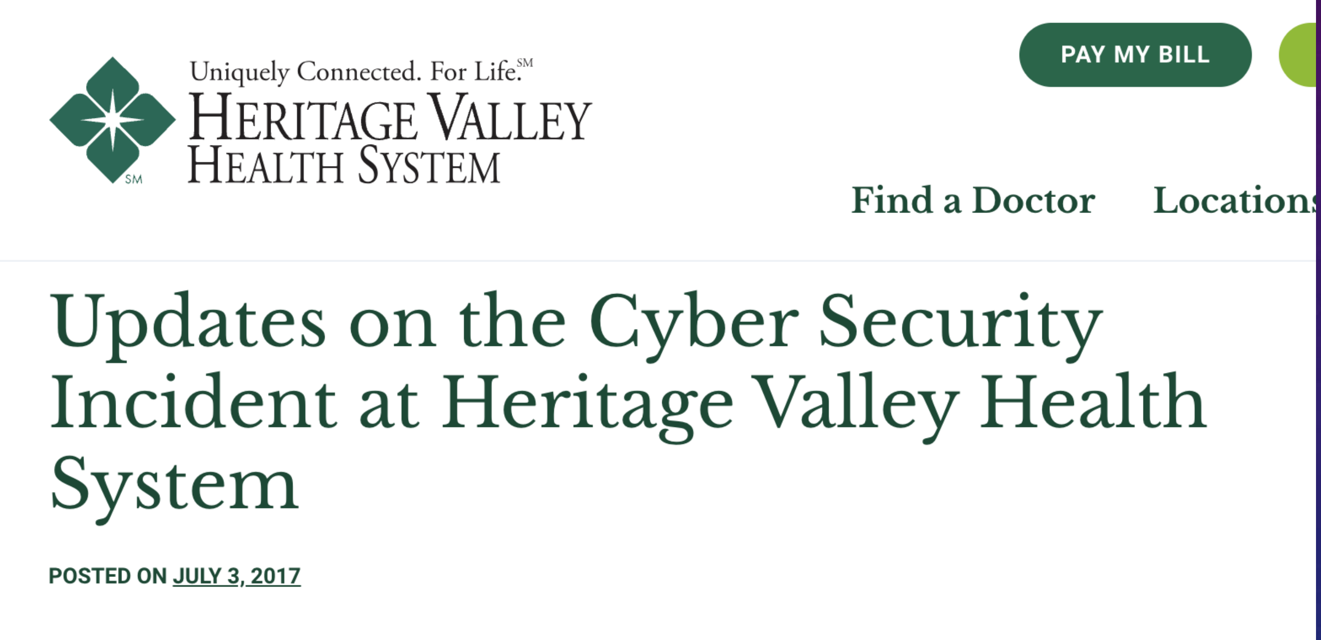


Ransomware

Andariel actors fund their espionage activity through ransomware operations against U.S. healthcare entities, and in some instances, the authoring agencies have observed the actors launching ransomware attacks and conducting cyber espionage operations on the same day and/or leveraging ransomware and cyber espionage against the same entity. For more information on this ransomware activity, see joint advisories #StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities and North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.

Image Courtesy of Wikimedia Commons, created by user Roke

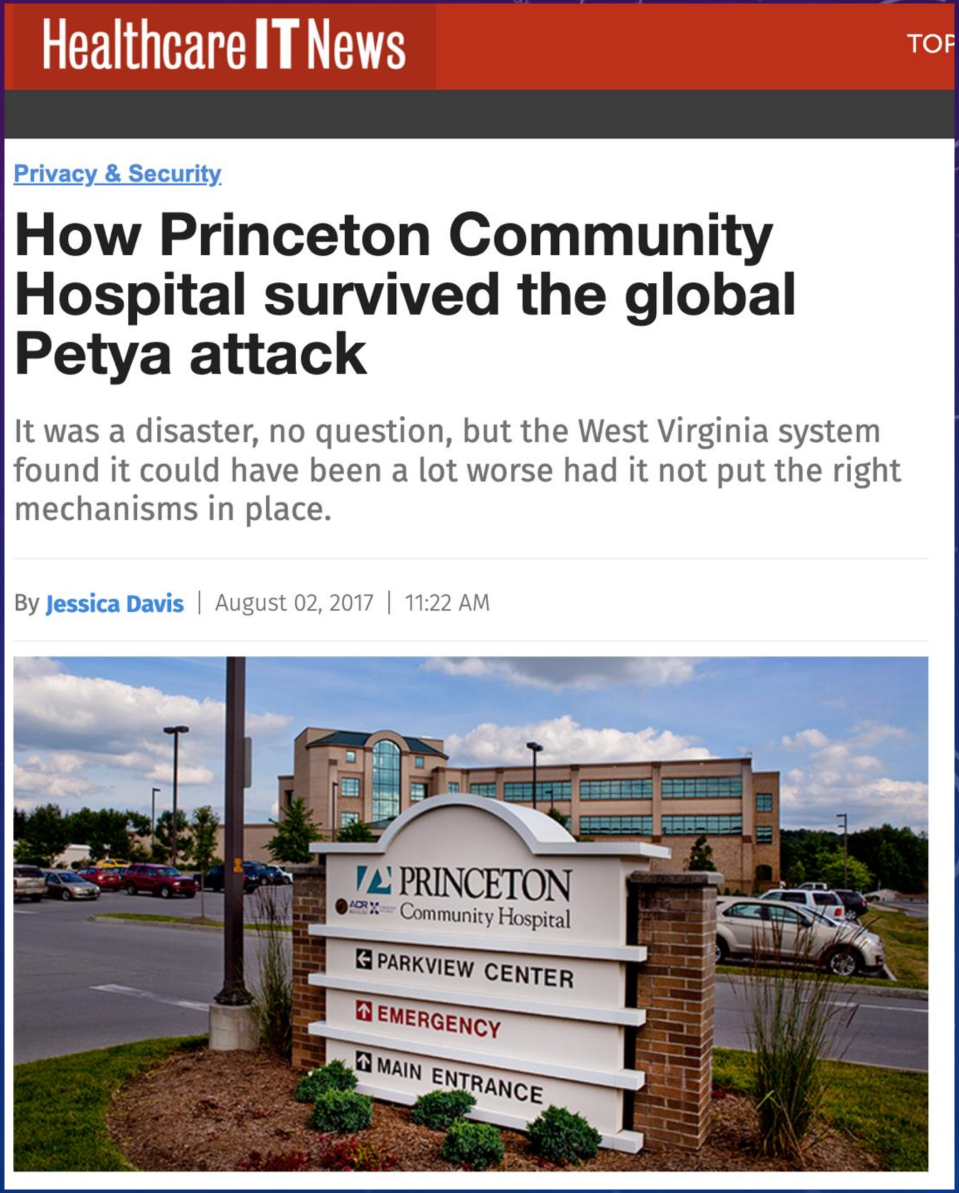
JUNE 2017: NOTPETYA - WORLDWIDE



Updates on the Cyber Security Incident at Heritage Valley Health System

POSTED ON JULY 3, 2017

https://www.heritagevalley.org/news/updates-on-the-cyber-security-incident-at-heritage-valley-health-system/



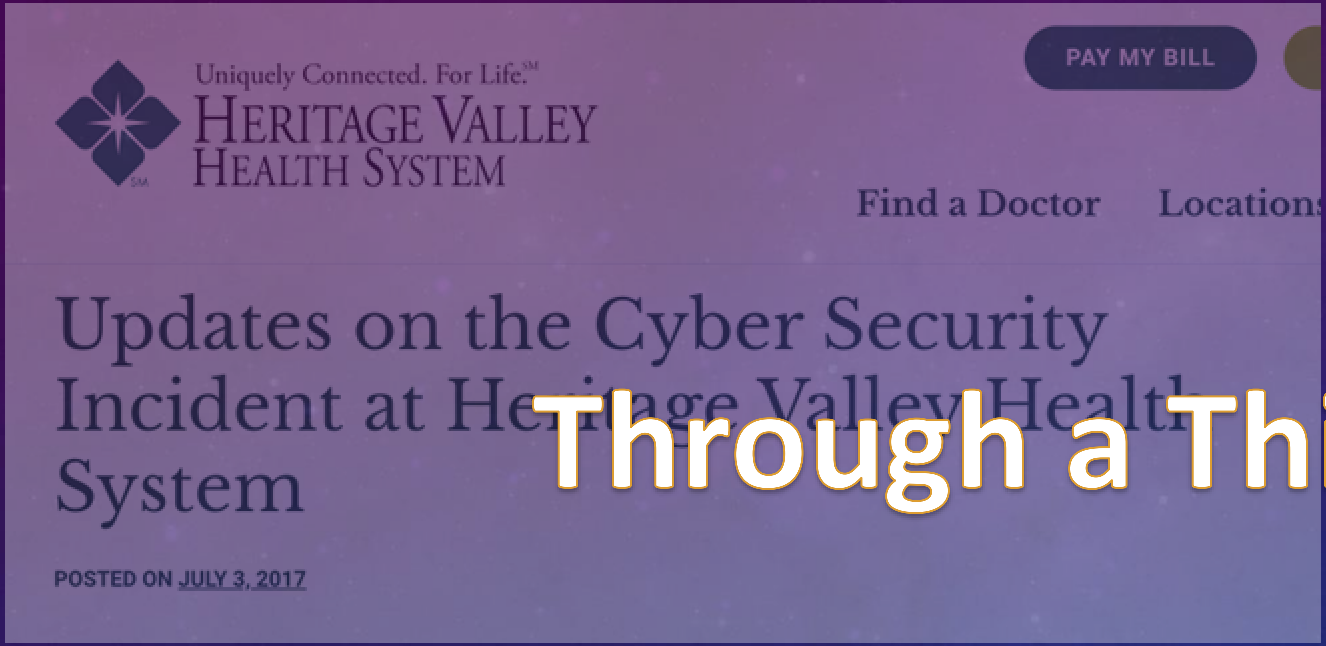
How Princeton Community Hospital survived the global Petya attack

It was a disaster, no question, but the West Virginia system found it could have been a lot worse had it not put the right mechanisms in place.

By Jessica Davis | August 02, 2017 | 11:22 AM

https://www.healthcareitnews.com/news/how-princeton-community-hospital-survived-global-petya-attack

JUNE 2017: NOTPETYA - WORLDWIDE



Uniquely Connected. For Life.SM

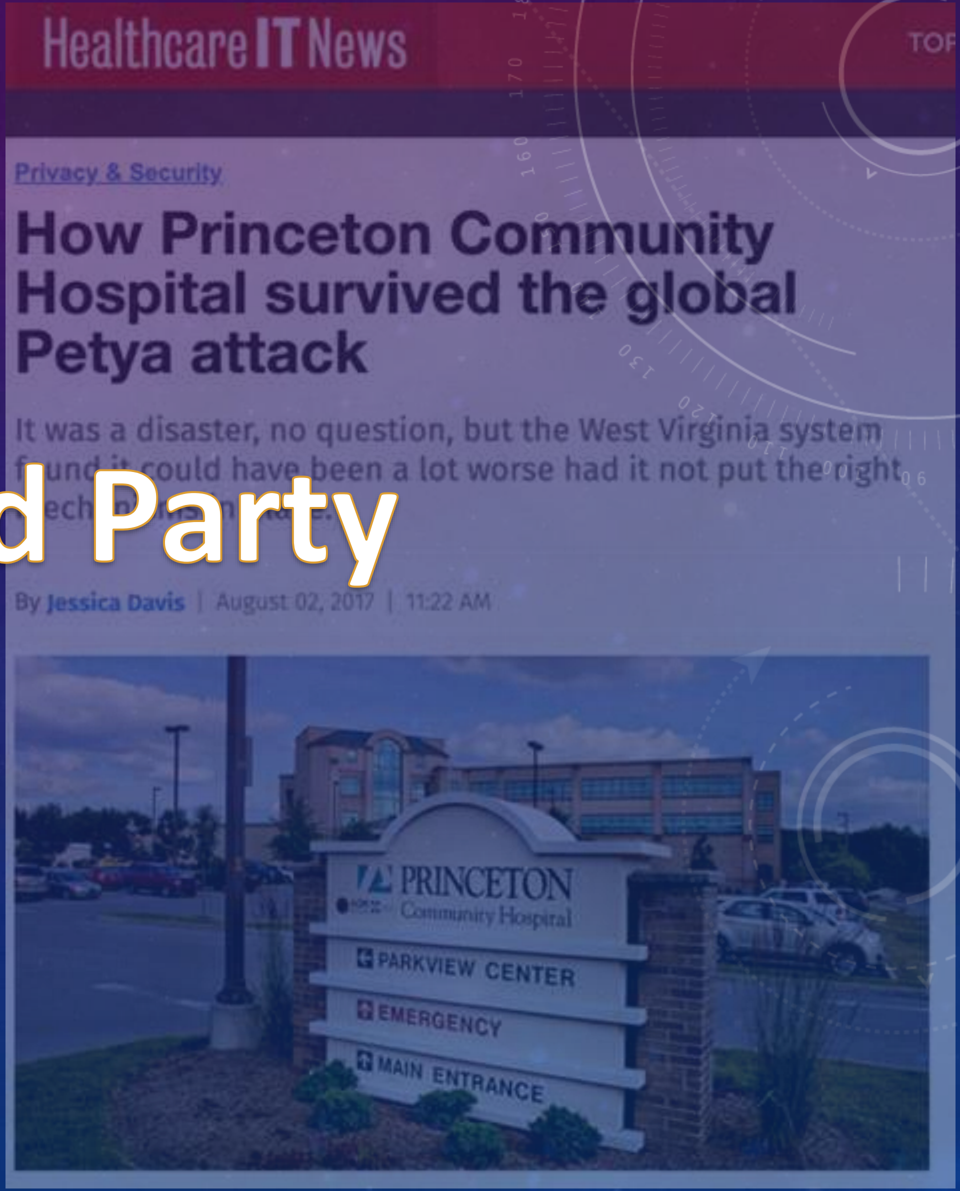
HERITAGE VALLEY HEALTH SYSTEM

Updates on the Cyber Security Incident at Heritage Valley Health System

POSTED ON JULY 3, 2017

https://www.heritagevalley.org/news/updates-on-the-cyber-security-incident-at-heritage-valley-health-system/

Through a Third Party



Privacy & Security

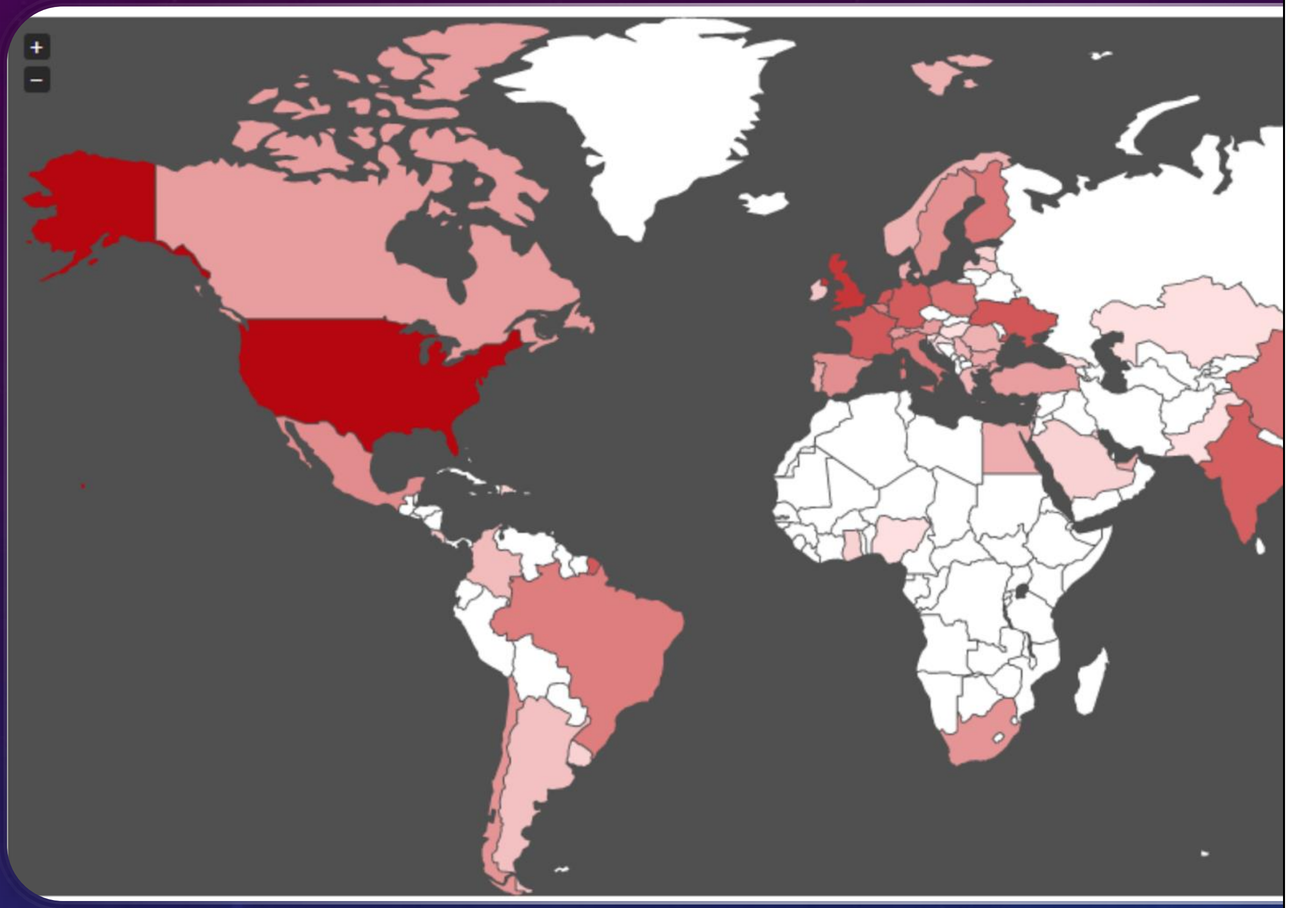
How Princeton Community Hospital survived the global Petya attack

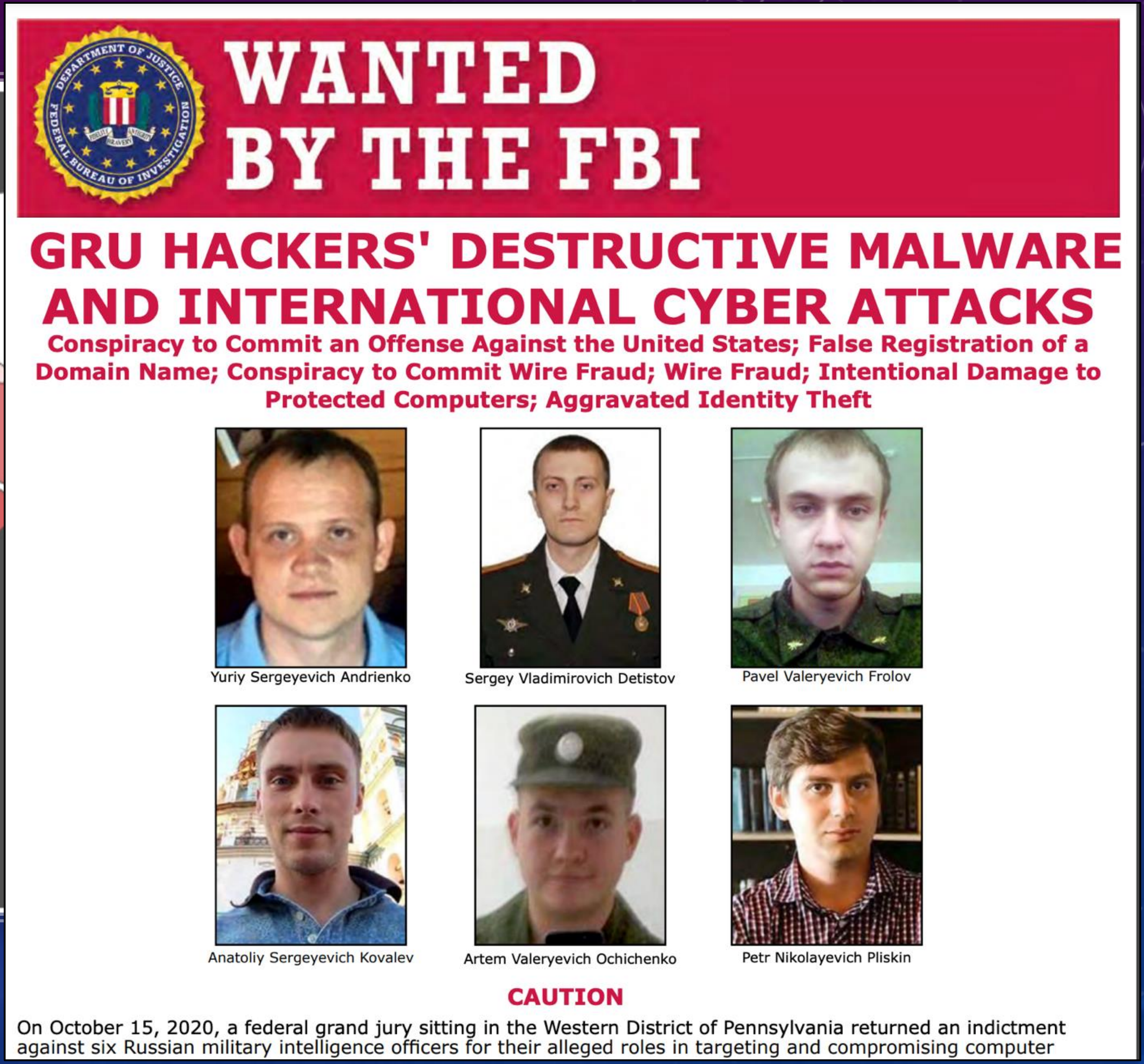
It was a disaster, no question, but the West Virginia system found it could have been a lot worse had it not put the right mechanisms in place.

By Jessica Davis | August 02, 2017 | 11:22 AM

https://www.healthcareitnews.com/news/how-princeton-community-hospital-survived-global-petya-attack

WHO ARE THE THREAT ACTORS?





WANTED BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

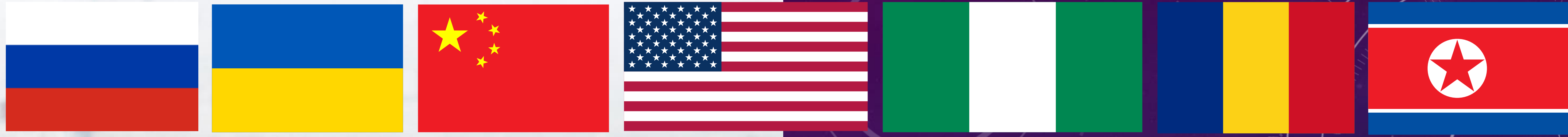
Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

CAUTION

On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers for their alleged roles in targeting and compromising computer

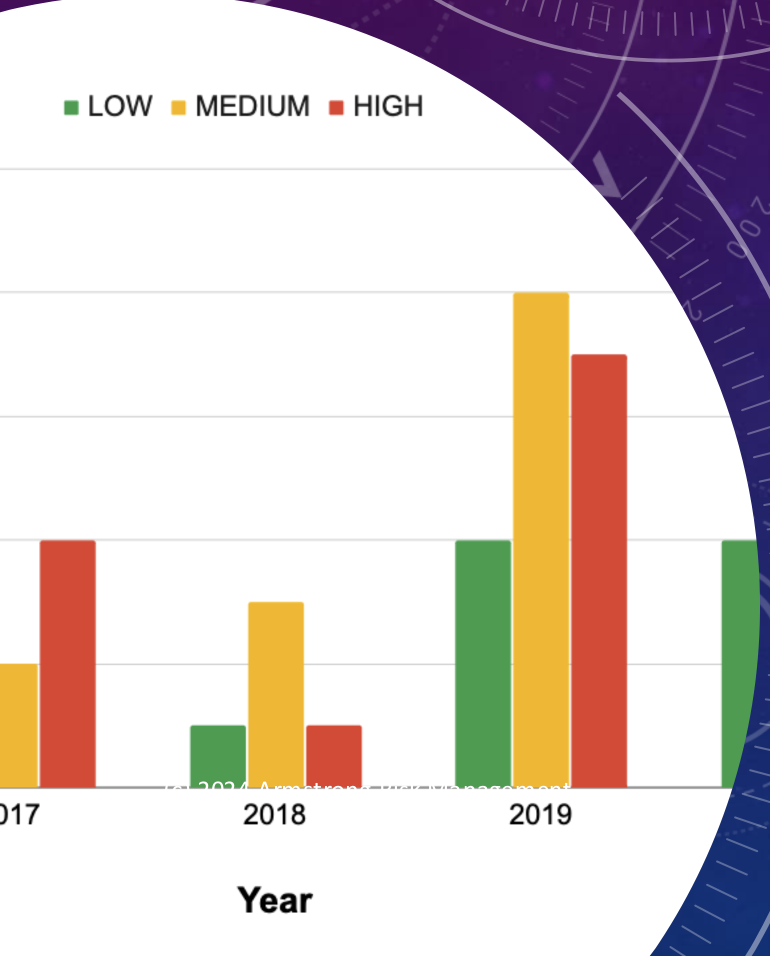
https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks



CRIMINAL ACTIVITY AS WELL

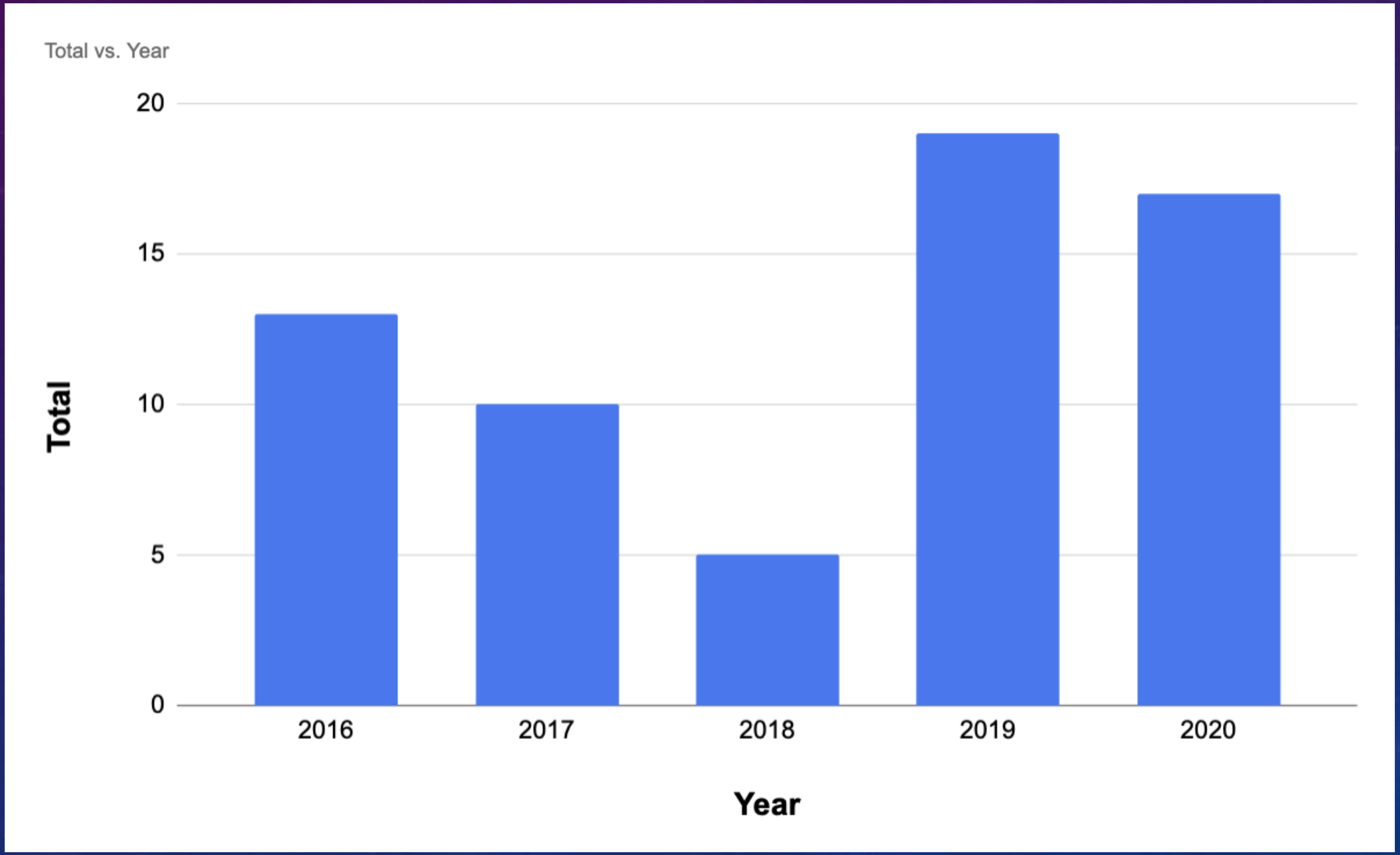
HOW BIG IS THE RISK?

?



Not easy to get good Statistics

THE ESCALATION OF RANSOMWARE



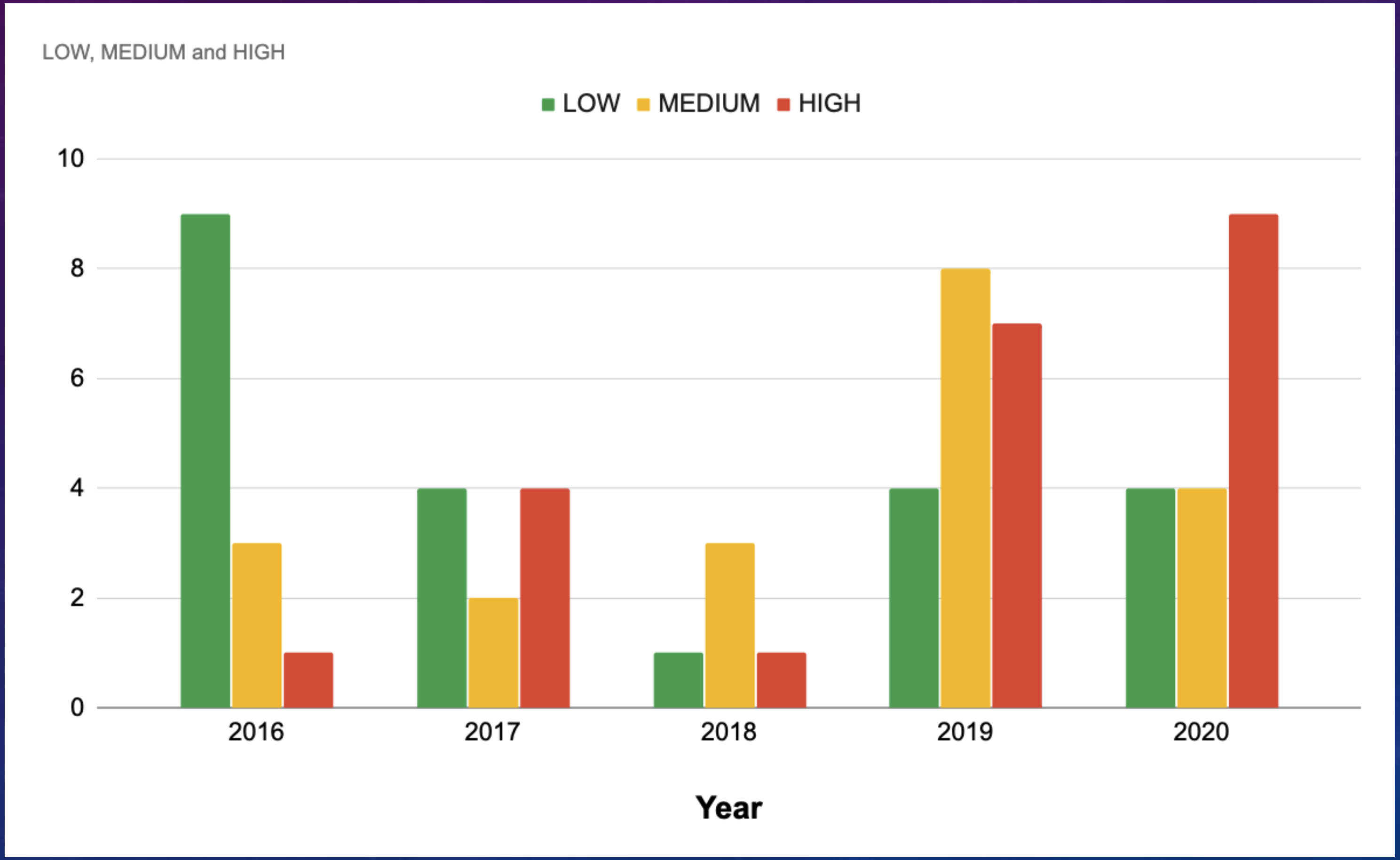
THE ESCALATION OF RANSOMWARE

Recovery Time

Low <1 day

Medium 2-7 days

High >1 week



2020

1%

THE ESCALATION OF RANSOMWARE

Office of the Director of National Intelligence provided this report:
Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double

“In the US, attacks against the healthcare sector were up 128 percent, with 258 victims in 2023 versus 113 in 2022.”

More than doubled in the U.S.! This represents 4% of the 6,120 Hospitals.

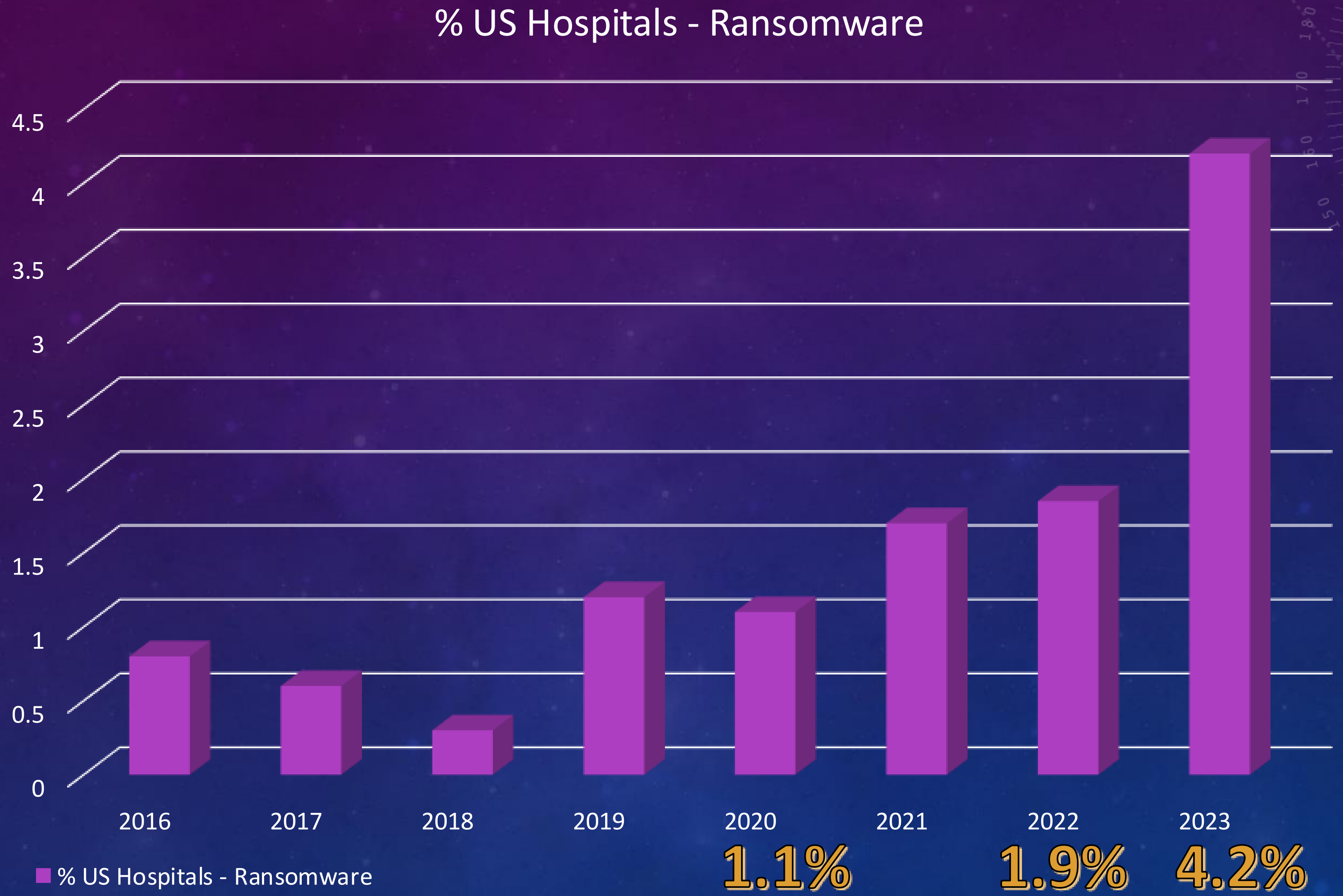
2023

4%

Photo by Ivan Dražić, at Pexels

https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

ESCALATION IN RANSOMWARE 2016-2024



1.1% 1.9% 4.2%

(c) 2024 Armstrong Risk Management

HOW DO THEY DO IT?

BLACK BASTA RANSOMWARE

- *Spear* phishing
- BITSAdmin
- Cobalt Strike
- Remote Access Tools
  - PSExec
  - ScreenConnect
  - Remote Desktop
- Powershell

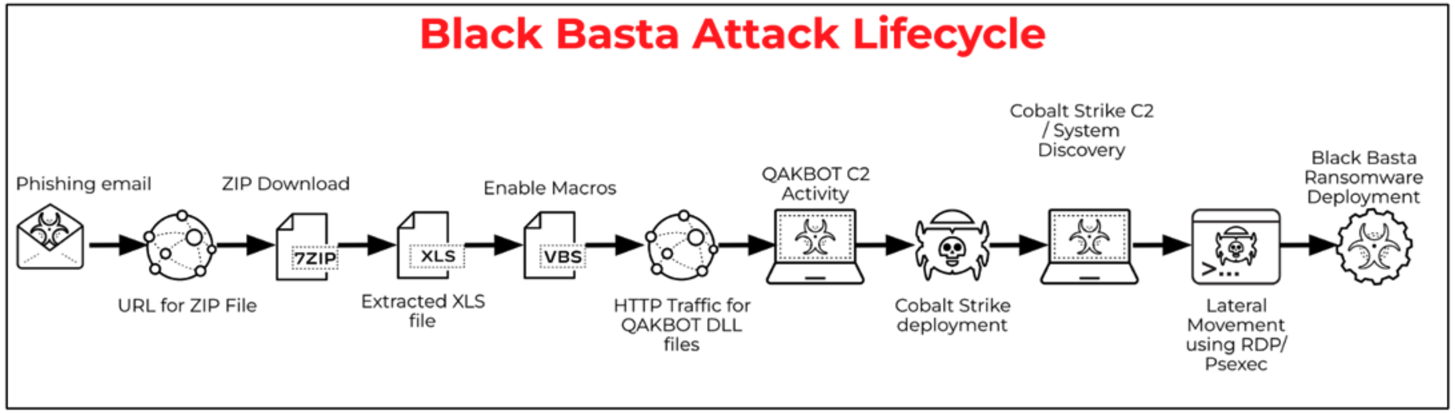

Black Basta Attack Lifecycle
Phishing email
URL for ZIP File
ZIP Download
7ZIP
XLS
Extracted XLS file
Enable Macros
VBS
HTTP Traffic for QAKBOT DLL files
QAKBOT C2 Activity
Cobalt Strike deployment
Cobalt Strike C2 / System Discovery
Lateral Movement using RDP/ Psexec
Black Basta Ransomware Deployment

Figure 2: Standard Attack Lifecycle Observed with Black Basta ransomware. *(Unit 42 Graphic)*

HOW RANSOMWARE IS DEPLOYED

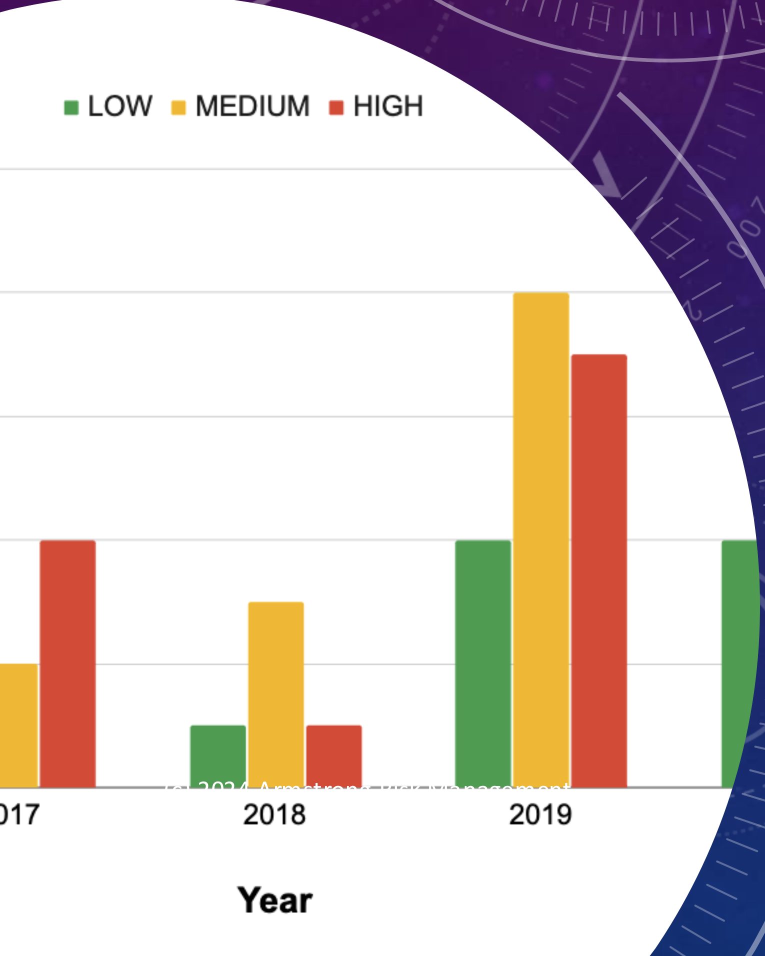
Ransomware is “noisy” – quickly detected!

Activated across all computers, all at once.

- Often at midnight
- Often on the weekend or on a holiday
- It rapidly encrypts pieces of files

(c) 2024 Armstrong Risk Management

Photo by Anne Nygård on Unsplash



- Escalation in **number** and **impact**
- Increasing Sophistication
- Incident Response is Complex

PATIENT SAFETY

CYBERSECURITY IS PATIENT SAFETY

Cynergistek's 2018 Report on Cybersecurity Findings in Healthcare — Impact on Patient Care:

*"**Increased medical errors** as downtime procedures are initiated on paper, making it more difficult to communicate changes to the patient's condition or to calculate appropriate drug dosages"*

CYBERSECURITY IS PATIENT SAFETY

Cynergistek's 2018 Report on Cybersecurity Findings in Healthcare — Impact on Patient Care:

*"**Increased stress on staff** operating in the more chaotic environment."*

(c) 2024 Armstrong Risk Management

CYBERSECURITY IS PATIENT SAFETY

Cynergistek's 2018 Report on Cybersecurity Findings in Healthcare — Impact on Patient Care:

*"**Increased risk of staff cutting corners** as they are asked to do work in a less efficient manner which increases compliance risks"*

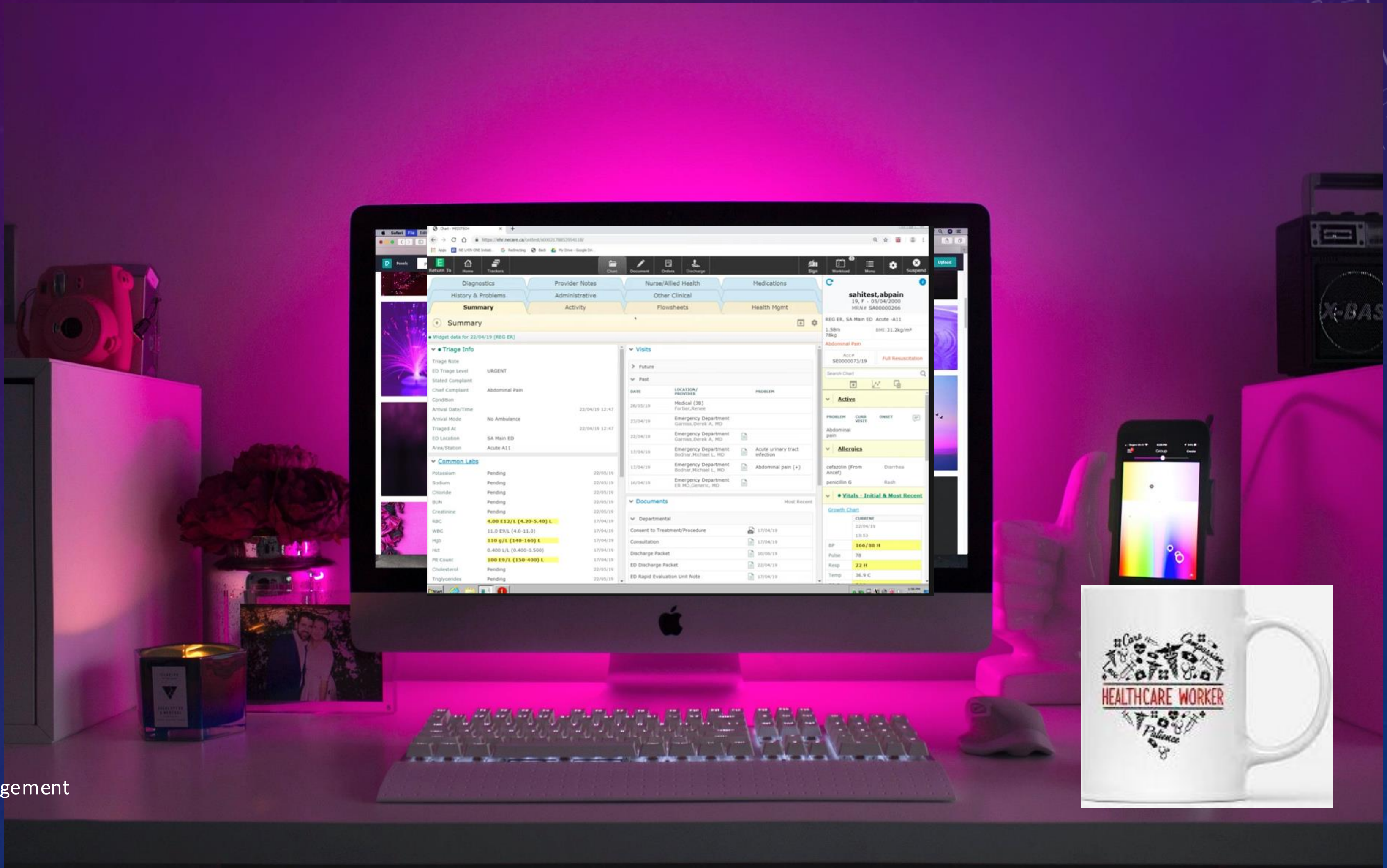
HEALTH OF THE HOSPITAL

Cynergistek's 2018 Report on Cybersecurity Findings in Healthcare — Financial Impact:

- ***Cancelling elective services*** *because systems are down which will result in a reduction in Revenue*
- ***Increased time lag to get charges submitted*** *which will lead to a lag in payment having implications on cash flow*
- ***Increased unanticipated cost to recover*** *from the data incident, provide notification to impacted individuals and hire external parties to assist*

CONTROVERSIAL QUESTION

TO PAY OR NOT TO PAY



Diagnostics | Provider Notes | Nurse/Allied Health | Medications
History & Problems | Administrative | Other Clinical
Summary | Activity | Flowsheets | Health Mgmt

Summary

Widget data for 22/04/19 (REG ER)

Triage Info

Triage Note		
ED Triage Level	URGENT	
Stated Complaint		
Chief Complaint	Abdominal Pain	
Condition		
Arrival Date/Time		22/04/19 12:47
Arrival Mode	No Ambulance	
Triaged At		22/04/19 12:47
ED Location	SA Main ED	
Area/Station	Acute A11	

Common Labs

Potassium	Pending	22/05/19
Sodium	Pending	22/05/19
Chloride	Pending	22/05/19
BUN	Pending	22/05/19
Creatinine	Pending	22/05/19
RBC	4.00 E12/L (4.20-5.40) L	17/04/19
WBC	11.0 E9/L (4.0-11.0)	17/04/19
Hgb	110 g/L (140-160) L	17/04/19
Hct	0.400 L/L (0.400-0.500)	17/04/19
Plt Count	100 E9/L (150-400) L	17/04/19
Cholesterol	Pending	22/05/19
Triglycerides	Pending	22/05/19

Visits

Future

Past

DATE	LOCATION/ PROVIDER	PROBLEM
28/05/19	Medical (3B) Fortier,Renee	
23/04/19	Emergency Department Garniss,Derek A, MD	
22/04/19	Emergency Department Garniss,Derek A, MD	
17/04/19	Emergency Department Bodnar,Michael L, MD	Acute urinary tract infection
17/04/19	Emergency Department Bodnar,Michael L, MD	Abdominal pain (+)
16/04/19	Emergency Department ER MD,Generic, MD	

Documents — Most Recent

Departmental

Consent to Treatment/Procedure	17/04/19
Consultation	17/04/19
Discharge Packet	10/06/19
ED Discharge Packet	22/04/19
ED Rapid Evaluation Unit Note	17/04/19

sahitest,abpain
19, F - 05/04/2000
MRN# SA00000266
REG ER, SA Main ED Acute -A11
1.58m 78kg BMI: 31.2kg/m²
Abdominal Pain
Acc# SE0000073/19
Full Resuscitation

Active

PROBLEM	CURR VISIT	ONSET
Abdominal pain		

Allergies

cefazolin (From Ancef)	Diarrhea
penicillin G	Rash

Vitals - Initial & Most Recent

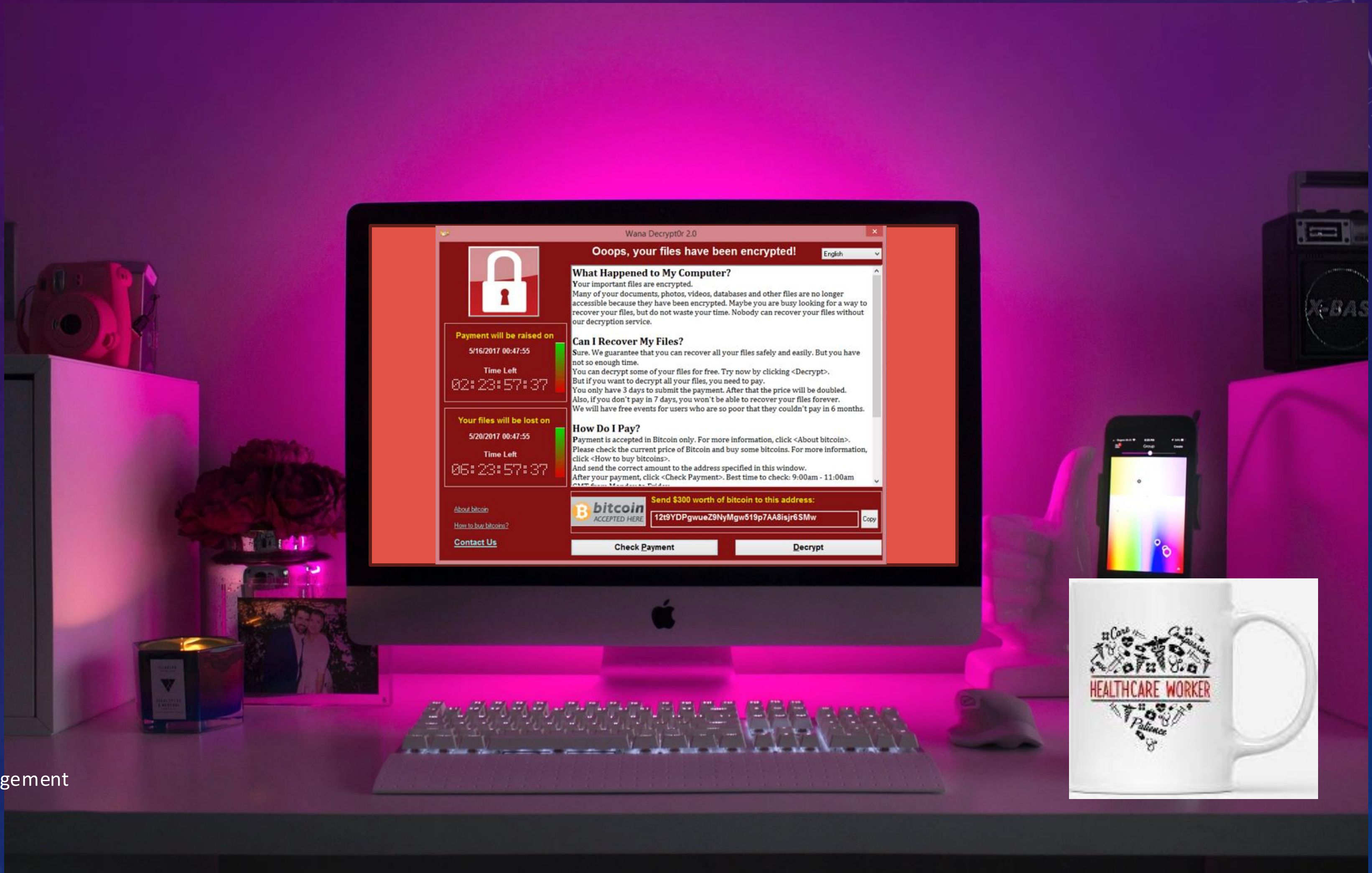
Growth Chart

	CURRENT 22/04/19 13:53
BP	166/88 H
Pulse	78
Resp	22 H
Temp	36.9 C

(c) 2024 Armstrong Risk Management

Photo by Designecologist: https://www.pexels.com/photo/silver-imac-displaying-collage-photos-1779487/

TO PAY OR NOT TO PAY – THE PROS AND CONS



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Photo by Designecologist: https://www.pexels.com/photo/silver-imac-displaying-collage-photos-1779487/

TO PAY OR NOT TO PAY

Funds

- Criminals
- Terrorism
- Failed States

Possibly Illegal

Photo by Fred Moon on Unsplash

Photo by Mati Mango on Pexels

TO PAY OR NOT TO PAY

Encourages attacks

- On your organization
- On others

Photo by Brock Wegner on Unsplash

TO PAY OR NOT TO PAY

Does it even work?

- Database corruption
- Out of Synch
- It takes a long time

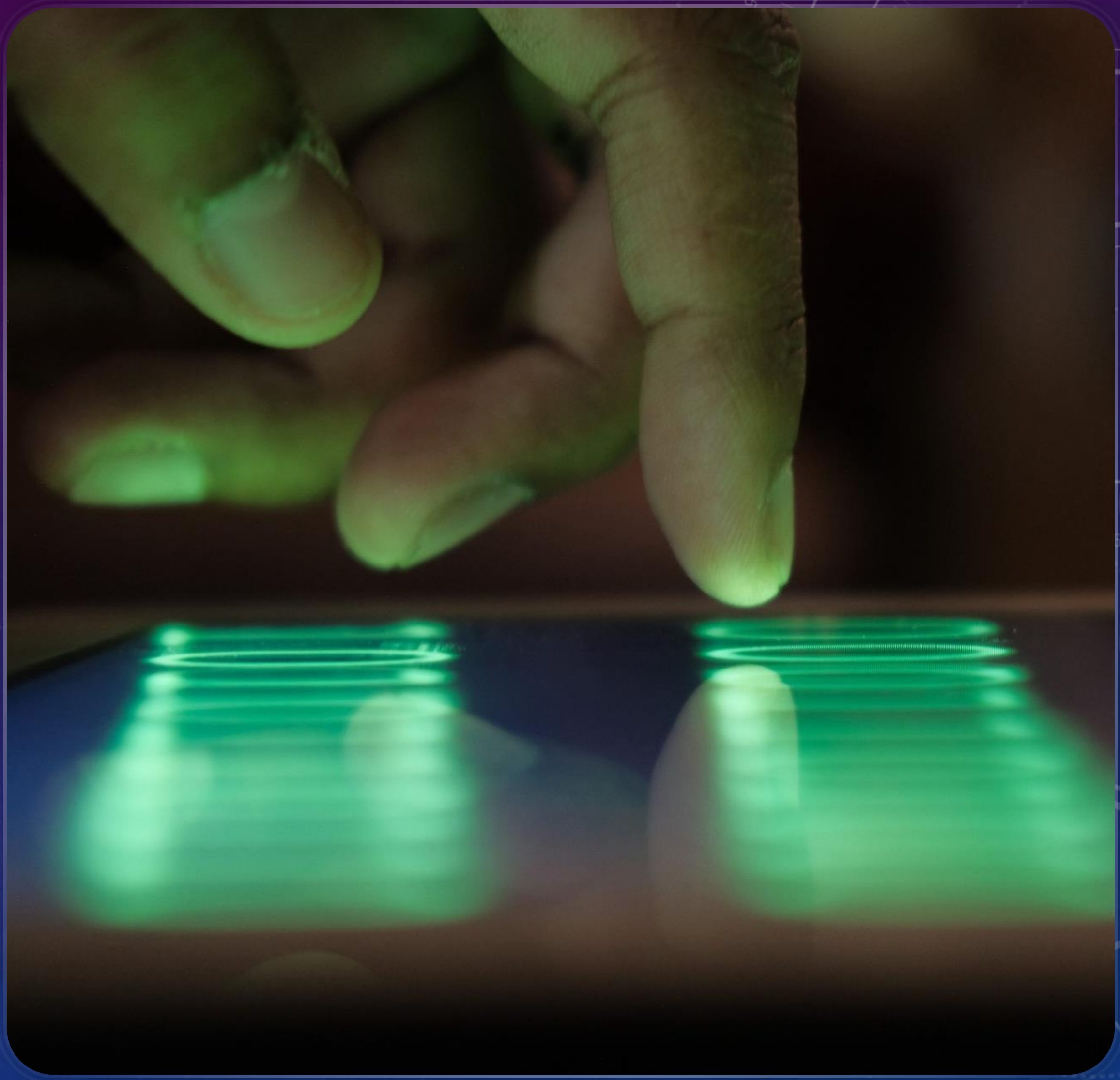
Photo by Chris Liverani on Unsplash

(c) 2024 Armstrong Risk Management

Photo by ammar sabaa on Unsplash

WAR STORIES

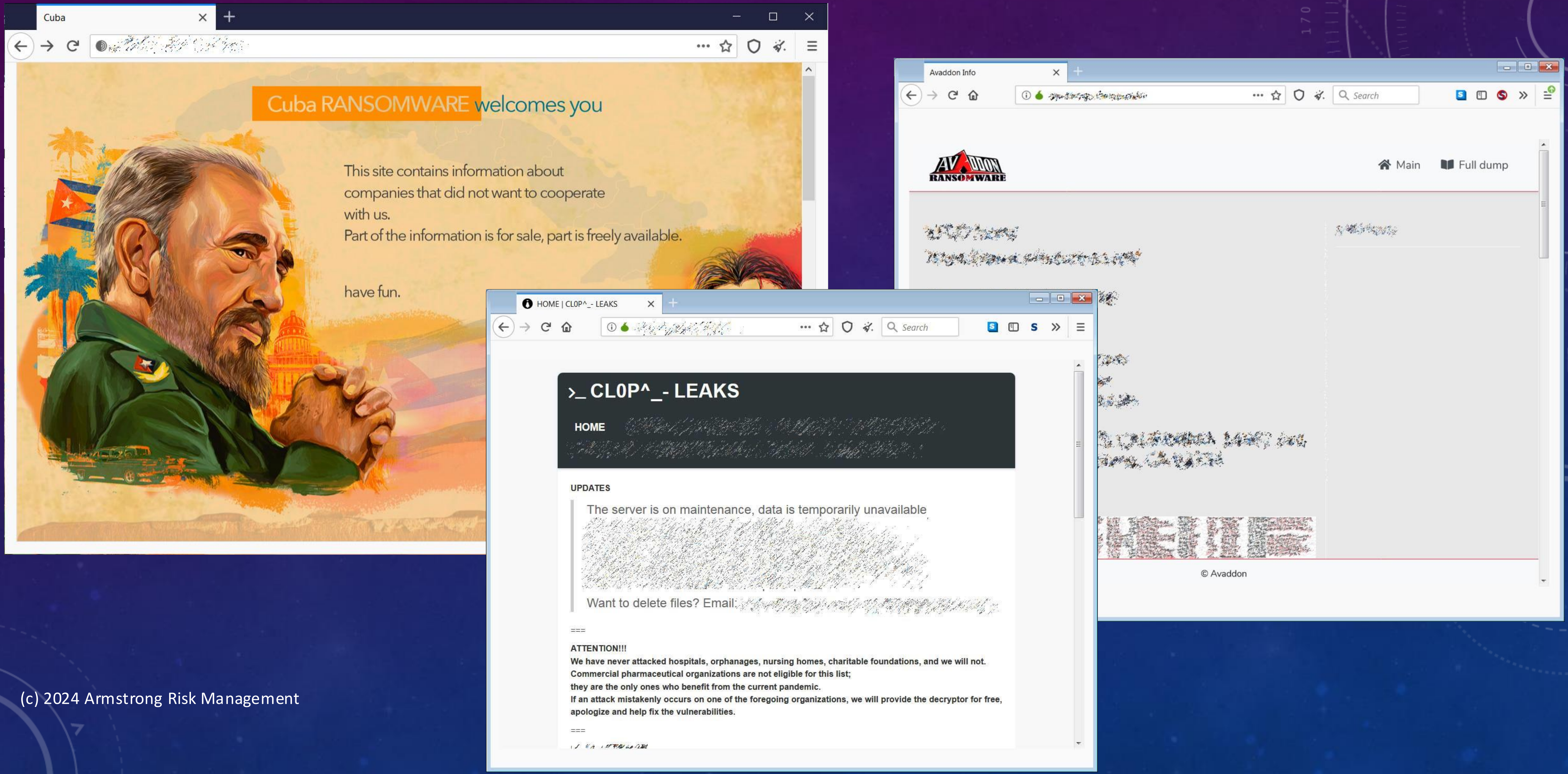
- Who do we call?
- Files out of synch, corrupted
- Paid the ransom – but FAL issue
- Antivirus deleted essential files
- Ransomware + Insider Threat
- Rush to Restore, is it a breach?   /



(c) 2024 Armstrong Risk Management

WHAT PRESURES CAN A HACKER PUT ON YOUR ORGANIZATION TO PAY?

PRESSURES – DATA EXFILTRATION



Cuba RANSOMWARE welcomes you

This site contains information about companies that did not want to cooperate with us.
Part of the information is for sale, part is freely available.

have fun.

[redacted]

© Avaddon

>_ CL0P^_- LEAKS

HOME [redacted]

UPDATES

> The server is on maintenance, data is temporarily unavailable
>
> [redacted]
>
> Want to delete files? Email: [redacted]

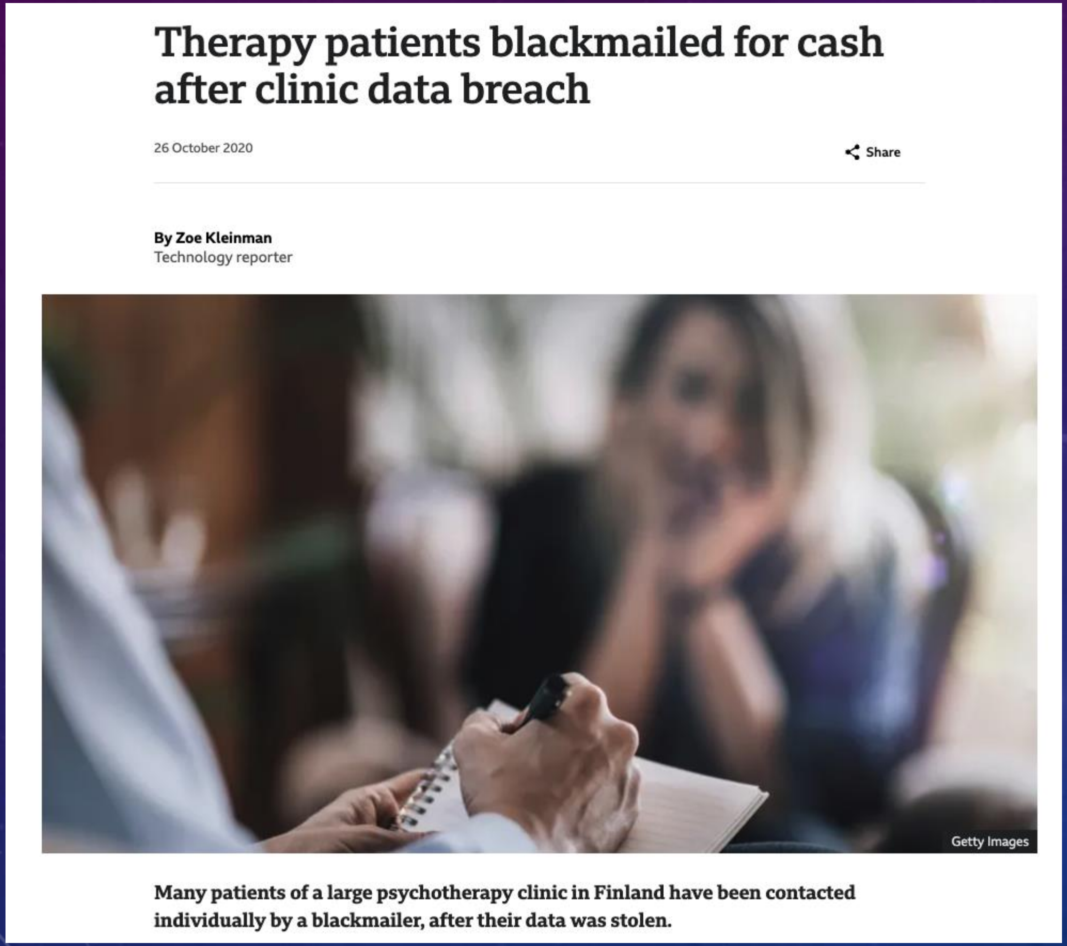
===

ATTENTION!!!
We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not.
Commercial pharmaceutical organizations are not eligible for this list;
they are the only ones who benefit from the current pandemic.
If an attack mistakenly occurs on one of the foregoing organizations, we will provide the decryptor for free, apologize and help fix the vulnerabilities.

===

https://www.bleepingcomputer.com/news/security/list-of-ransomware-that-leaks-victims-stolen-files-if-not-paid/

PRESSURES - SHAMING



Therapy patients blackmailed for cash after clinic data breach

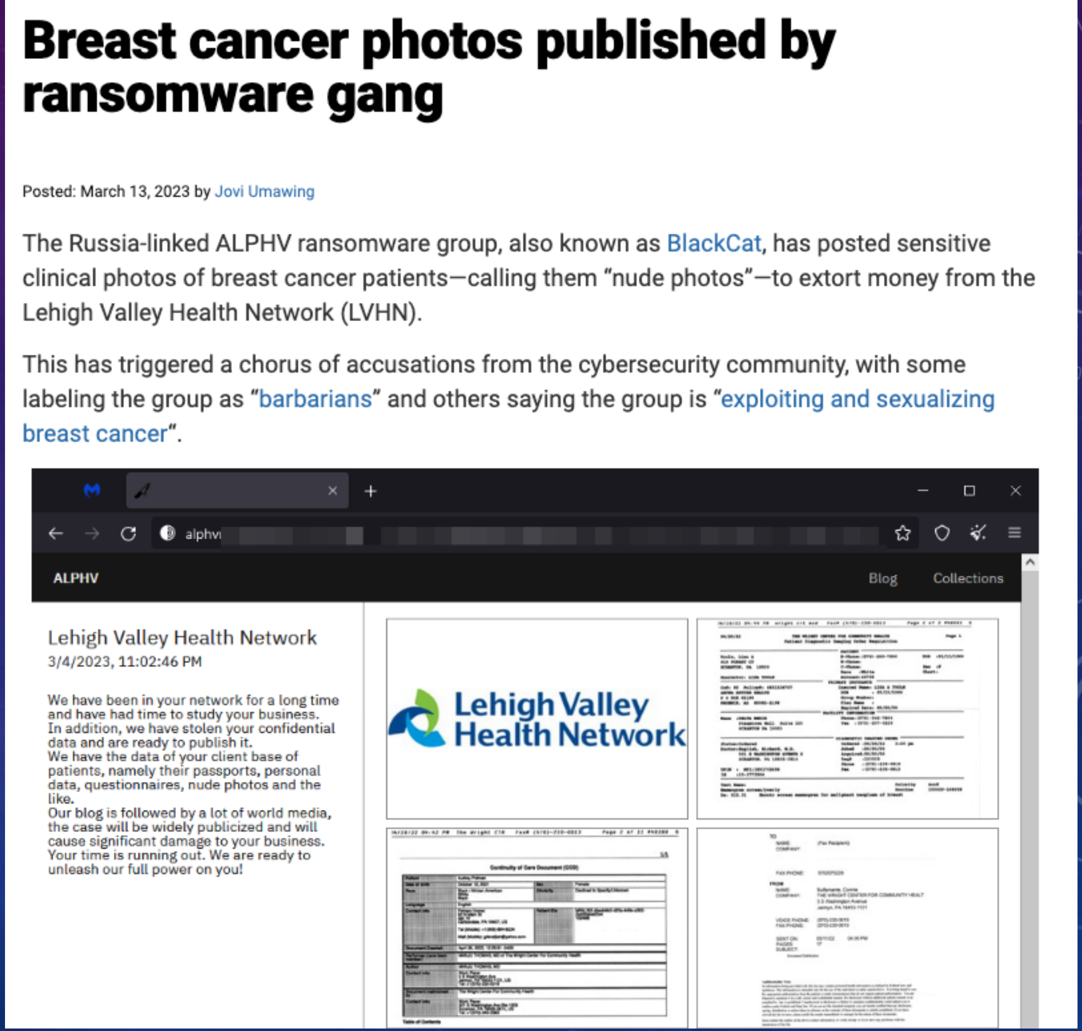
26 October 2020

By Zoe Kleinman
Technology reporter

Getty Images

Many patients of a large psychotherapy clinic in Finland have been contacted individually by a blackmailer, after their data was stolen.

https://www.bbc.com/news/technology-54692120



Breast cancer photos published by ransomware gang

Posted: March 13, 2023 by Jovi Umawing

The Russia-linked ALPHV ransomware group, also known as BlackCat, has posted sensitive clinical photos of breast cancer patients—calling them "nude photos"—to extort money from the Lehigh Valley Health Network (LVHN).

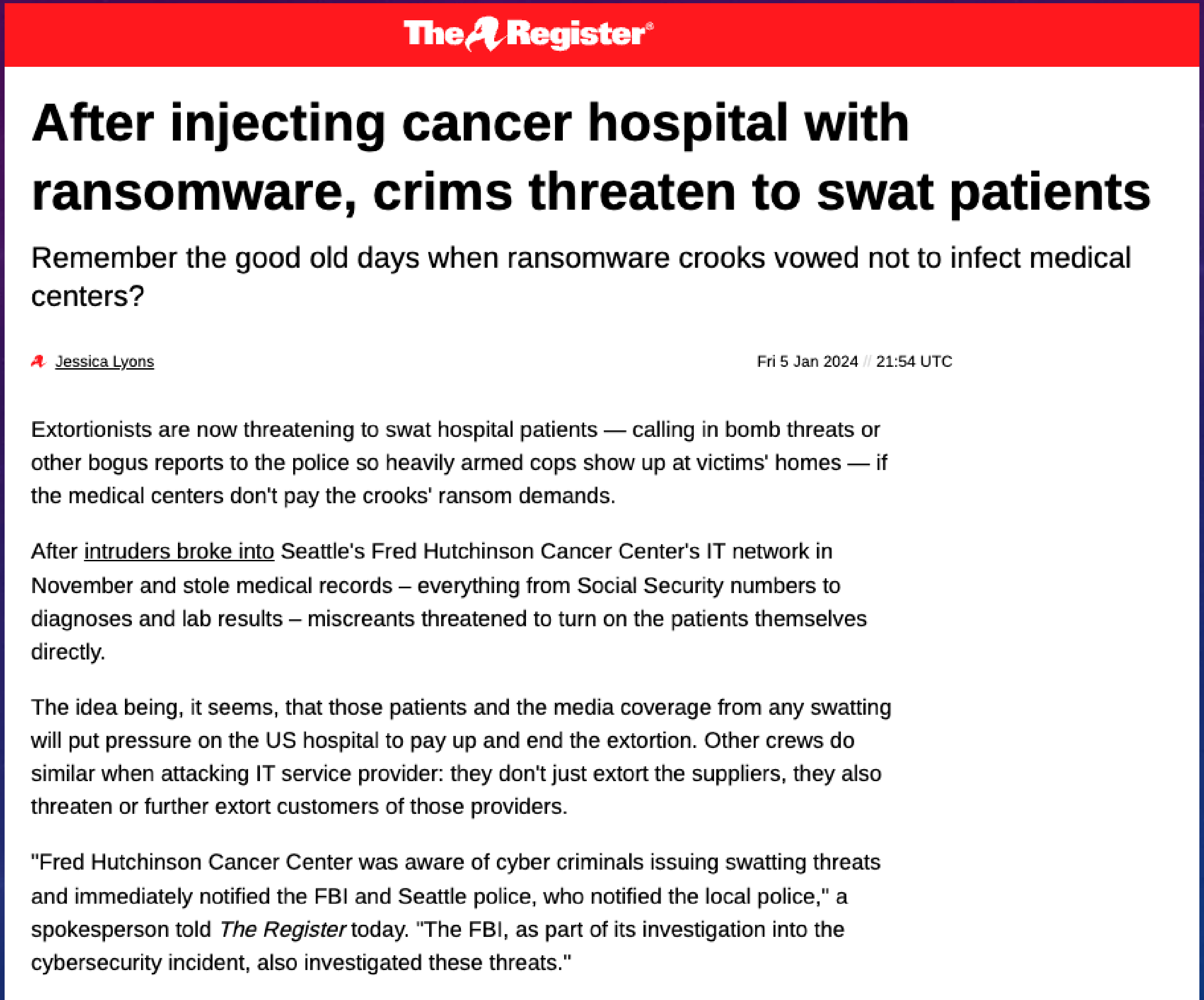
This has triggered a chorus of accusations from the cybersecurity community, with some labeling the group as "barbarians" and others saying the group is "exploiting and sexualizing breast cancer".

Lehigh Valley Health Network
3/4/2023, 11:02:46 PM

We have been in your network for a long time and have had time to study your business.
In addition, we have stolen your confidential data and are ready to publish it.
We have the data of your client base of patients, namely their passports, personal data, questionnaires, nude photos and the like.
Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business.
Your time is running out. We are ready to unleash our full power on you!

https://www.malwarebytes.com/blog/news/2023/03/breast-cancer-photos-published-by-ransomware-gang

PRESSURES - SWATTING



The Register®

After injecting cancer hospital with ransomware, crims threaten to swat patients

Remember the good old days when ransomware crooks vowed not to infect medical centers?

Jessica Lyons   Fri 5 Jan 2024 // 21:54 UTC

Extortionists are now threatening to swat hospital patients — calling in bomb threats or other bogus reports to the police so heavily armed cops show up at victims' homes — if the medical centers don't pay the crooks' ransom demands.

After intruders broke into Seattle's Fred Hutchinson Cancer Center's IT network in November and stole medical records – everything from Social Security numbers to diagnoses and lab results – miscreants threatened to turn on the patients themselves directly.

The idea being, it seems, that those patients and the media coverage from any swatting will put pressure on the US hospital to pay up and end the extortion. Other crews do similar when attacking IT service provider: they don't just extort the suppliers, they also threaten or further extort customers of those providers.

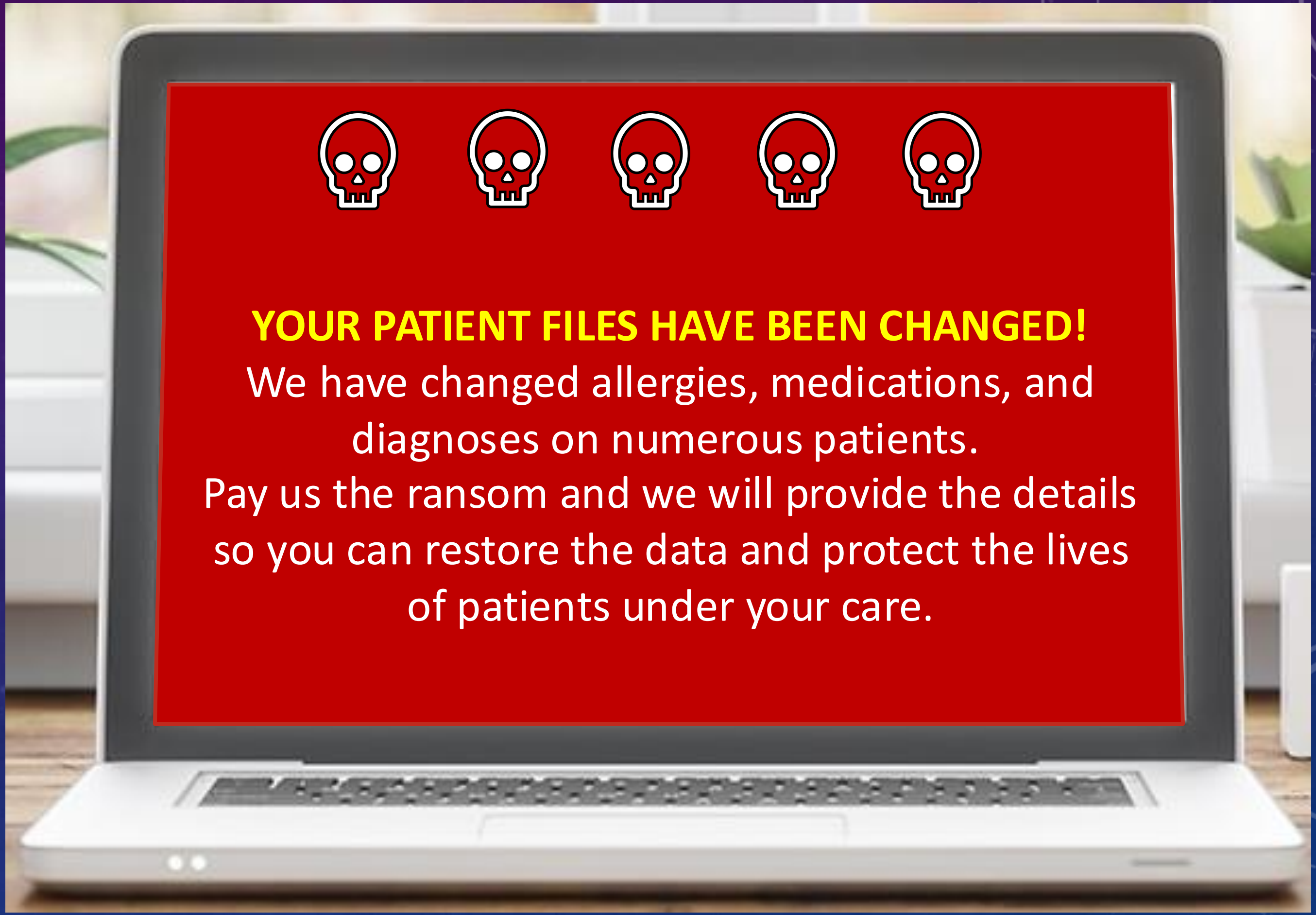
"Fred Hutchinson Cancer Center was aware of cyber criminals issuing swatting threats and immediately notified the FBI and Seattle police, who notified the local police," a spokesperson told *The Register* today. "The FBI, as part of its investigation into the cybersecurity incident, also investigated these threats."

https://www.theregister.com/2024/01/05/swatting_extorion_tactics/

WHAT'S NEXT?

WHAT’S NEXT?

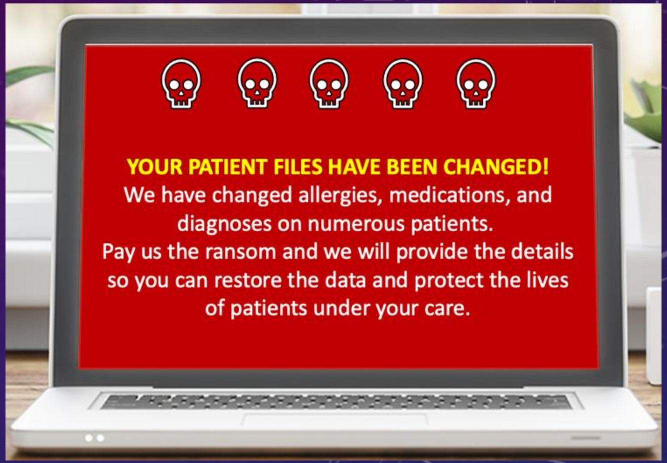
Attacks on Integrity



YOUR PATIENT FILES HAVE BEEN CHANGED!
We have changed allergies, medications, and diagnoses on numerous patients.
Pay us the ransom and we will provide the details so you can restore the data and protect the lives of patients under your care.

(c) 2024 Armstrong Risk Management

ATTACKS ON INTEGRITY



YOUR PATIENT FILES HAVE BEEN CHANGED!
We have changed allergies, medications, and diagnoses on numerous patients.
Pay us the ransom and we will provide the details so you can restore the data and protect the lives of patients under your care.

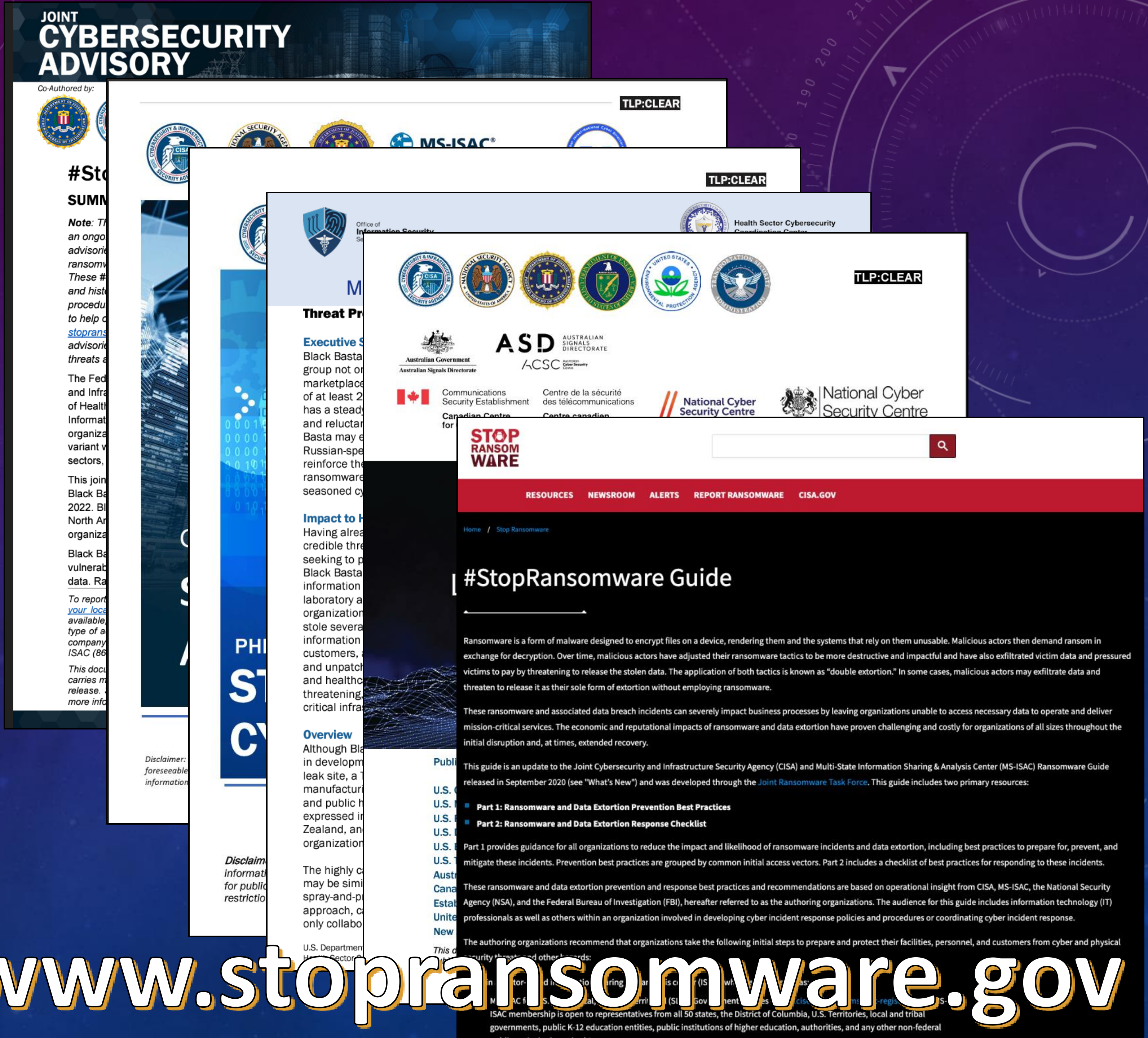
Prepare Now – Some Ideas

- Maintain logs longer
- Monitoring
  - Unusual behavior on disk?
  - Administrator, privileged, and service accounts
- Work with Clinical teams to develop a plan for validating clinical data

WHAT DO WE DO?

GOOD NEWS!

There has never been more information!



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR

Black Basta

Threat Pr

Executive S

Impact to H

Overview

Australian Government Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC

Communications Security Establishment

Centre de la sécurité des télécommunications

National Cyber Security Centre

STOP RANSOMWARE

RESOURCES NEWSROOM ALERTS REPORT RANSOMWARE CISA.GOV

Home / Stop Ransomware

#StopRansomware Guide

Ransomware is a form of malware designed to encrypt files on a device, rendering them and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Over time, malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim data and pressured victims to pay by threatening to release the stolen data. The application of both tactics is known as “double extortion.” In some cases, malicious actors may exfiltrate data and threaten to release it as their sole form of extortion without employing ransomware.

These ransomware and associated data breach incidents can severely impact business processes by leaving organizations unable to access necessary data to operate and deliver mission-critical services. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery.

This guide is an update to the Joint Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing & Analysis Center (MS-ISAC) Ransomware Guide released in September 2020 (see "What’s New") and was developed through the Joint Ransomware Task Force. This guide includes two primary resources:

- **Part 1: Ransomware and Data Extortion Prevention Best Practices**
- **Part 2: Ransomware and Data Extortion Response Checklist**

Part 1 provides guidance for all organizations to reduce the impact and likelihood of ransomware incidents and data extortion, including best practices to prepare for, prevent, and mitigate these incidents. Prevention best practices are grouped by common initial access vectors. Part 2 includes a checklist of best practices for responding to these incidents.

These ransomware and data extortion prevention and response best practices and recommendations are based on operational insight from CISA, MS-ISAC, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI), hereafter referred to as the authoring organizations. The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

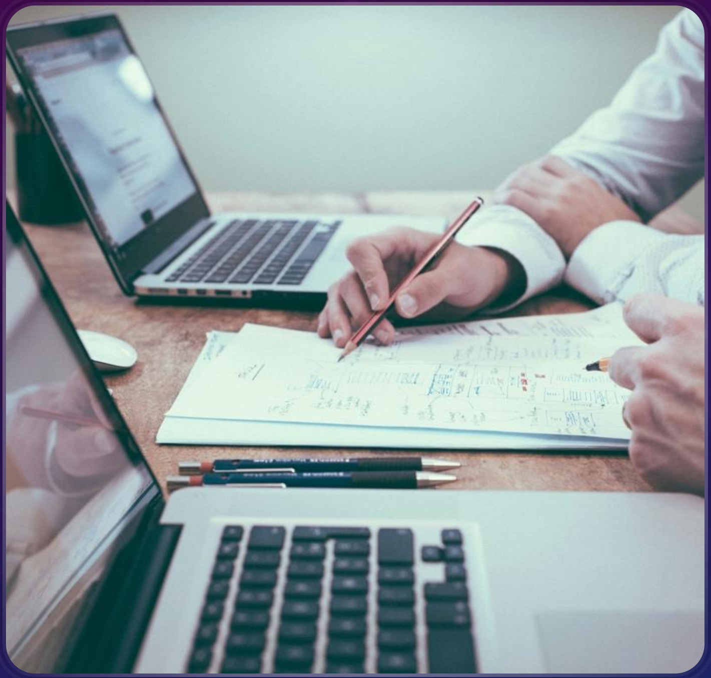
The authoring organizations recommend that organizations take the following initial steps to prepare and protect their facilities, personnel, and customers from cyber and physical security threats and other hazards:

ISAC membership is open to representatives from all 50 states, the District of Columbia, U.S. Territories, local and tribal governments, public K-12 education entities, public institutions of higher education, authorities, and any other non-federal

www.stopransomware.gov

(c) 2024 Armstrong Risk Management

ACTION PLAN



ASSESS

SPRINT

MARATHON

CULTURE

(c) 2024 Armstrong Risk Management

PEOPLE

Strong Security culture

- **People speak up**
- **Not afraid to admit a mistake**

(c) 2024 Armstrong Risk Management

PEOPLE

Strong Security culture

- People speak up
- Not afraid to admit a mistake
- **“Pull that thread!”**

(c) 2024 Armstrong Risk Management

PEOPLE

Strong Security culture

- People speak up
- Not afraid to admit a mistake
- “Pull that thread!”
- **Security Champions**

PEOPLE

Strong Security culture

- People speak up
- Not afraid to admit a mistake
- “Pull that thread!”
- Security Champions
- **Be a business person**
- **Educate the executives**

BUILD YOUR SECURITY CULTURE

- **Educate the Executives and Top Management**
- **Set the Tone from the Top**
- **Create a Blame Free Culture**
  - “Security is everyone’s responsibility”
  - We all make mistakes and no one will be berated
  - Speak up ASAP
- **Interactive Security Awareness Training**
  - Hands on with email, links, shortened urls, etc.
  - Skills for online banking and shopping
- **Monthly Reminders, Posters, Swag**

Security Culture

Building a Security Culture

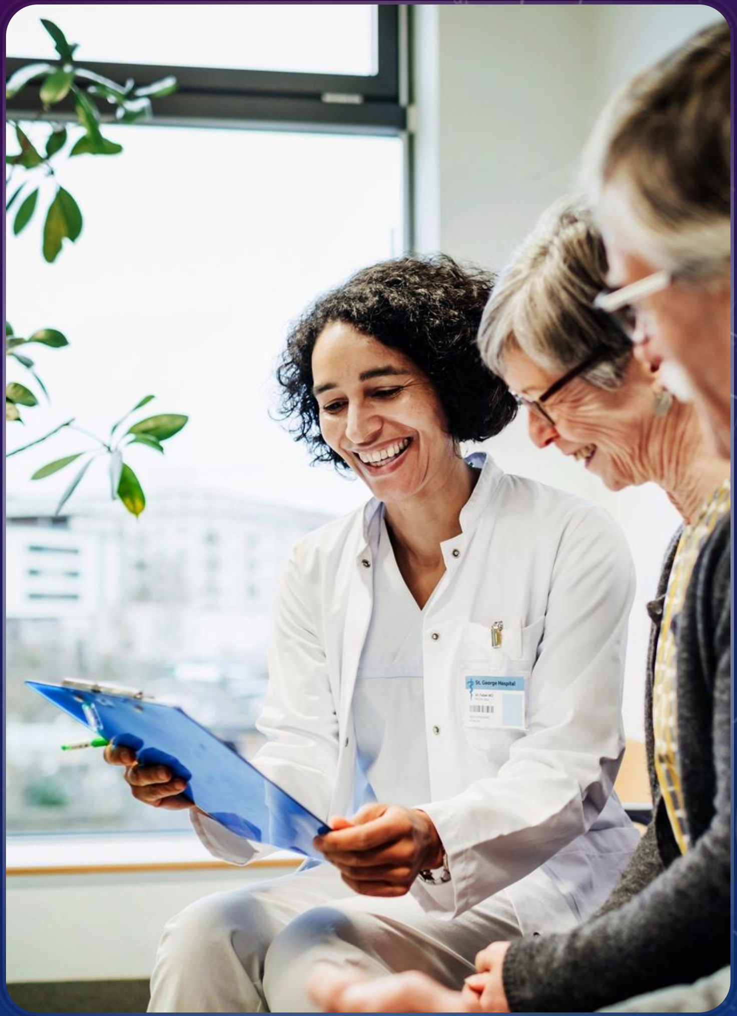
Go beyond dry Security Awareness trainings with interactive trainings designed for your people.

PROCESS

DOWNTIME PROCEDURES

Back to Paper

- Paper forms match the EHR
- Solicit feedback on the forms from staff
- How will these forms will be provided?
  - Pre-printed supply of forms?
  - Where will they be stored?
  - How print as needed?
  - Make staff aware of how to obtain the forms



DOWNTIME PROCEDURES

Returning from Downtime

- Start with paper, finish with paper
- New admissions – ensure critical data entered ASAP (allergies, meds, etc.)
- Enter a note in the patient's medical record that indicates that the EHR was down

INCIDENT RESPONSE PLANNING

"Plans are worthless,
but planning is everything"
attributed to Dwight D. Eisenhower

- Determine what is Critical
- Create Playbooks
- Decide upon Reporting, Triage, escalation procedures
- Educate Staff
- Run Tabletop Exercises (TTX)
- Refine the Plan
- Repeat

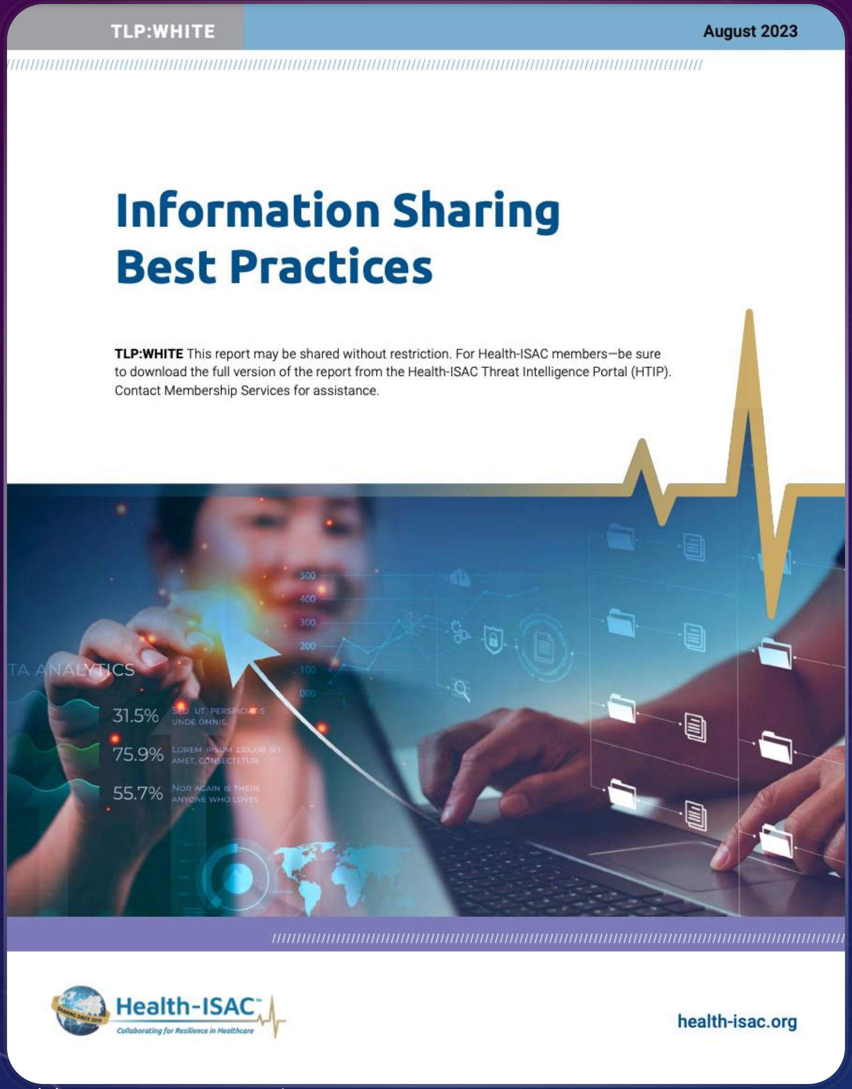
INTENSE TRAINING

(c) 2024 Armstrong Risk Management

TABLETOP EXERCISES

- Key Stakeholders
  - Clinicians
  - Executives
  - Legal
- Exercise the Plans
- Cyber Range
- “Live Fire”
- Other Hospitals!

RESILIENCE



TLP:WHITE

August 2023

Information Sharing Best Practices

TLP:WHITE This report may be shared without restriction. For Health-ISAC members—be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC

Collaborating for Resilience in Healthcare

health-isac.org

H-ISAC
INFORMATION SHARING

- Strategic
- Tactical
- Operational
- Open Source Intel
- Industry Best Practices
- Incident Response
- Defender Resources
- Media Response

PARTNERSHIPS

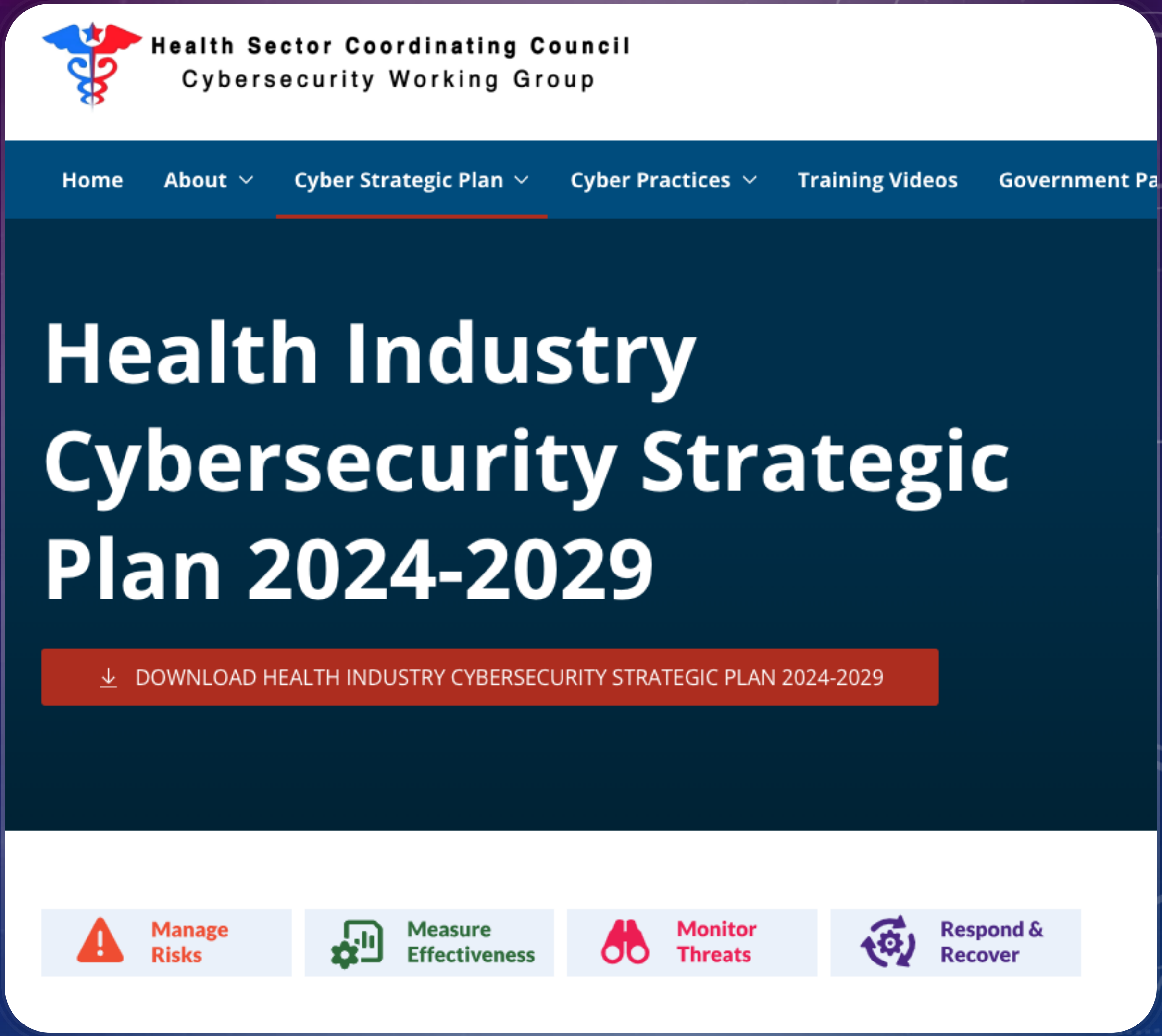
- **InfraGard** - Partnership with the FBI
- **H-ISAC - Health Information Sharing and Analysis Center**
- **ASPR TRACIE** - Healthcare Emergency Preparedness Information Gateway
- **HIMSS** - Healthcare Information and Management Systems Society

(c) 2024 Armstrong Risk Management

THERE IS A PLAN!

”Cyber Safety is *Patient Safety*”

- Get involved!
- Lots of Resources
  - Health Industry Cybersecurity Practices (HICP)
  - HPH Cybersecurity Framework Implementation Guide



Health Sector Coordinating Council
Cybersecurity Working Group

Health Industry Cybersecurity Strategic Plan 2024-2029

ACTION PLAN AND DISCUSSION

ASSESS

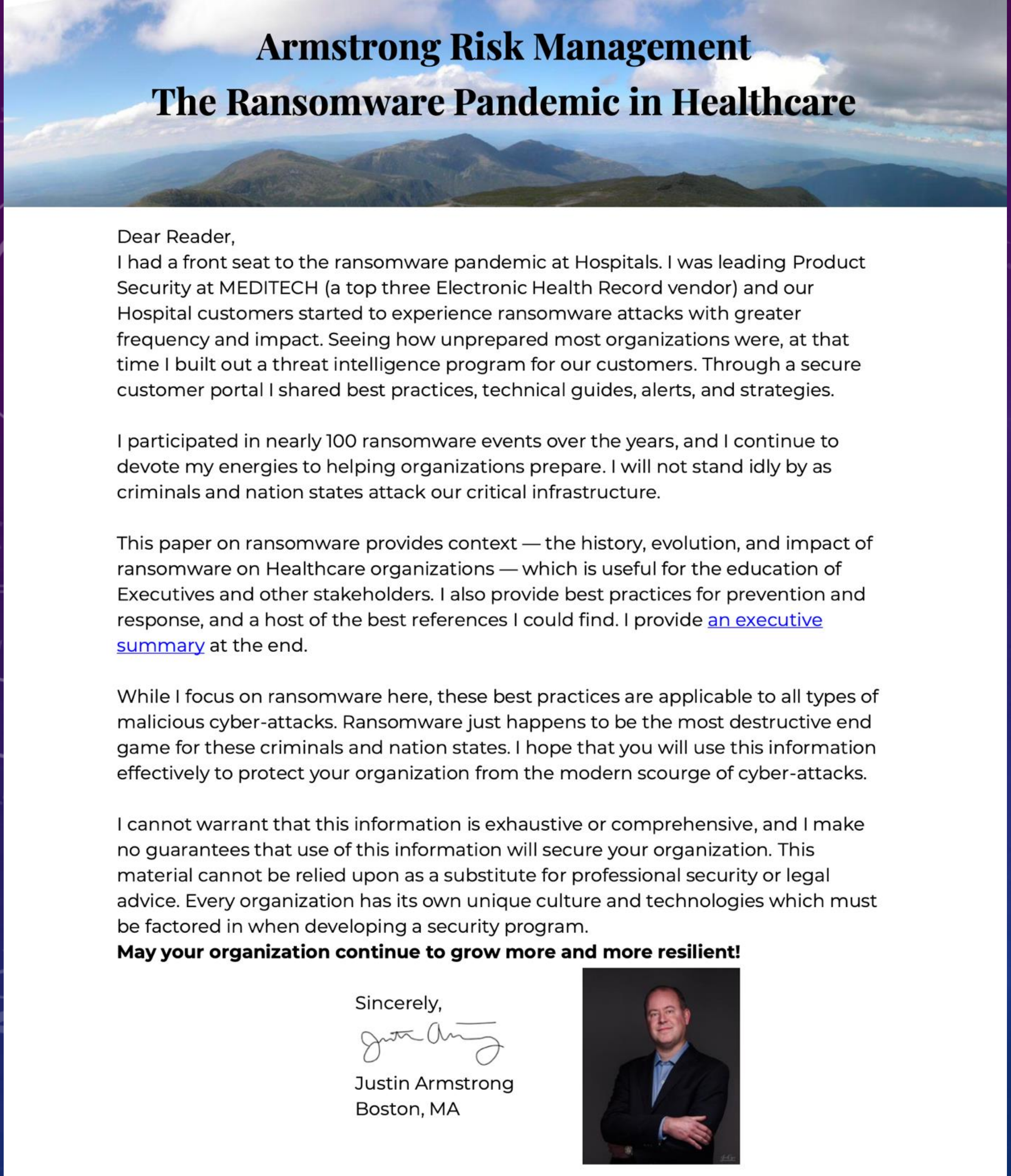
- Identify Critical Systems
- Assess Risk

SPRINT

- Security Culture
- Strong Authentication
- Lock down IT Tools and Privileged Access
- Incident Preparedness

MARATHON

- Process Improvement
- Reduce Technical Debt
- Measure and Monitor
- Managed Security Services



Armstrong Risk Management
The Ransomware Pandemic in Healthcare

Dear Reader,
I had a front seat to the ransomware pandemic at Hospitals. I was leading Product Security at MEDITECH (a top three Electronic Health Record vendor) and our Hospital customers started to experience ransomware attacks with greater frequency and impact. Seeing how unprepared most organizations were, at that time I built out a threat intelligence program for our customers. Through a secure customer portal I shared best practices, technical guides, alerts, and strategies.

I participated in nearly 100 ransomware events over the years, and I continue to devote my energies to helping organizations prepare. I will not stand idly by as criminals and nation states attack our critical infrastructure.

This paper on ransomware provides context — the history, evolution, and impact of ransomware on Healthcare organizations — which is useful for the education of Executives and other stakeholders. I also provide best practices for prevention and response, and a host of the best references I could find. I provide an executive summary at the end.

While I focus on ransomware here, these best practices are applicable to all types of malicious cyber-attacks. Ransomware just happens to be the most destructive end game for these criminals and nation states. I hope that you will use this information effectively to protect your organization from the modern scourge of cyber-attacks.

I cannot warrant that this information is exhaustive or comprehensive, and I make no guarantees that use of this information will secure your organization. This material cannot be relied upon as a substitute for professional security or legal advice. Every organization has its own unique culture and technologies which must be factored in when developing a security program.
May your organization continue to grow more and more resilient!

Sincerely,

Justin Armstrong
Boston, MA

CHECK OUT MY E-BOOK!

WWW.ARMSTRONGRISK.COM

JUSTIN@ARMSTRONGRISK.COM