Cybersecurity Considerations for the Financial Industry

Cam Murphy

15 March 2024

Introductions

Cam Murphy

- Cybersecurity Operations Manager - Defense Contractor (2024 - Present)

- Director of Cybersecurity at MSSP w/ 50+ SMB clients (2022 – 2024)

- Sr Cybersecurity Engineer - Defense Contractor (2019 – 2021)

- Active Duty Navy (2003 – 2019)
  - Navy Special Warfare (2012 – 2019)
  - National Security Agency, Sr Exploitation Analyst (2007 – 2012)
  - Submarines Surveillance Operations (2003 – 2007)

Agenda

- What is a Cyber Attack?
- Why is the Financial Industry Targeted?
- Cyber Attack Statistics
- 3rd Party Enabled Cyber Attacks
- Preventative Measures
- Questions

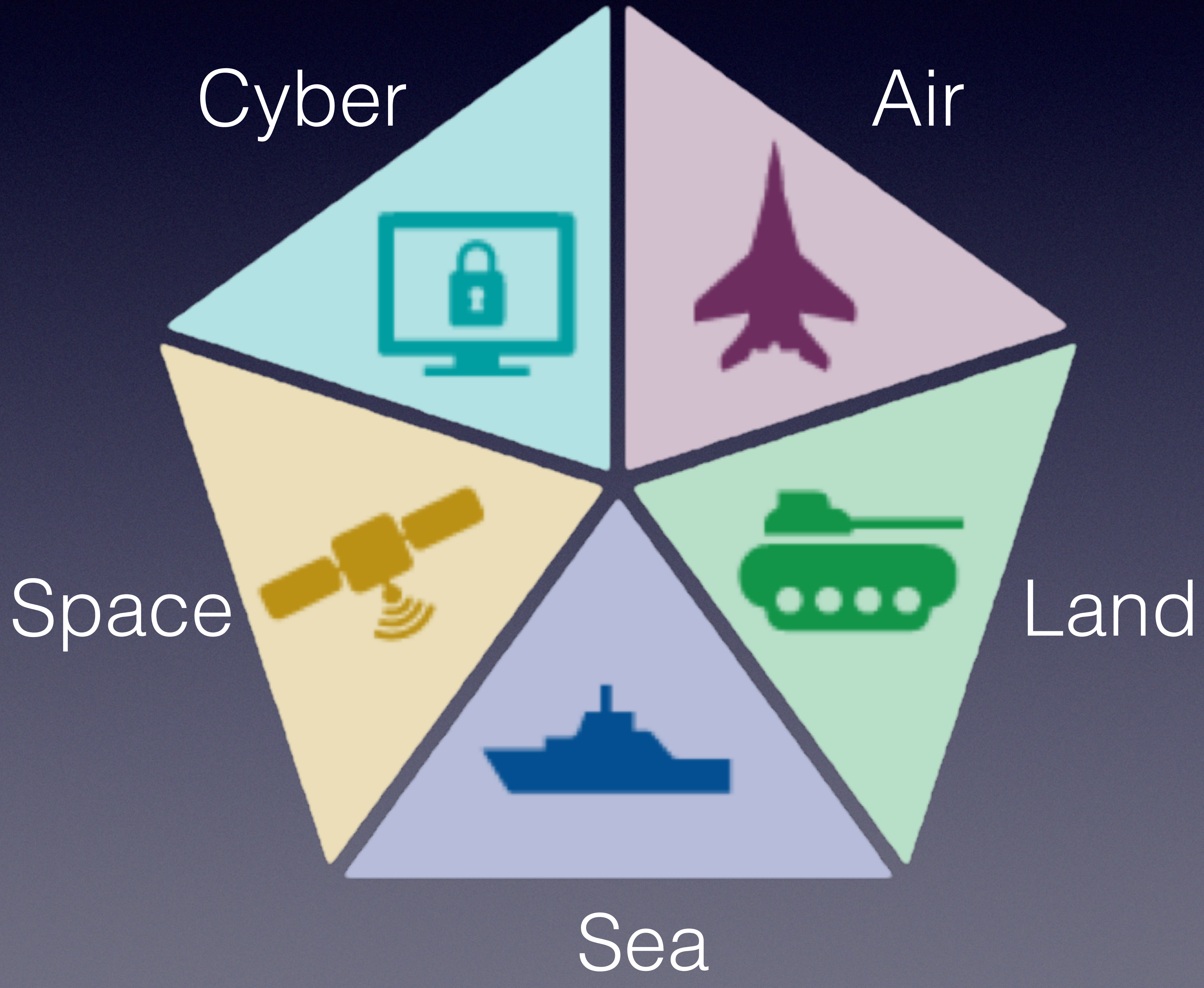
What is a Cyber Attack

IBM's Definition

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.

Cam's Definition

Computer network activity with malicious and unlawful intent.

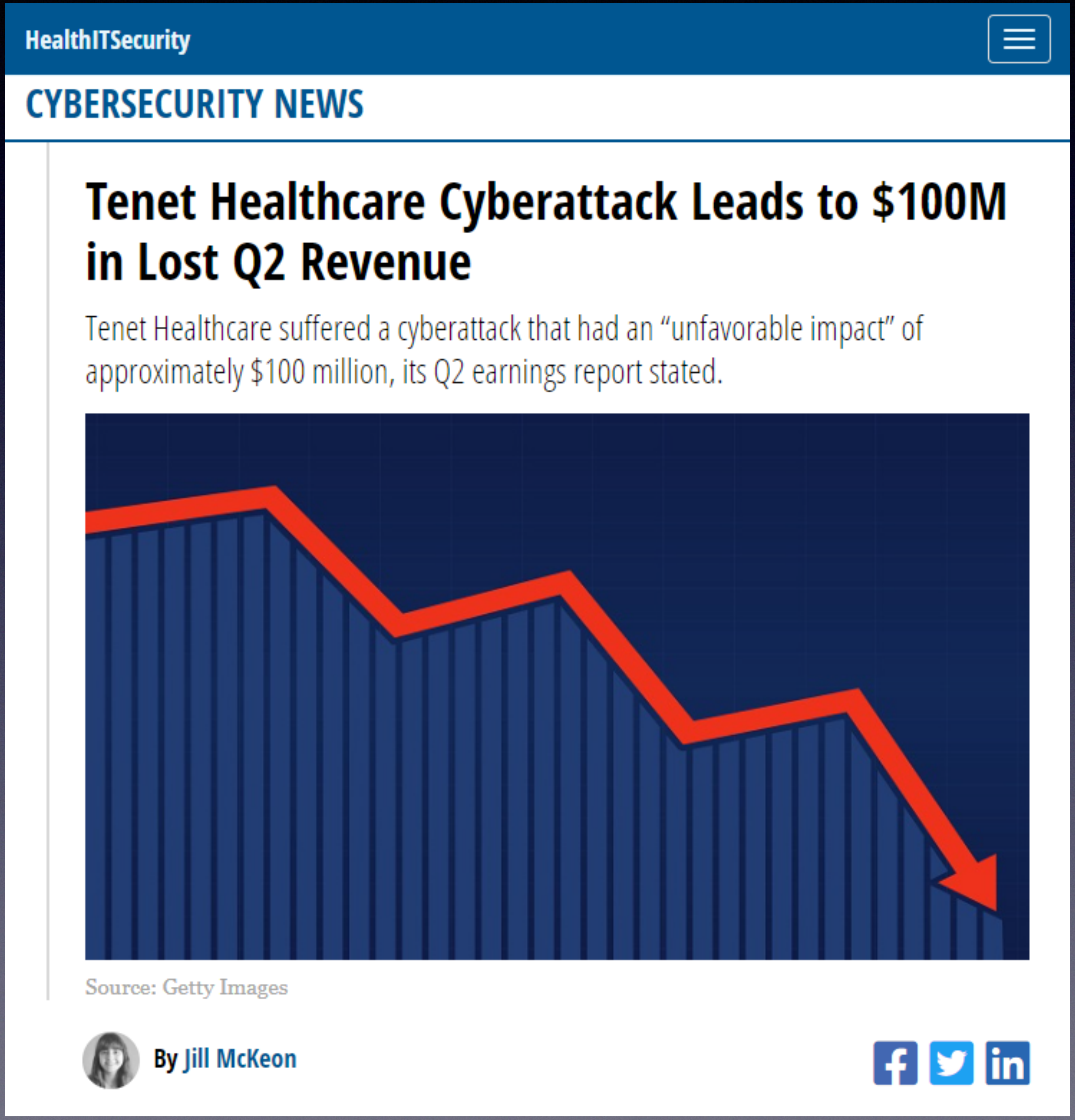


Cyber Attack Ripple Effects

- Initial Affects –
  - Resources diverted to recovery,
  - PR team activated

- Secondary Affects –
  - Investigations, legal processes,
  - insurance claims,
  - preventative measures,
  - employee turnover,

- Tertiary Affects –
  - Usually unaccounted for,
  - reputation impact,
  - business partnerships impact,
  - increased operating costs



HealthITSecurity

CYBERSECURITY NEWS

Tenet Healthcare Cyberattack Leads to $100M in Lost Q2 Revenue

Tenet Healthcare suffered a cyberattack that had an "unfavorable impact" of approximately $100 million, its Q2 earnings report stated.

Source: Getty Images

By Jill McKeon

Why is the Financial Industry Targeted?

Why is the ~~Financial Industry~~ Anyone Targeted?

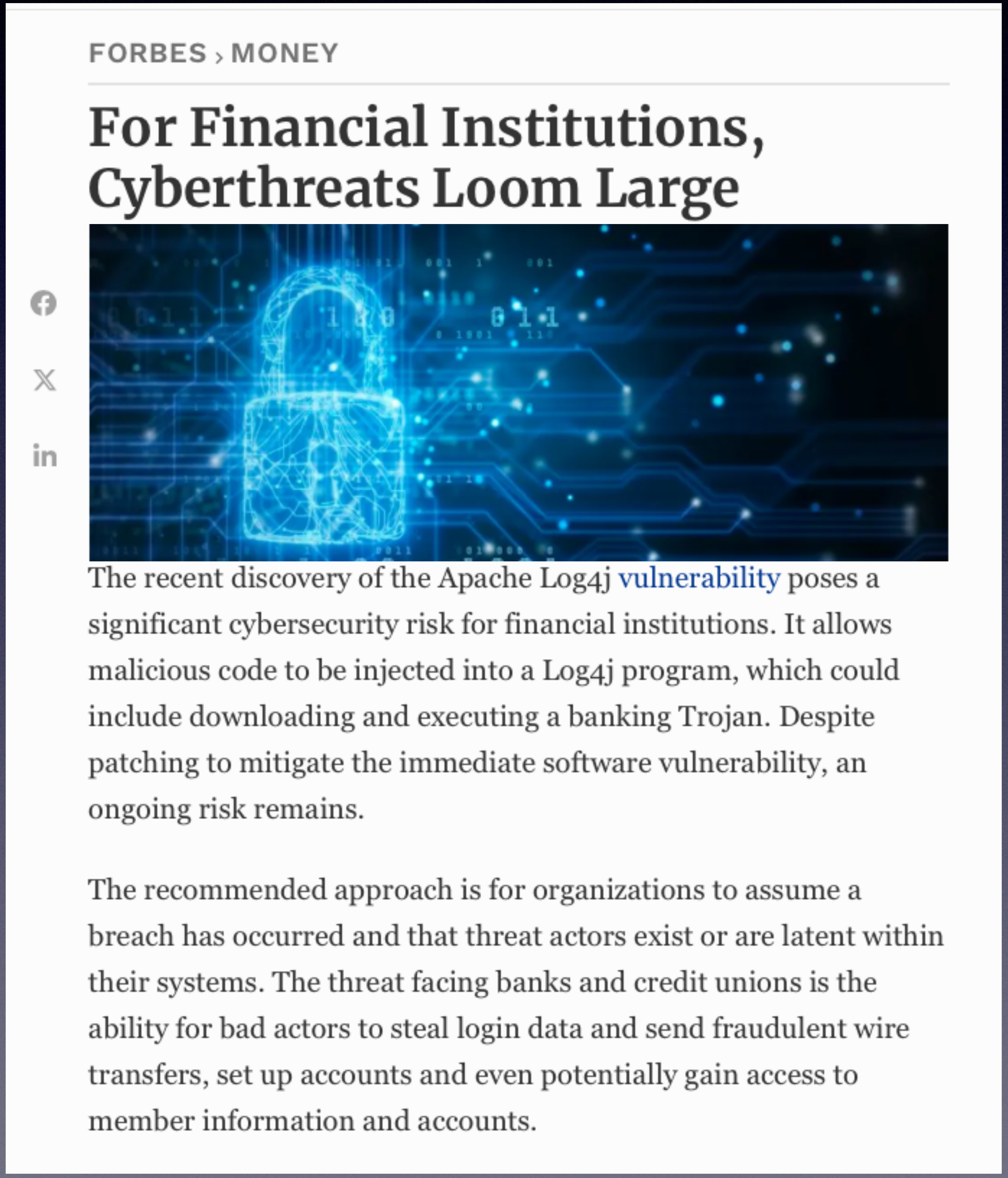
- Financial Gain
    - Most businesses will at least consider paying ransoms
    - Many have a cyber insurance policy that will pay ransoms

- Entry Point for Larger Attack Campaign
    - Attackers will piece together a series of attacks to go after the largest target possible first
    - One compromise can lead to higher probability a social engineering attack is successful against another, more profitable target

- Lack of Cybersecurity Professionals
    - Cybersecurity workforce will need to grow 35% over the next 6 years
    - Cybersecurity vacancies take months to fill
    - Nearly 0% unemployment rate for cybersecurity professionals

Why is the Financial Industry Successfully Targeted?

- Target-Rich Environment
  - Large industry
  - Access to large amount of valuable data
  - Access to large amount of capital
- Likely to pay a ransom
  - 50% of ransomware finance industry attacks resulted in payment
    - 40% ransom is $1M or more
  - 70% restored from backups in all other cases



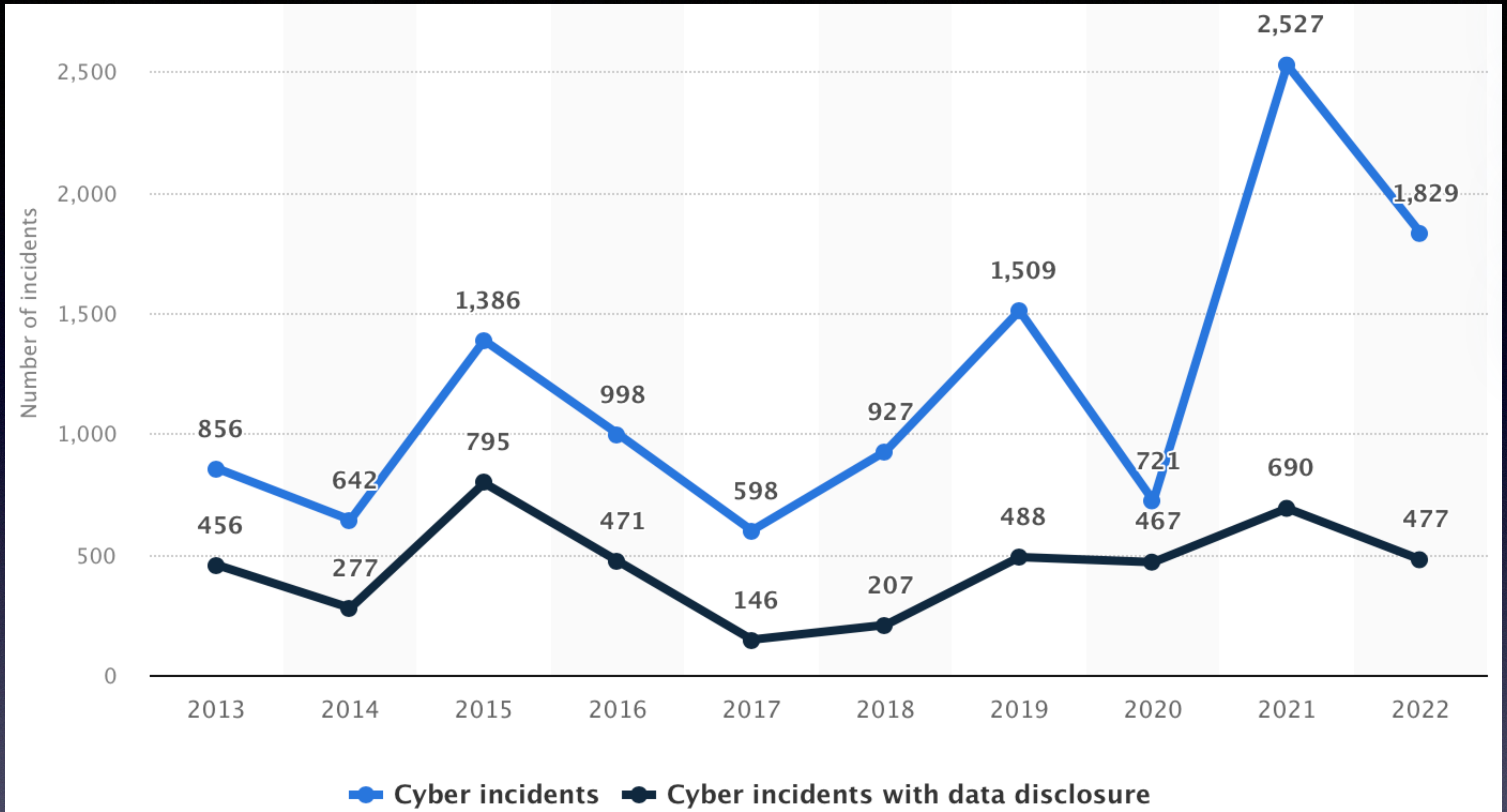
FORBES › MONEY

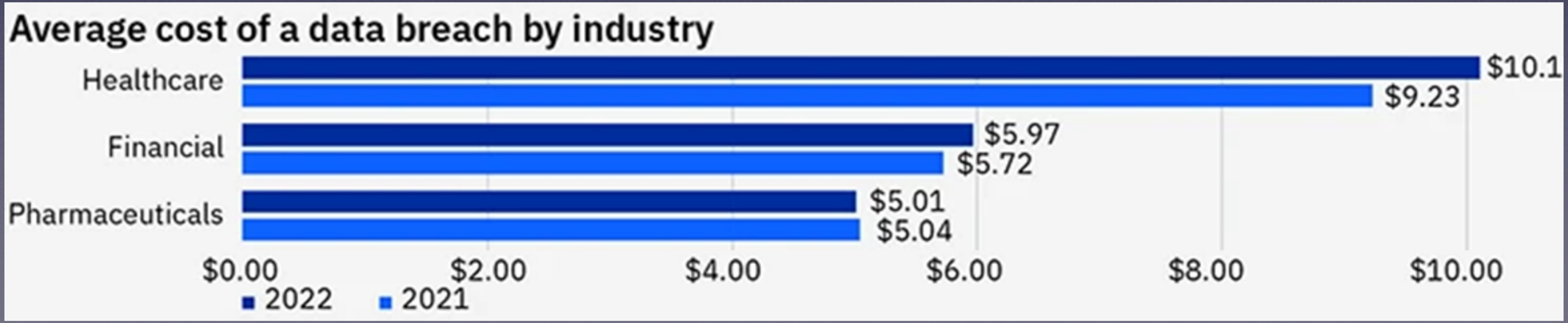
For Financial Institutions, Cyberthreats Loom Large

The recent discovery of the Apache Log4j vulnerability poses a significant cybersecurity risk for financial institutions. It allows malicious code to be injected into a Log4j program, which could include downloading and executing a banking Trojan. Despite patching to mitigate the immediate software vulnerability, an ongoing risk remains.

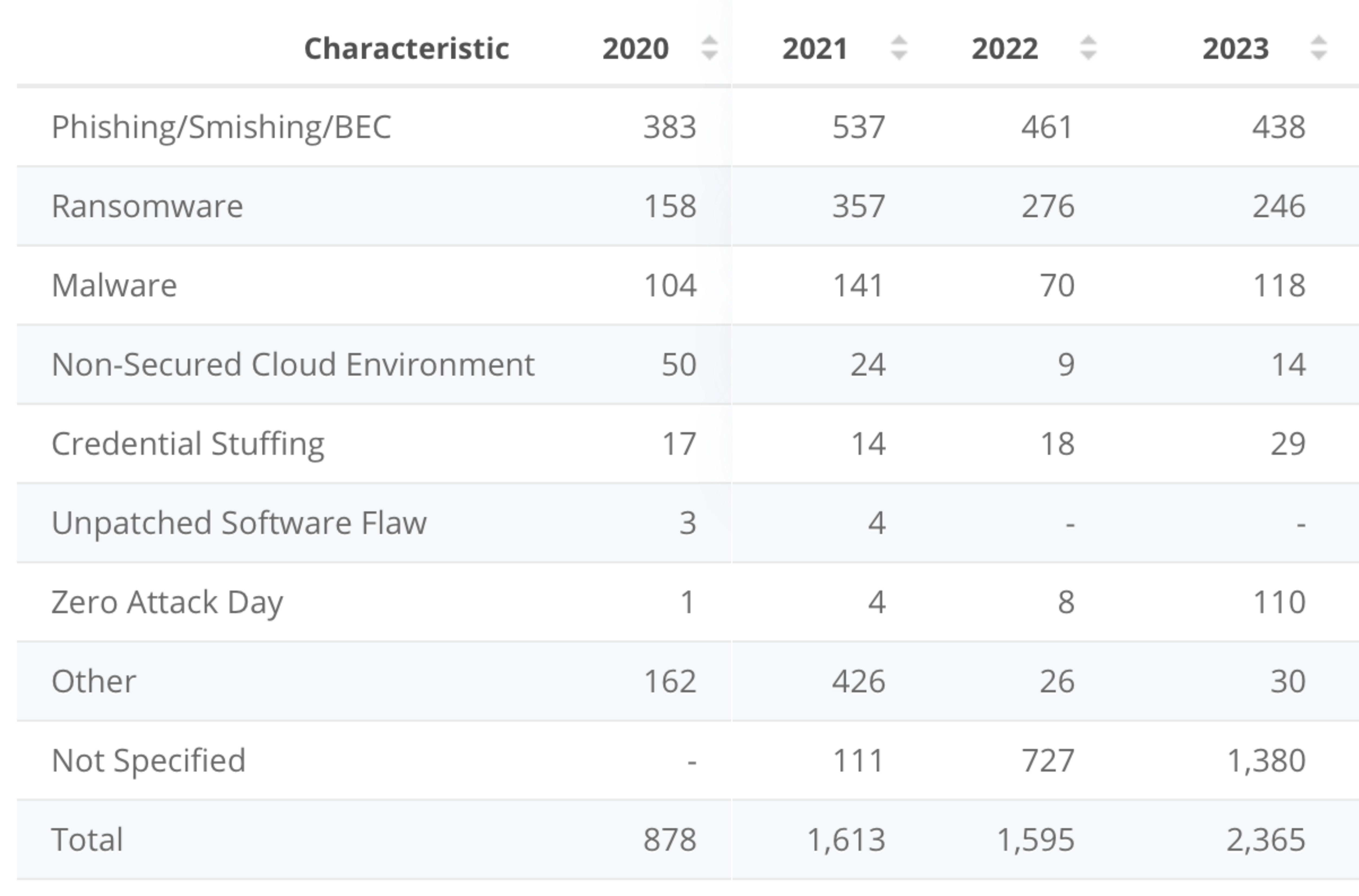
The recommended approach is for organizations to assume a breach has occurred and that threat actors exist or are latent within their systems. The threat facing banks and credit unions is the ability for bad actors to steal login data and send fraudulent wire transfers, set up accounts and even potentially gain access to member information and accounts.

Cyber Attacks

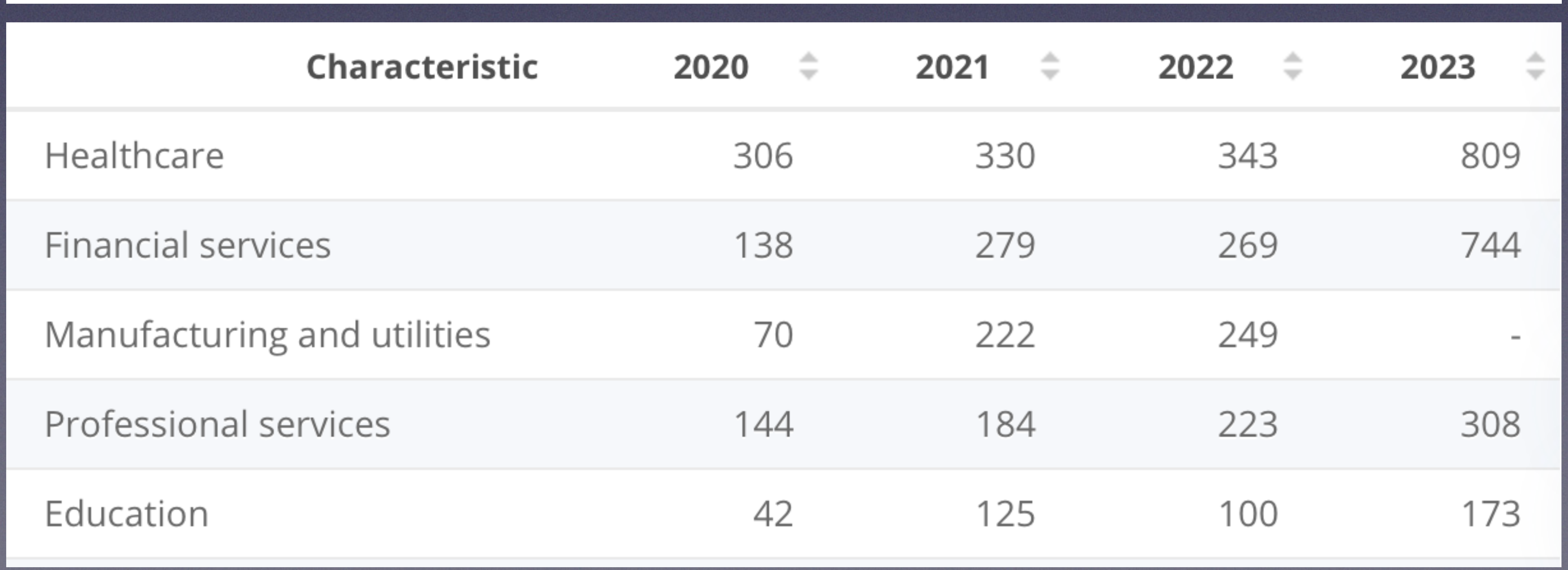



Average cost of a data breach by industry

Cyber Attacks



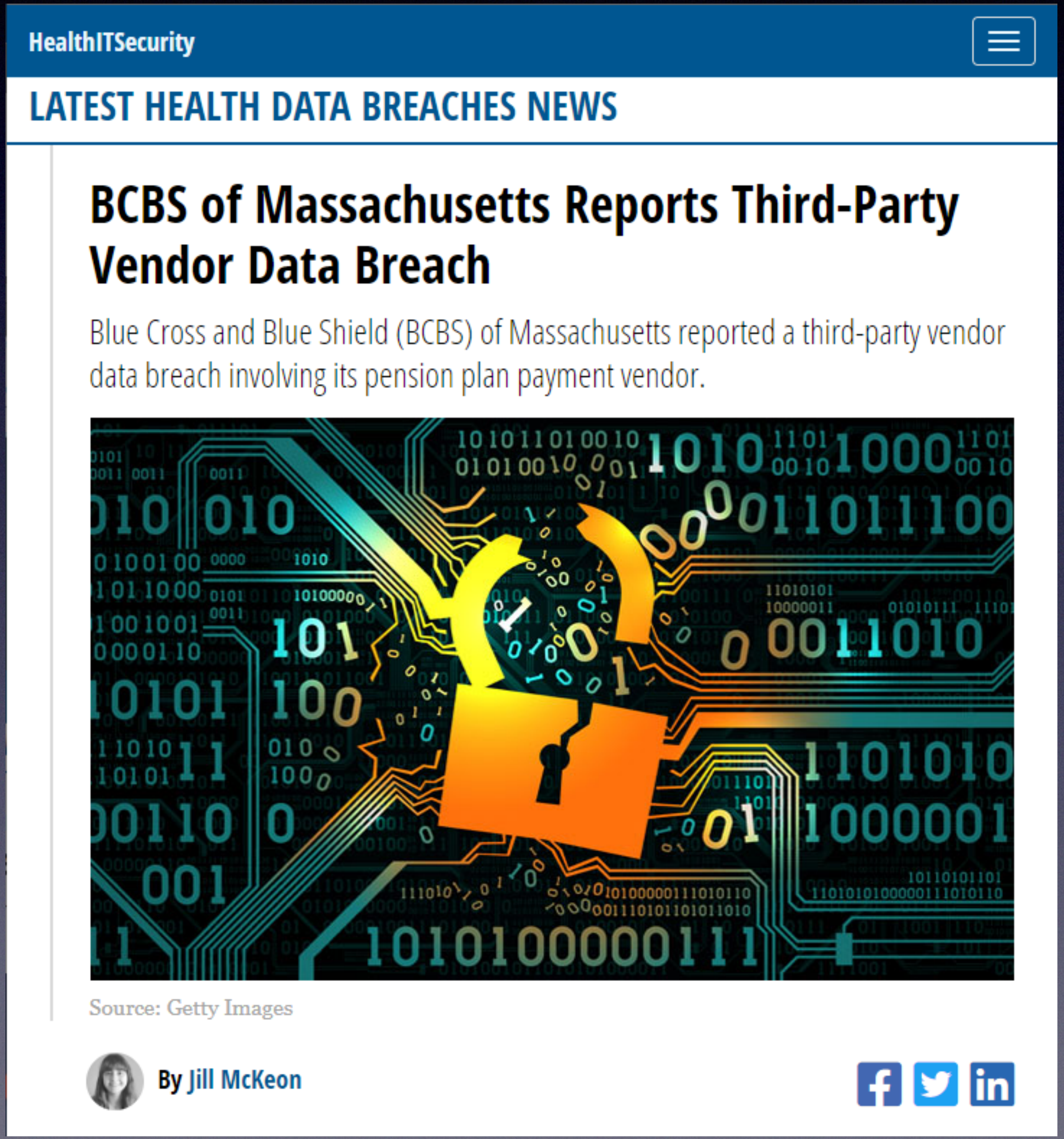
Characteristic	2020	2021	2022	2023
Phishing/Smishing/BEC	383	537	461	438
Ransomware	158	357	276	246
Malware	104	141	70	118
Non-Secured Cloud Environment	50	24	9	14
Credential Stuffing	17	14	18	29
Unpatched Software Flaw	3	4	-	-
Zero Attack Day	1	4	8	110
Other	162	426	26	30
Not Specified	-	111	727	1,380
Total	878	1,613	1,595	2,365



Characteristic	2020	2021	2022	2023
Healthcare	306	330	343	809
Financial services	138	279	269	744
Manufacturing and utilities	70	222	249	-
Professional services	144	184	223	308
Education	42	125	100	173

3rd Party Enabled Cyber Attacks

- Blue Cross Blue Shield, Massachusetts
- Third-party breach led to compromise of BCBS in 2021
- Strengthening your cybersecurity posture is critical
- Verifying your partner organizations cybersecurity posture is too
- BCBS's vendor lacked proper data-loss prevention (DLP) solution which would have likely prevented this incident.
  - "Do you have a DLP?"



HealthITSecurity

LATEST HEALTH DATA BREACHES NEWS

BCBS of Massachusetts Reports Third-Party Vendor Data Breach

Blue Cross and Blue Shield (BCBS) of Massachusetts reported a third-party vendor data breach involving its pension plan payment vendor.

Source: Getty Images

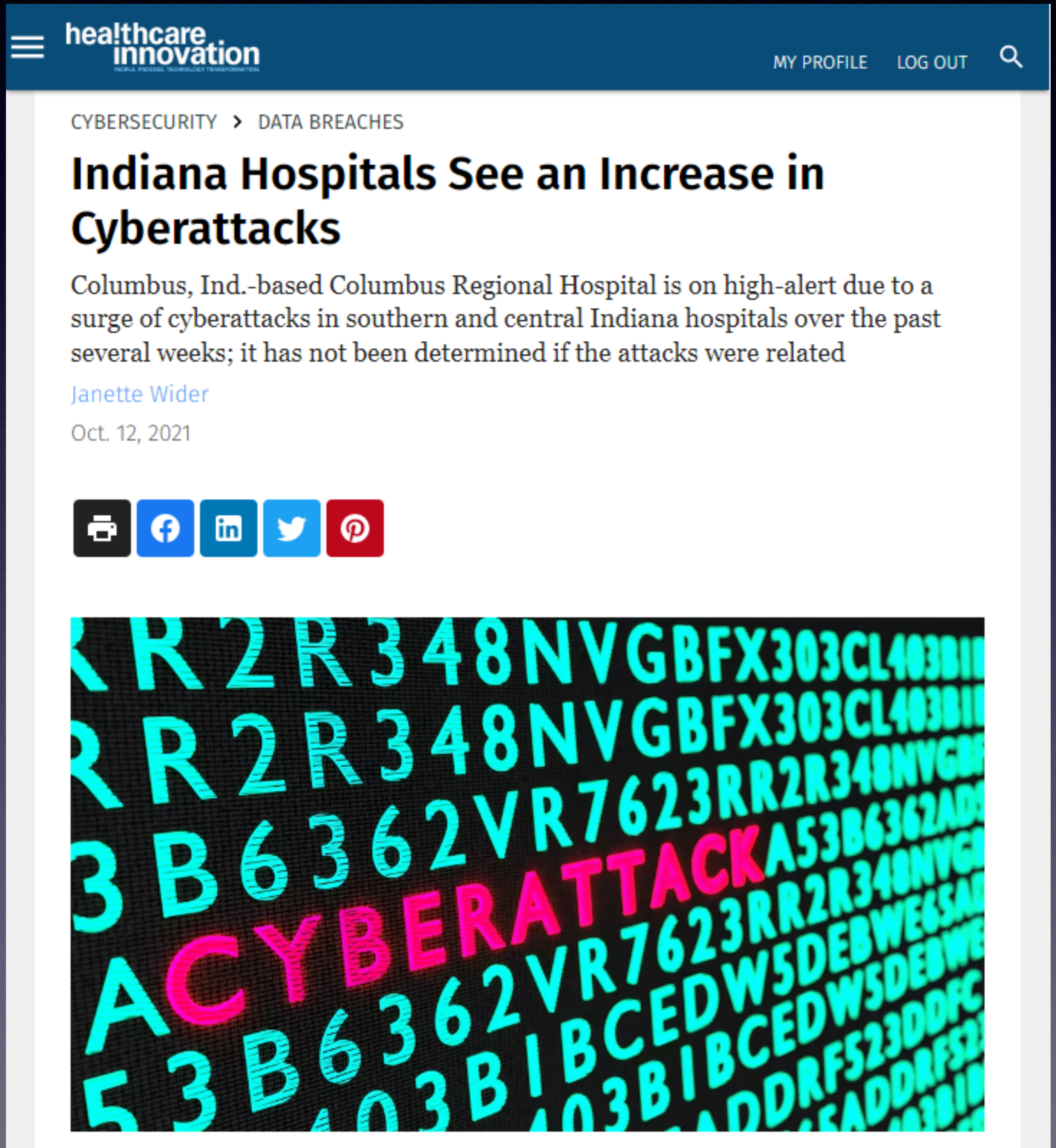
By Jill McKeon

Recent Cyber Attacks

- **Royal Mail Faces Huge Financial Loss Following LockBit Attack (Jan 2023)**
  - Ransomware which resulted in a temporary halt to international deliveries. The Royal Mail refused the pay the £65.7m ($79.85m) demand from the LockBit group to return the stolen data
- **Enormous Data Breach at T-Mobile (November 2022 - March 2023)**
  - 37 million affected customers
- **City of Oakland Declares State of Emergency After Ransomware Attack (February 2023)**
  - City of Oakland, California, declared a state of emergency as a result of a ransomware attack.
- **MOVEit File Transfer Exploitation (May 2023)**
  - Zero-day vulnerability impacted thousands of organizations.
- **Chinese Espionage Campaign Infiltrates US Government (May 2023)**
  - Chinese cyber-attackers gained access to US government agencies' data via Microsoft's engineer's account.
- **UK Electoral Commission Attack Exposes 40 Million Voters' Data (August 2023)**
  - "Complex cyber-attack" exposing data of UK voters who registered between 2014 and 2022.
- **Casinos Taken Down by Cyber-Attacks (September 2023)**
  - MGM Resorts International reported a ransomware which cost them over $100M in recovery. Caesars Entertainment, revealed it had also been compromised by ransomware threat actors.
- **Logistics Firm Closes Due to Ransomware Attack (September 2023)**
  - One of the UK's largest privately owned logistics firms bankrupt following a ransomware attack.
- **23andMe Suffers Major Data Breach (October 2023)**
  - Cyber attack breach of 20 million 23andMe data records.
- **British Library Suffers Damaging Ransomware Incident (October 2023)**
  - British Library, was hit by a ransomware attack resulting in user data offered for sale on the dark web.

Indiana Healthcare Cyber Attacks

- Three healthcare facilities attacked from May to October 2021
- Facility responses mostly consistent
- Public response mostly consistent
- Attacker M.O. was consistent
- Offensive patterns (should) trigger defensive solutions



CYBERSECURITY > DATA BREACHES

Indiana Hospitals See an Increase in Cyberattacks

Columbus, Ind.-based Columbus Regional Hospital is on high-alert due to a surge of cyberattacks in southern and central Indiana hospitals over the past several weeks; it has not been determined if the attacks were related

Janette Wider

Oct. 12, 2021

Indiana Healthcare Cyber Attacks

- Eskenazi Health, Indianapolis

- “WannaCry” Ransomware attack

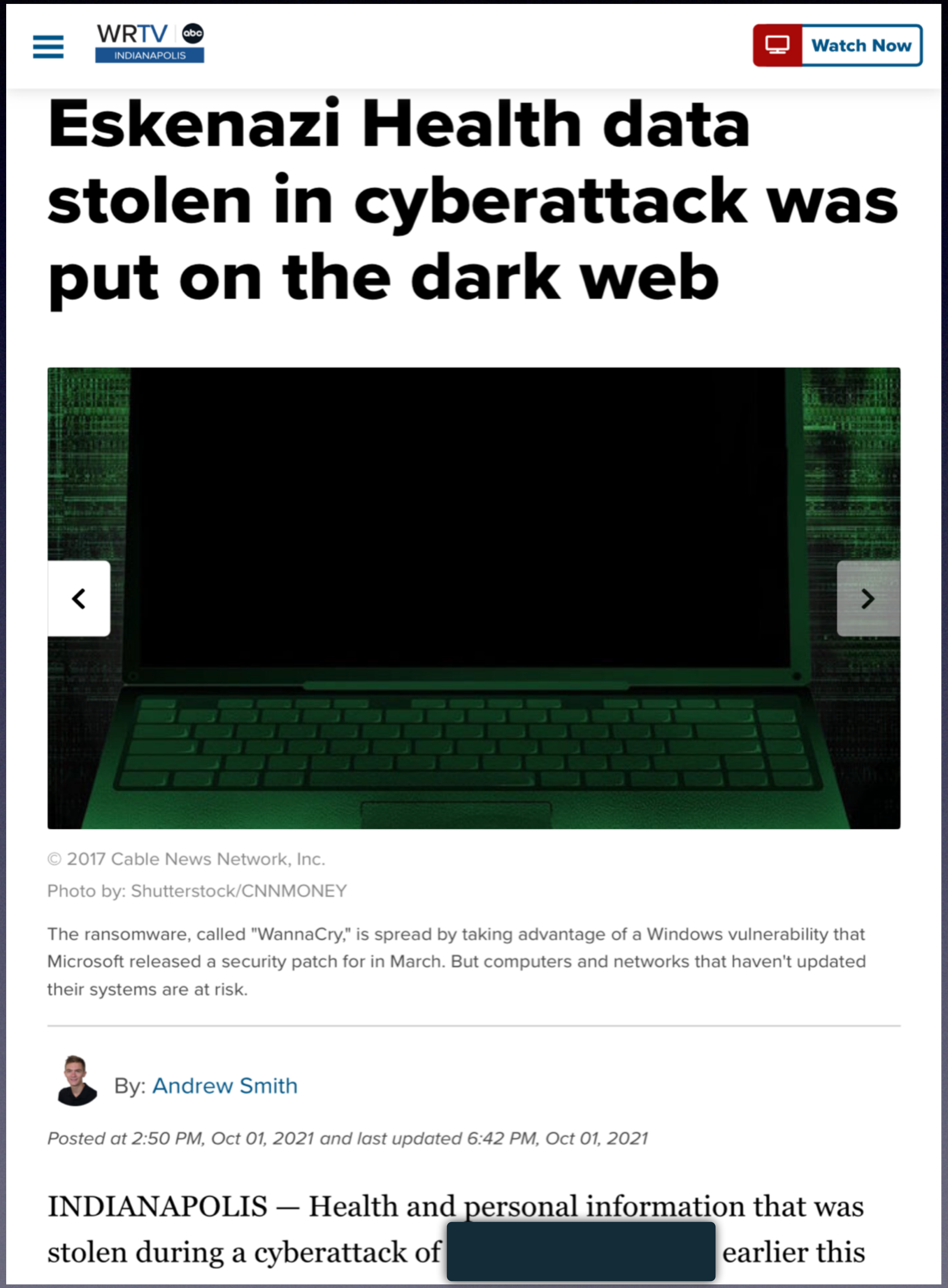
Breach Date:	19 May 2021
Breach Discovery:	4 Aug 2021
Breach Disclosure:	4 Aug 2021
Impact Awareness:	__________
Patients notified:	11 Nov 2021
Breach to Notify:	7 months

- Security patch was available in March 2021

- IT systems, EHR were offline for multiple days

- Attackers exfiltrated and published PHI and employee PII on the Internet

- Patients file lawsuit



Eskenazi Health data stolen in cyberattack was put on the dark web

© 2017 Cable News Network, Inc.
Photo by: Shutterstock/CNNMONEY

The ransomware, called "WannaCry," is spread by taking advantage of a Windows vulnerability that Microsoft released a security patch for in March. But computers and networks that haven't updated their systems are at risk.

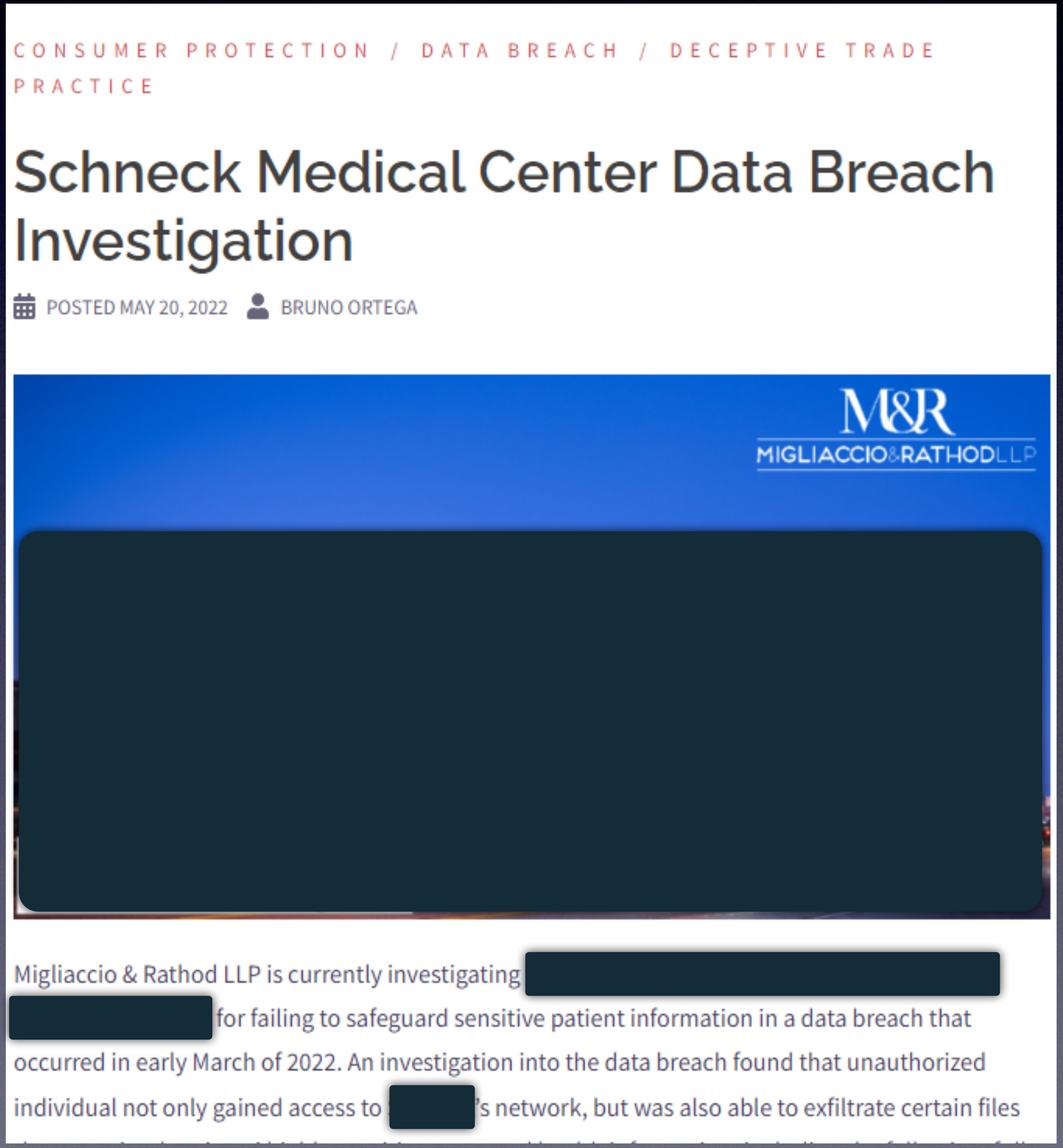
By: Andrew Smith

Posted at 2:50 PM, Oct 01, 2021 and last updated 6:42 PM, Oct 01, 2021

INDIANAPOLIS — Health and personal information that was stolen during a cyberattack of [redacted] earlier this

Indiana Healthcare Cyber Attacks

- Schneck Medical Center, Sep 2021
  - Breach Date: ____________
  - Breach Discovery: 29 Sep 2021
  - Breach Disclosure: 29 Sep 2021
  - Impact Awareness: 17 Mar 2022
  - Patients notified: 13 May 2022
  - Breach to Notify: *8 months
- IT systems, EHR offline for 10 days
- Investigations are still underway
- Patients file lawsuit



CONSUMER PROTECTION / DATA BREACH / DECEPTIVE TRADE PRACTICE

Schneck Medical Center Data Breach Investigation

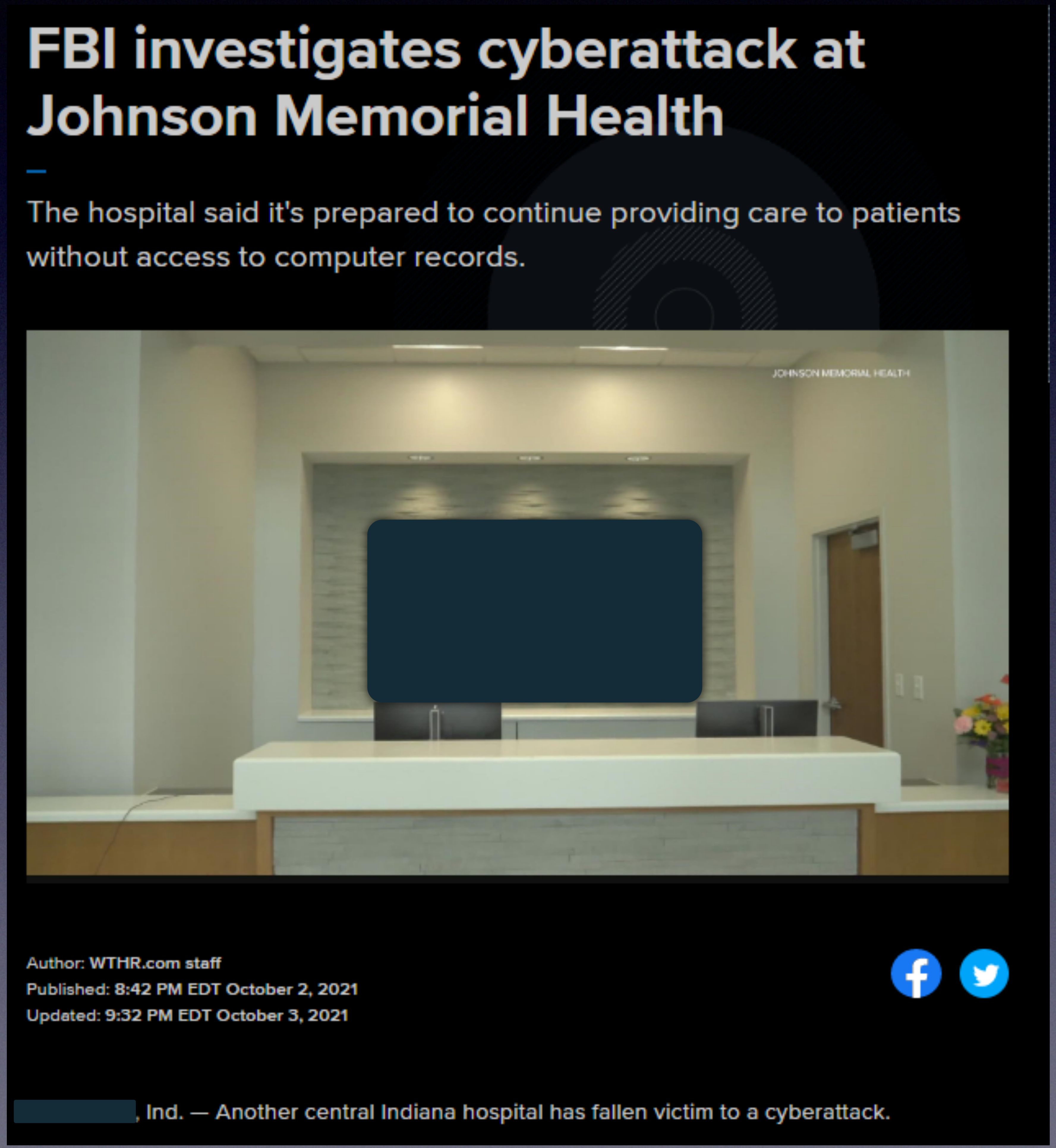
POSTED MAY 20, 2022 BRUNO ORTEGA

[redacted]

Migliaccio & Rathod LLP is currently investigating [redacted] for failing to safeguard sensitive patient information in a data breach that occurred in early March of 2022. An investigation into the data breach found that unauthorized individual not only gained access to [redacted]'s network, but was also able to exfiltrate certain files

Indiana Healthcare Cyber Attacks

- Johnson Memorial Health, Oct 2021
- Ransomware attack
  - Breach Date: 2 Oct 2021
  - Breach Discovery: 2 Oct 2021
  - Breach Disclosure: 2 Oct 2021
  - Impact Awareness: __________
  - Patients notified: 13 May 2022
  - Breach to Notify: 7 months
- Entire computer network offline
- IT systems, EHR were offline for multiple days
- Legal firms investigated



FBI investigates cyberattack at Johnson Memorial Health

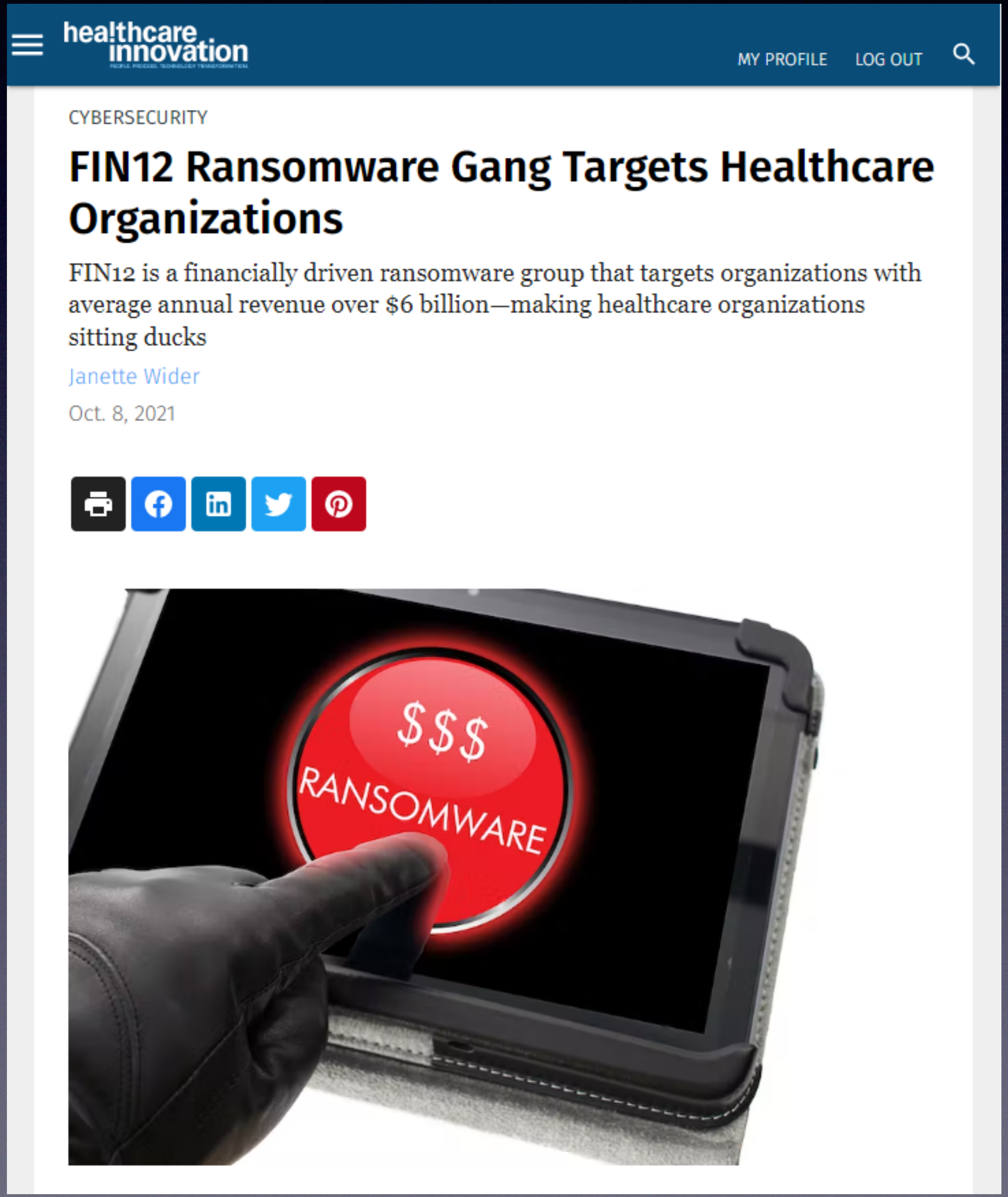
The hospital said it's prepared to continue providing care to patients without access to computer records.

Author: WTHR.com staff
Published: 8:42 PM EDT October 2, 2021
Updated: 9:32 PM EDT October 3, 2021

[redacted], Ind. — Another central Indiana hospital has fallen victim to a cyberattack.

Organized Cyber Crime – FIN12

- Not your average geeks, cyber cartel
- Annual Revenue: $6B
- Preferred weapon: Ryuk Ransomware
- Preferred target: Healthcare Facility
- Method of Operation: Using a sophisticated bot-net, loosely affiliated attackers deploy ransomware, encrypting victim devices. Attack ends with the ransom notification and demand for cryptocurrency payment.
- Responsible for at least one death, likely more



CYBERSECURITY

FIN12 Ransomware Gang Targets Healthcare Organizations

FIN12 is a financially driven ransomware group that targets organizations with average annual revenue over $6 billion—making healthcare organizations sitting ducks

Janette Wider

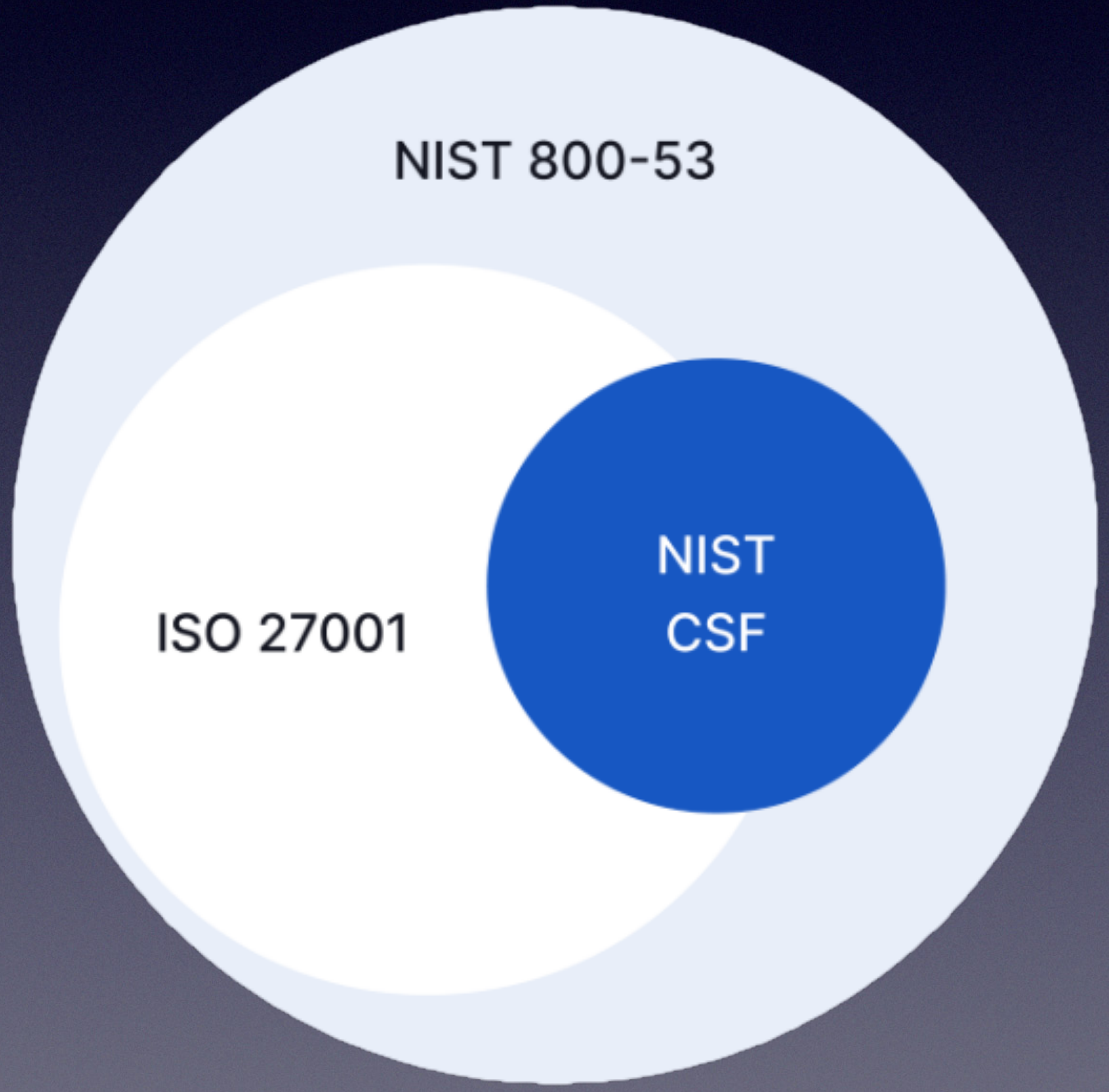
Oct. 8, 2021

Finance Cyber Compliance Regulations

- General Data Protection Regulation (GDPR)
- Sarbanes-Oxley
- PCI DSS
- Bank Secrecy Act (BSA)
- Gramm-Leach-Bliley Act (GLBA)

Meeting Finance Cyber Compliance

- Assets - Asset, Change, and Configuration Management
- Threats - Threat Modeling
- Vulnerabilities - Vulnerability Management
- Risks - Risk Management
- Roles - Identity & Privileged Access Management (IAM, PIM)
- Response - Event and Incident Response, Continuity of Operations
- 3rd Parties - Third-Party Risk Management (TRPM)
- Architecture - Cybersecurity Architecture
- Program - Cybersecurity Program Management



Preventative Measures

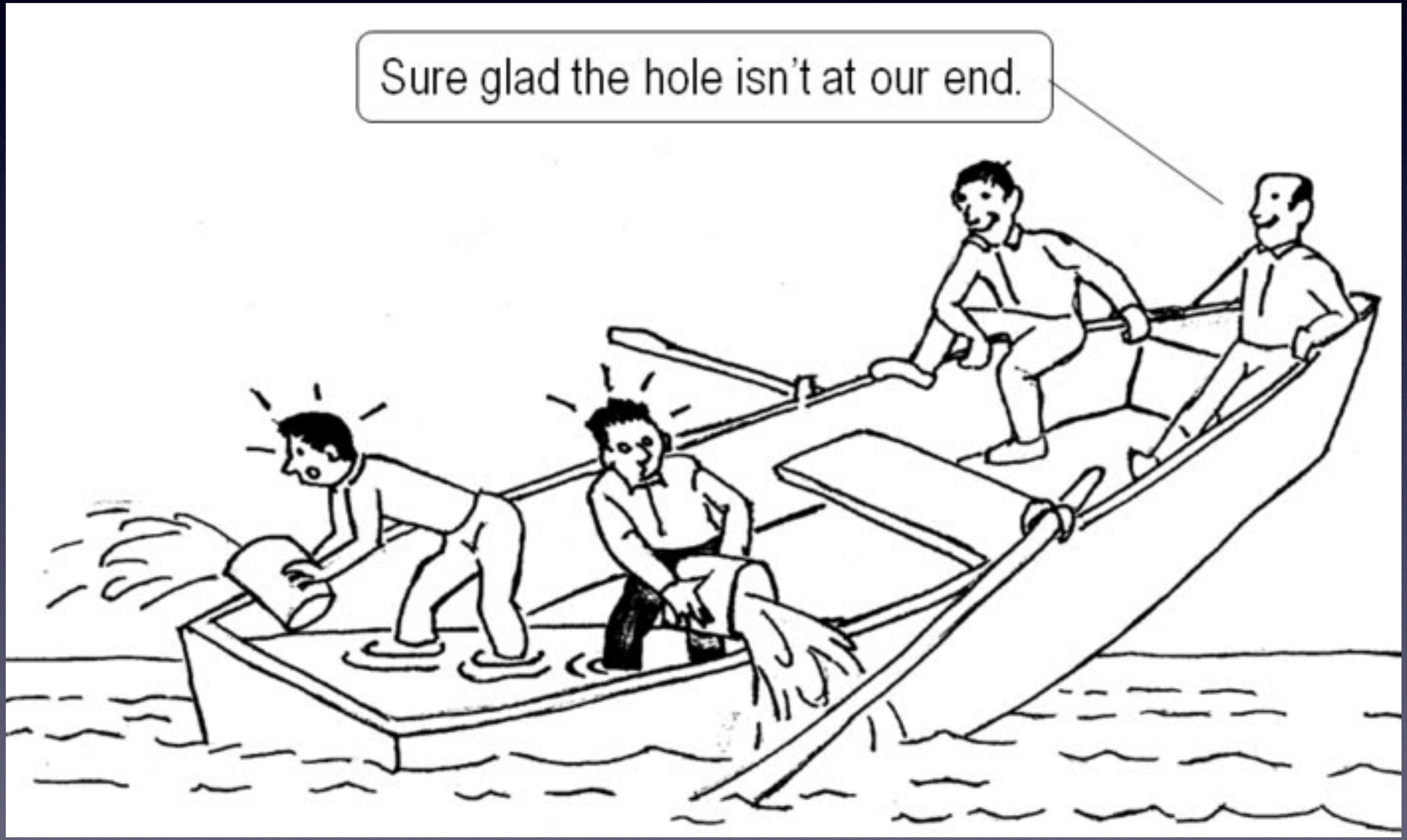
- Cybersecurity Insurance
- Everyone Has a Role
- Email Security

Cyber Insurance

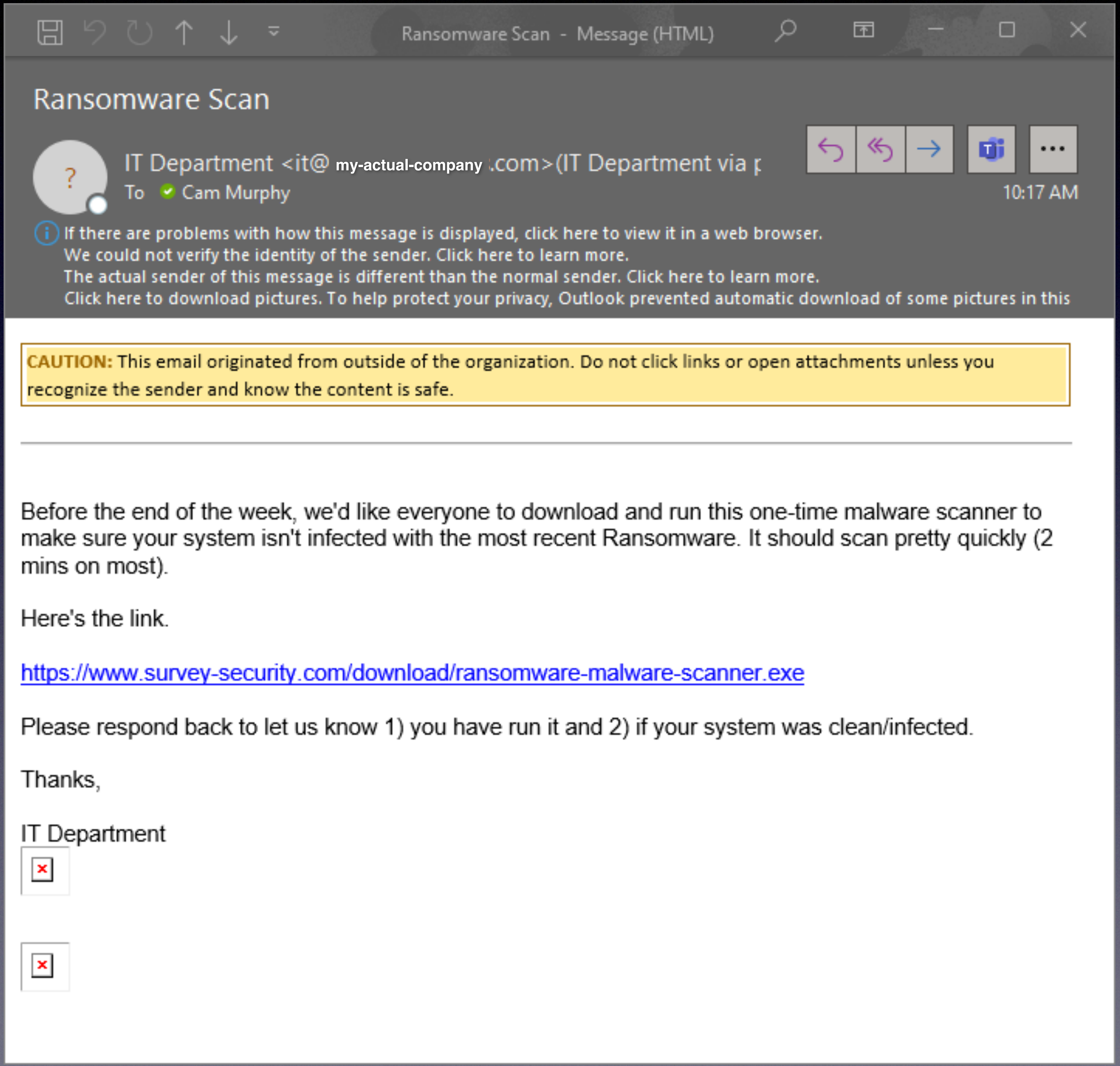
- 78% of large organizations are now opting for cyber insurance
- 93% of organizations with insurance coverage report 2022 renewal process requires more details of current cybersecurity posture
- 51% reported increased cyber protection was required to qualify

Everyone Has a Role

- “That’s not my job” could not be more wrong
  - Cybersecurity is a moving target. It’s all hands on deck!
- Cyber domain connects all aspects of our lives.
- “We have always done it that way”
  - The most expensive business philosophy
- Your company has YOUR DATA too… help them protect it!



Email Security



Ransomware Scan

IT Department <it@ my-actual-company .com>(IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

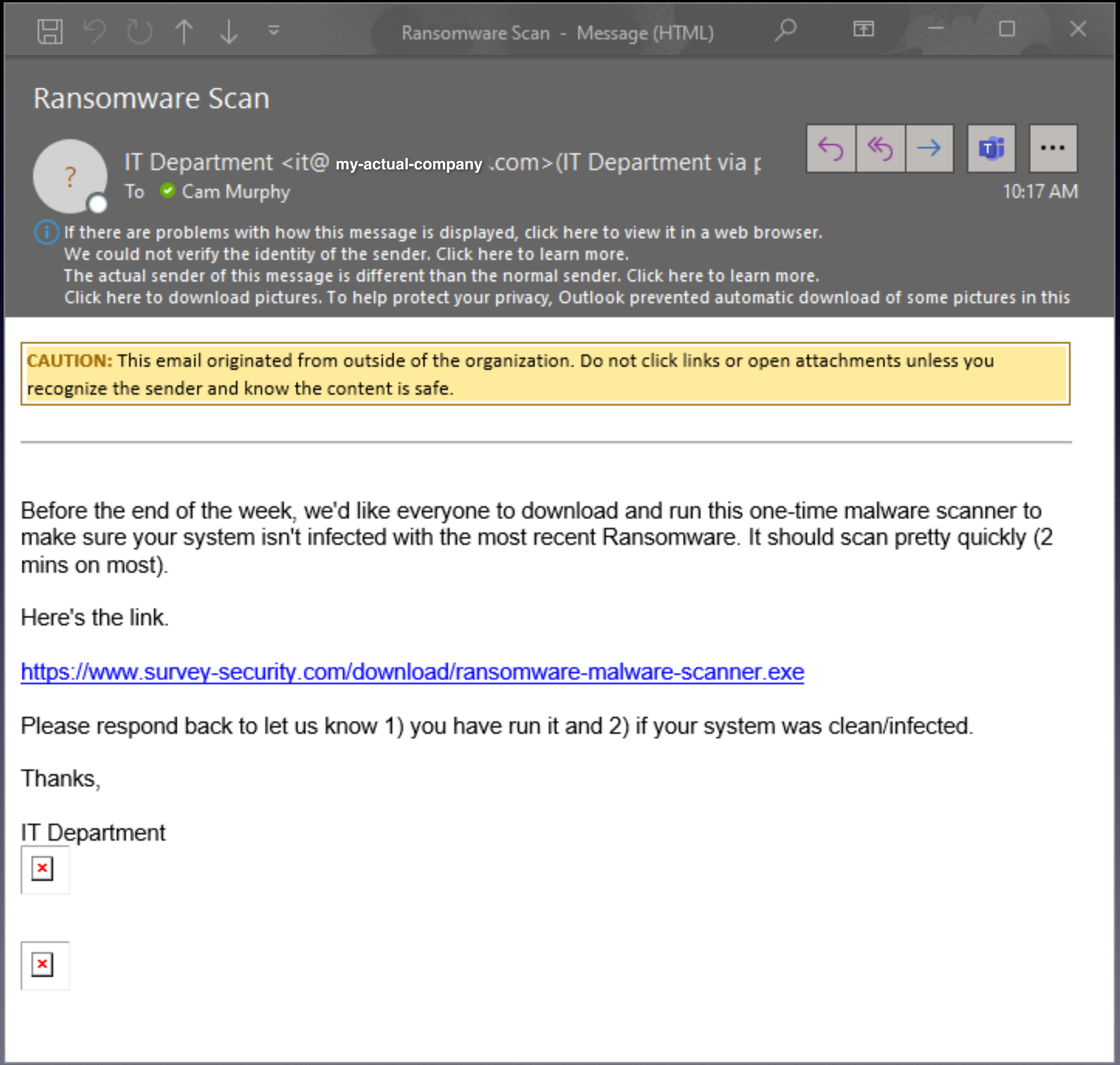
Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

IT Department

Email Security

Red Flags:



Ransomware Scan

IT Department <it@ my-actual-company .com>(IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

IT Department

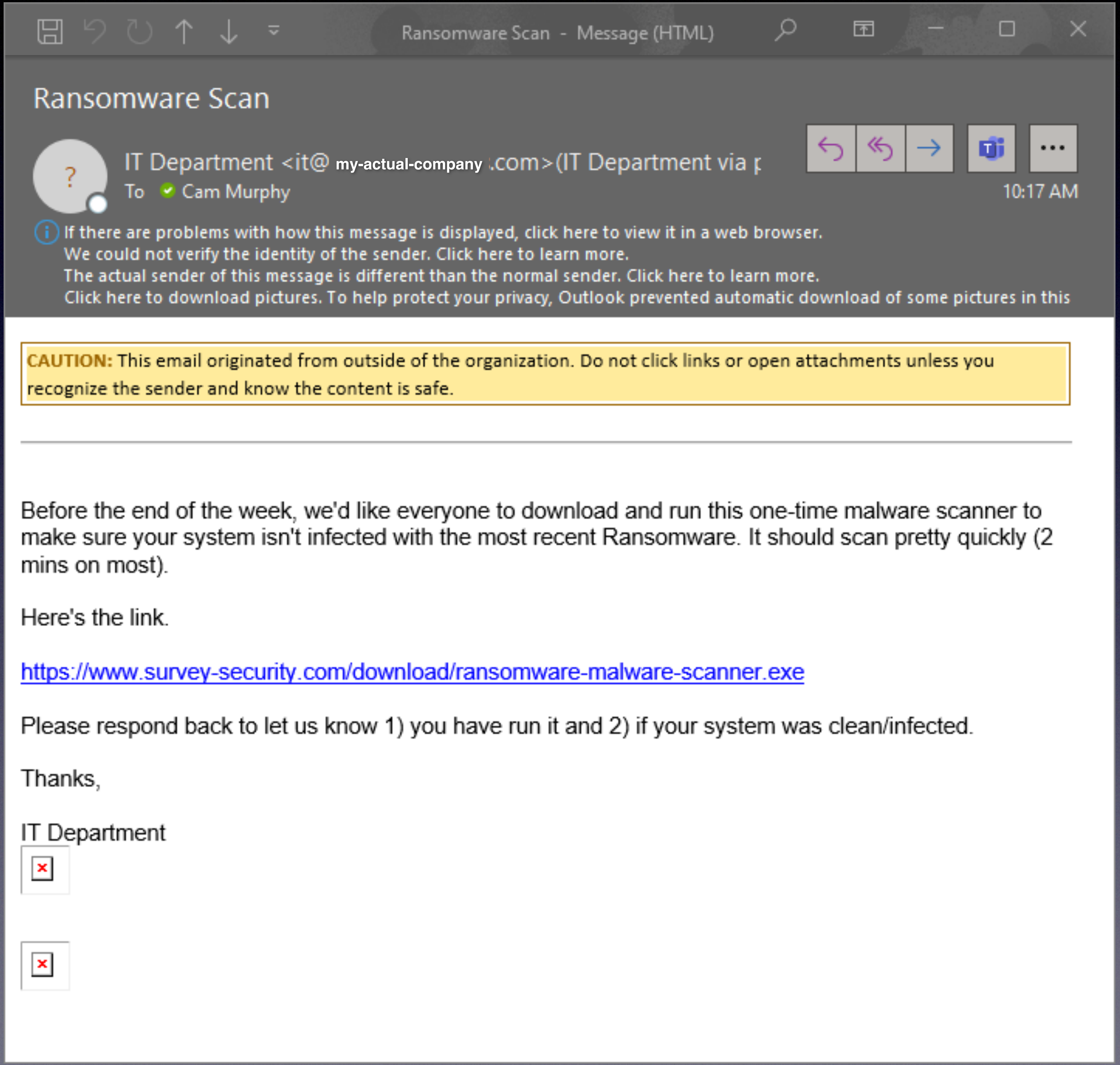
Email Security

Red Flags:

- From IT@my-actual-company.com

🚩
- External Organization Banner

- Verify URL link
  - www.survey-security.com



Ransomware Scan

IT Department <it@ my-actual-company .com>(IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

IT Department

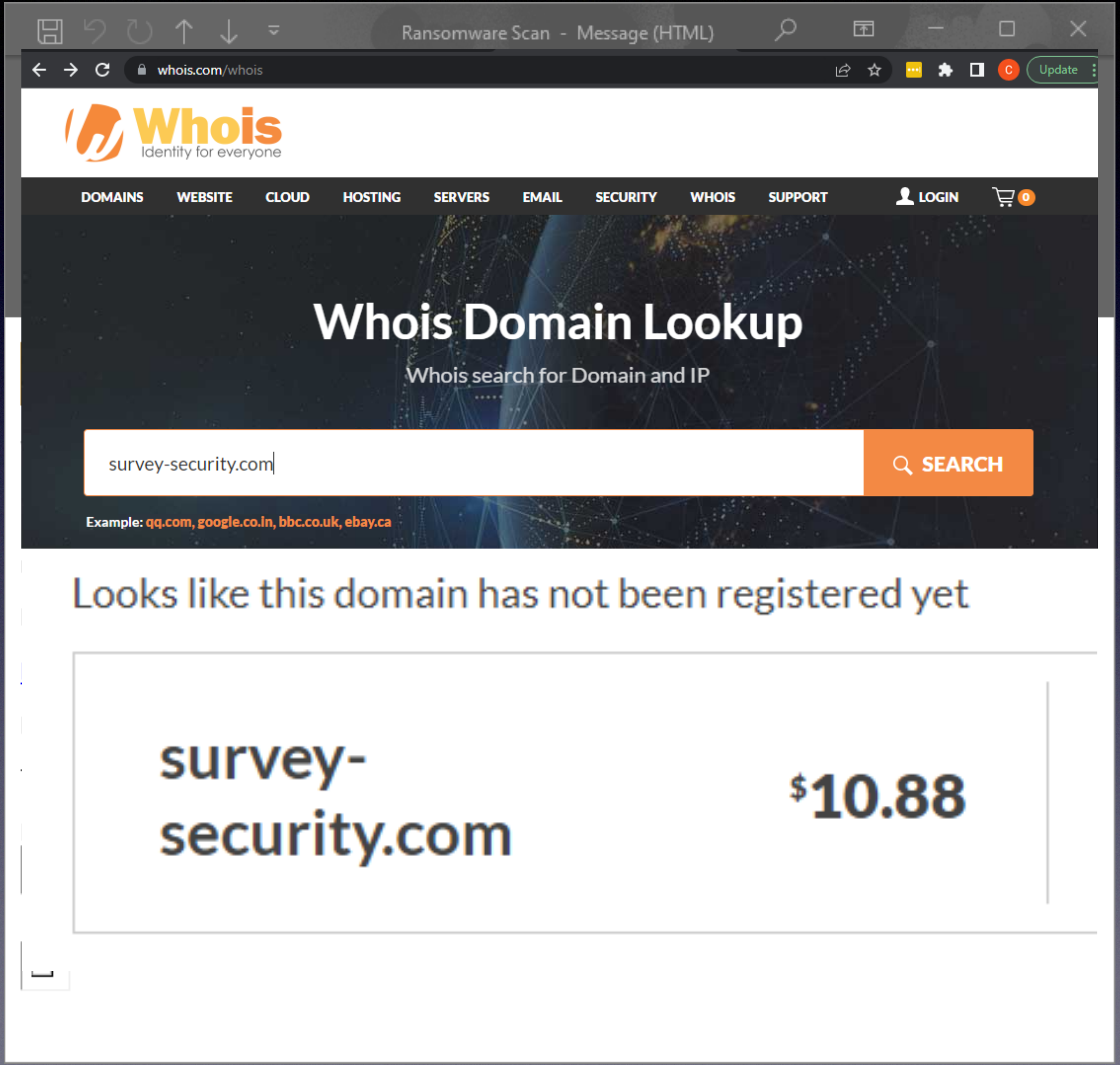
Email Security

Red Flags:

- From IT@my-actual-company.com

  - External Organization Banner

- Verify URL link
  - www.survey-security.com



Ransomware Scan - Message (HTML)

whois.com/whois

Whois Domain Lookup

Whois search for Domain and IP

survey-security.com

SEARCH

Example: qq.com, google.co.in, bbc.co.uk, ebay.ca

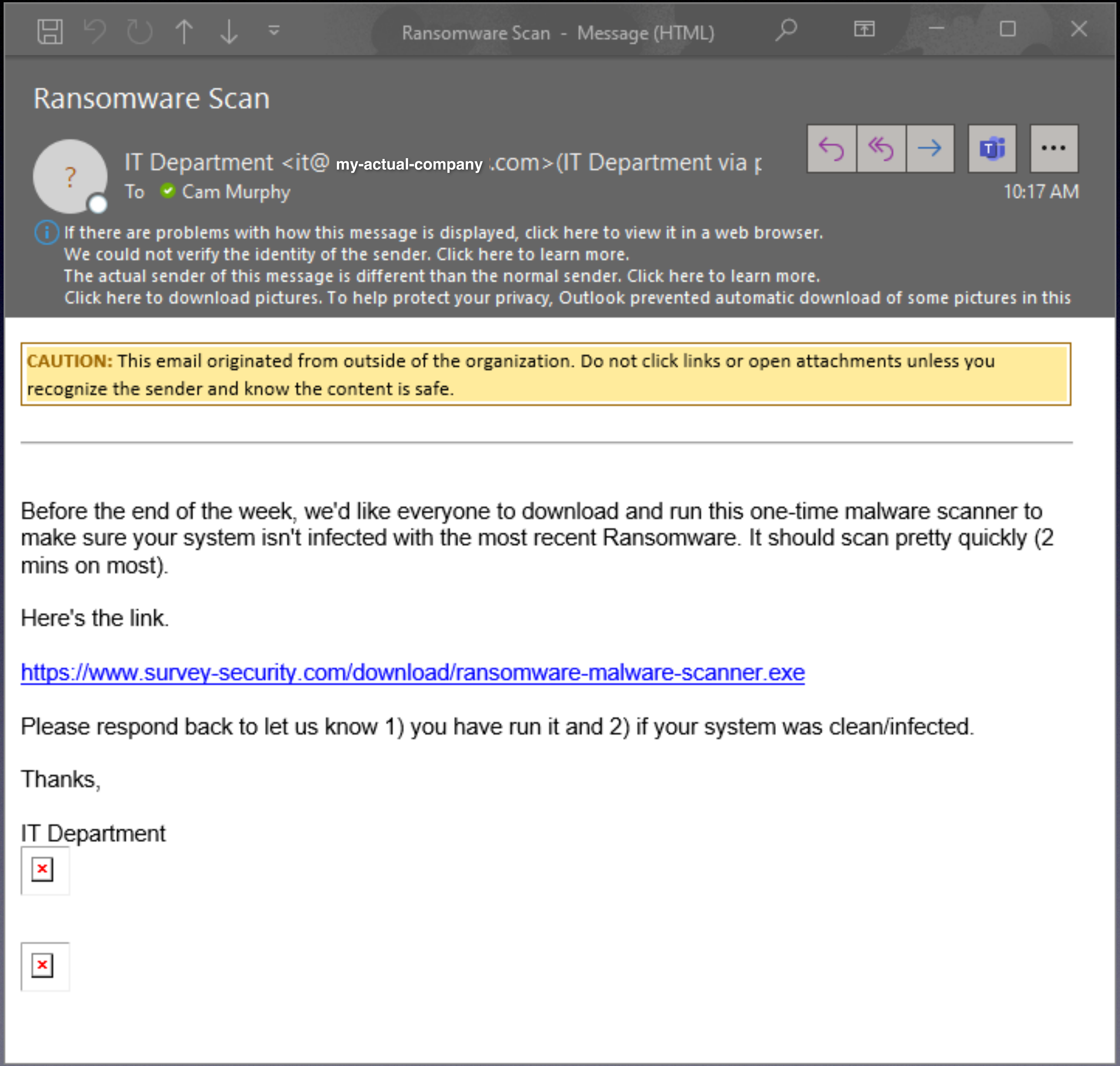
Looks like this domain has not been registered yet

survey-security.com $10.88

Email Security

Red Flags:

- From IT@my-actual-company.com
  - 🚩 External Organization Banner
- Verify URL link
  - www.survey-security.com
  - 🚩 Domain is not registered
  - 🚩 Mouse-Hover reveals actual URL



Ransomware Scan

IT Department <it@ my-actual-company .com>(IT Department via p
To Cam Murphy
10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

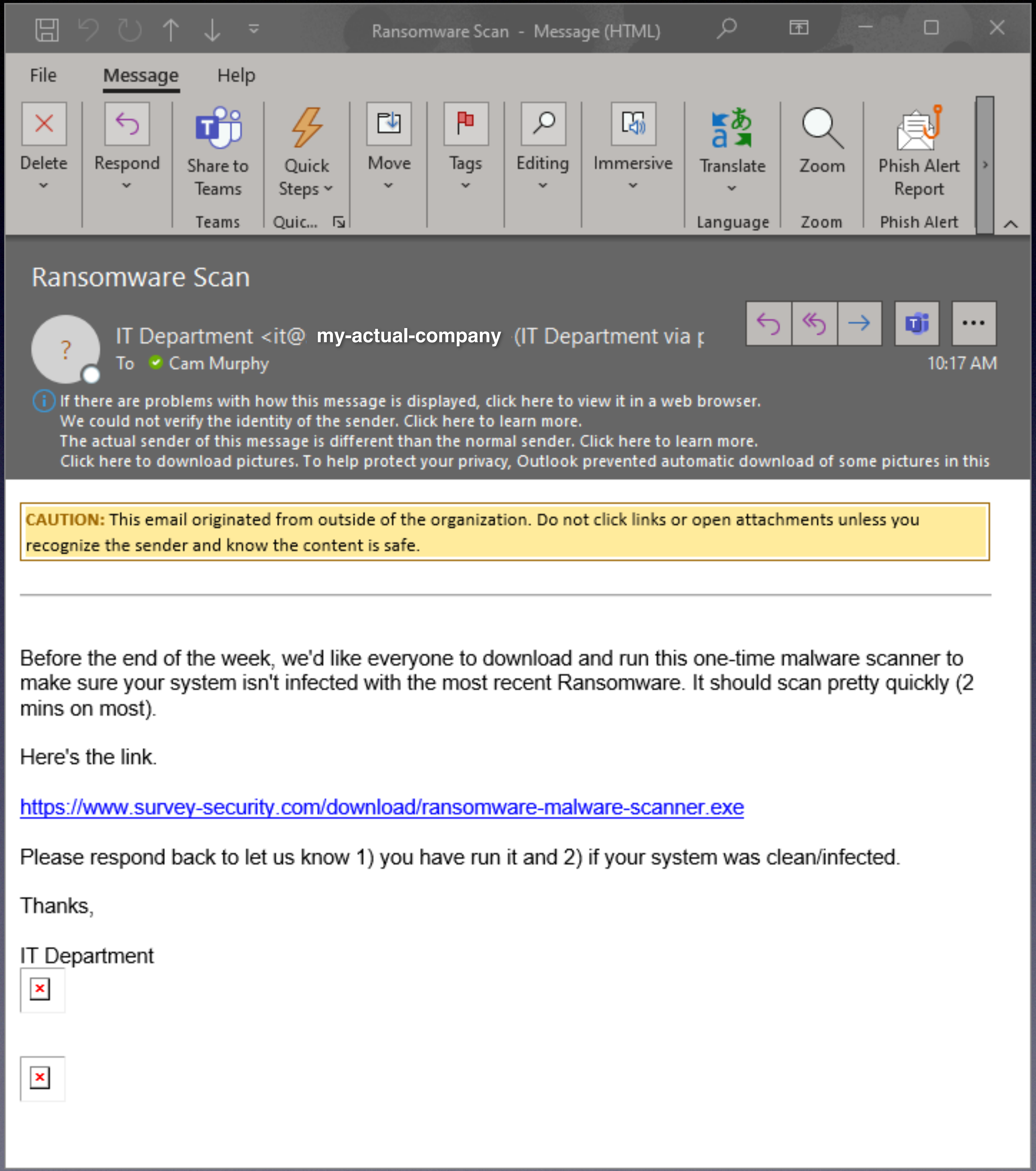
Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

IT Department

Email Security

What Do I Do?



Ransomware Scan

IT Department <it@ my-actual-company (IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

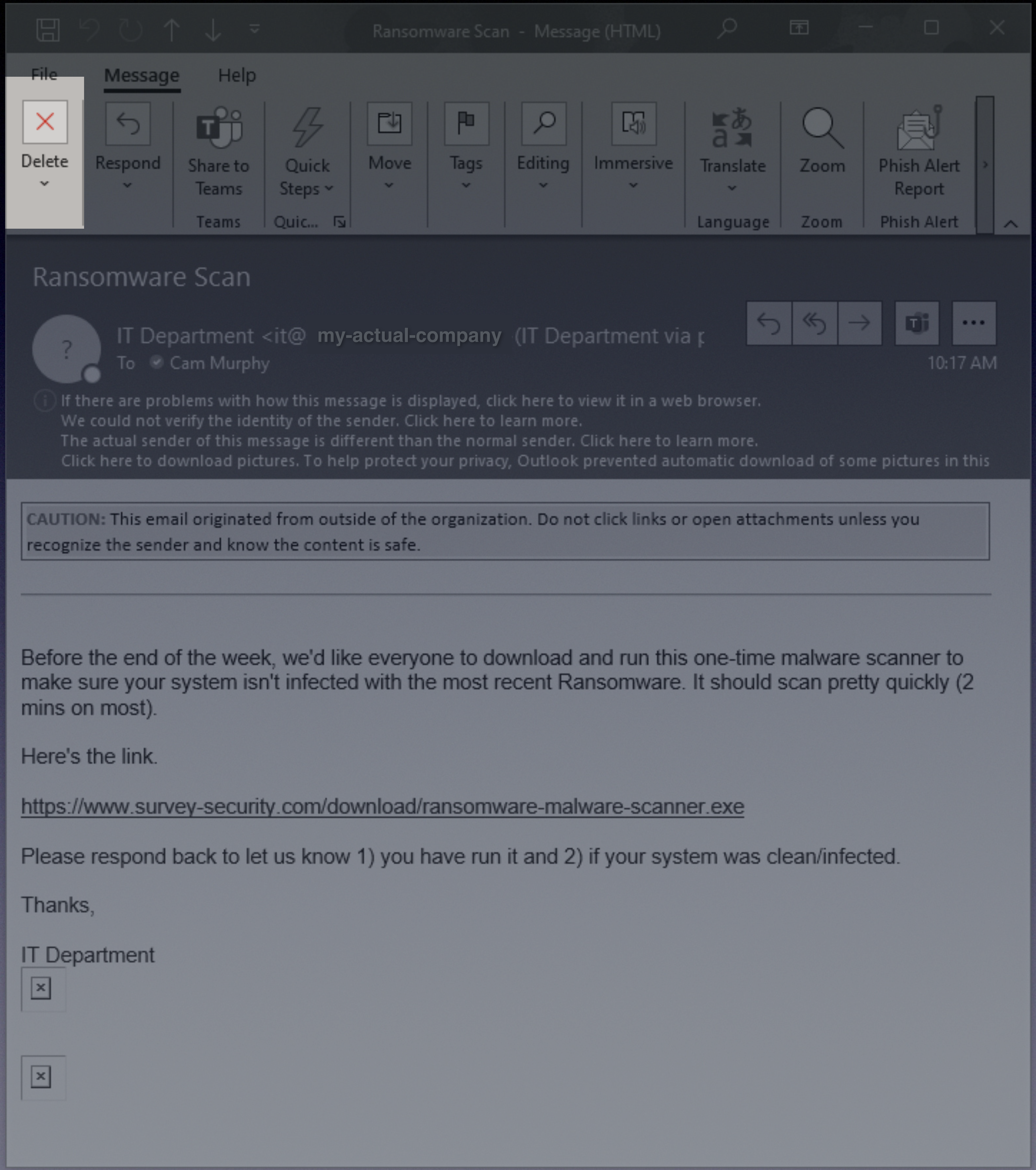
Thanks,

IT Department

Email Security

What Do I Do?

Ignore, Delete ★☆☆



Ransomware Scan

IT Department <it@ my-actual-company (IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

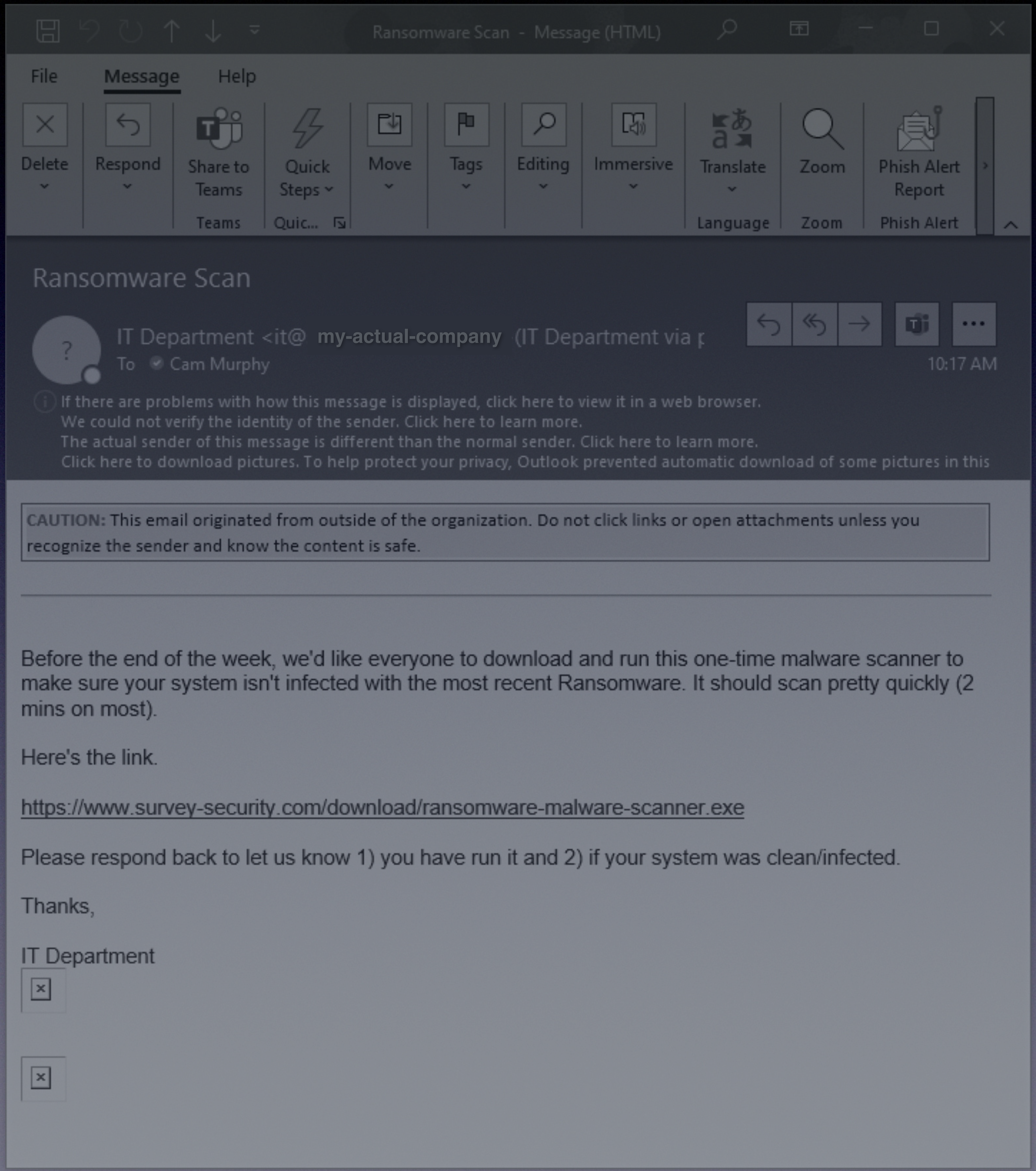
IT Department

Email Security

What Do I Do?

Ignore, Delete ★☆☆

Notify cyber team ★★☆



Ransomware Scan

IT Department <it@ my-actual-company (IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

https://www.survey-security.com/download/ransomware-malware-scanner.exe

Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

IT Department

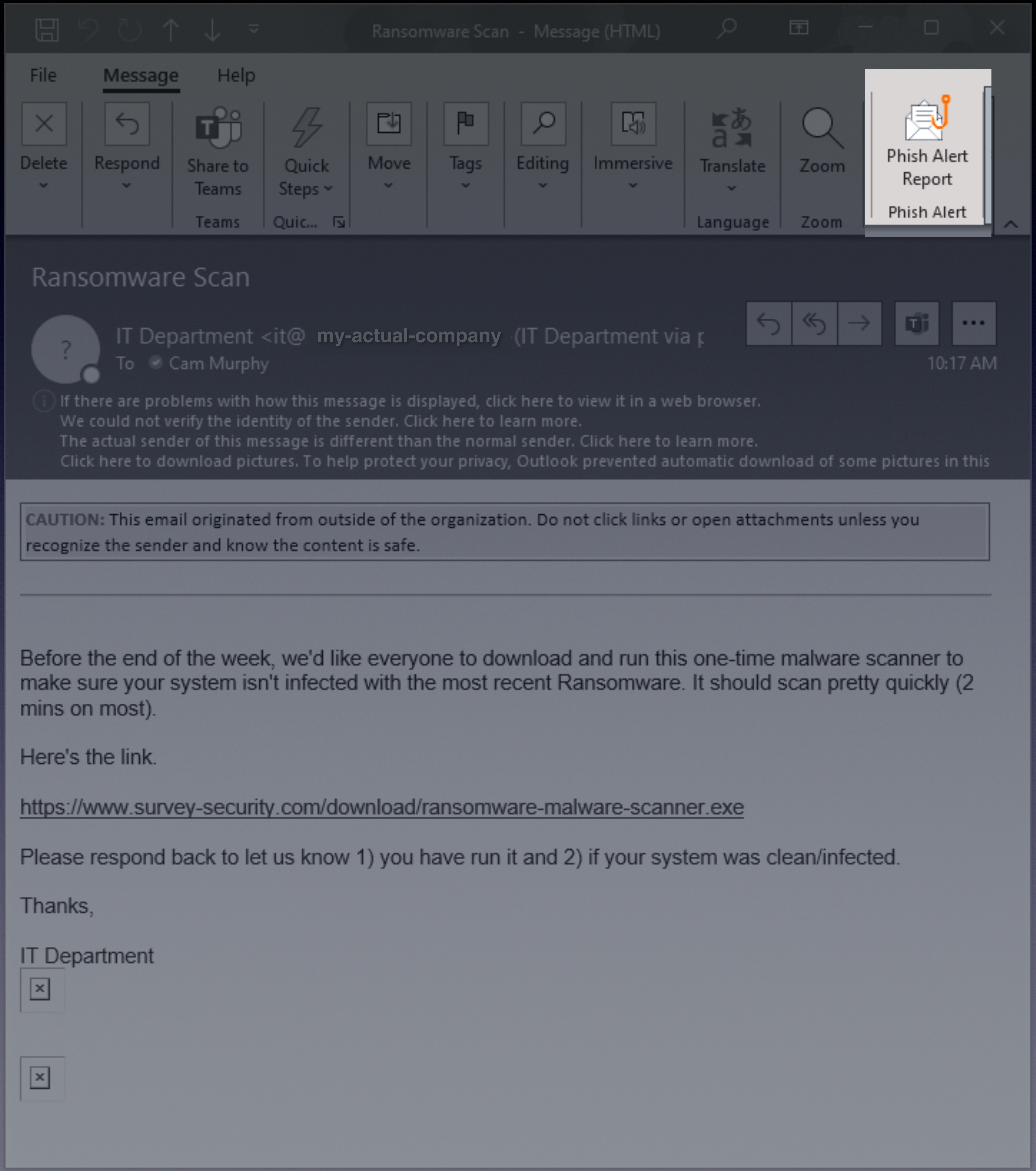
Email Security

What Do I Do?

Ignore, Delete ★☆☆

Notify cyber team ★★☆

Integrated Reporting ★★★



Ransomware Scan

IT Department <it@ my-actual-company (IT Department via p

To Cam Murphy

10:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Before the end of the week, we'd like everyone to download and run this one-time malware scanner to make sure your system isn't infected with the most recent Ransomware. It should scan pretty quickly (2 mins on most).

Here's the link.

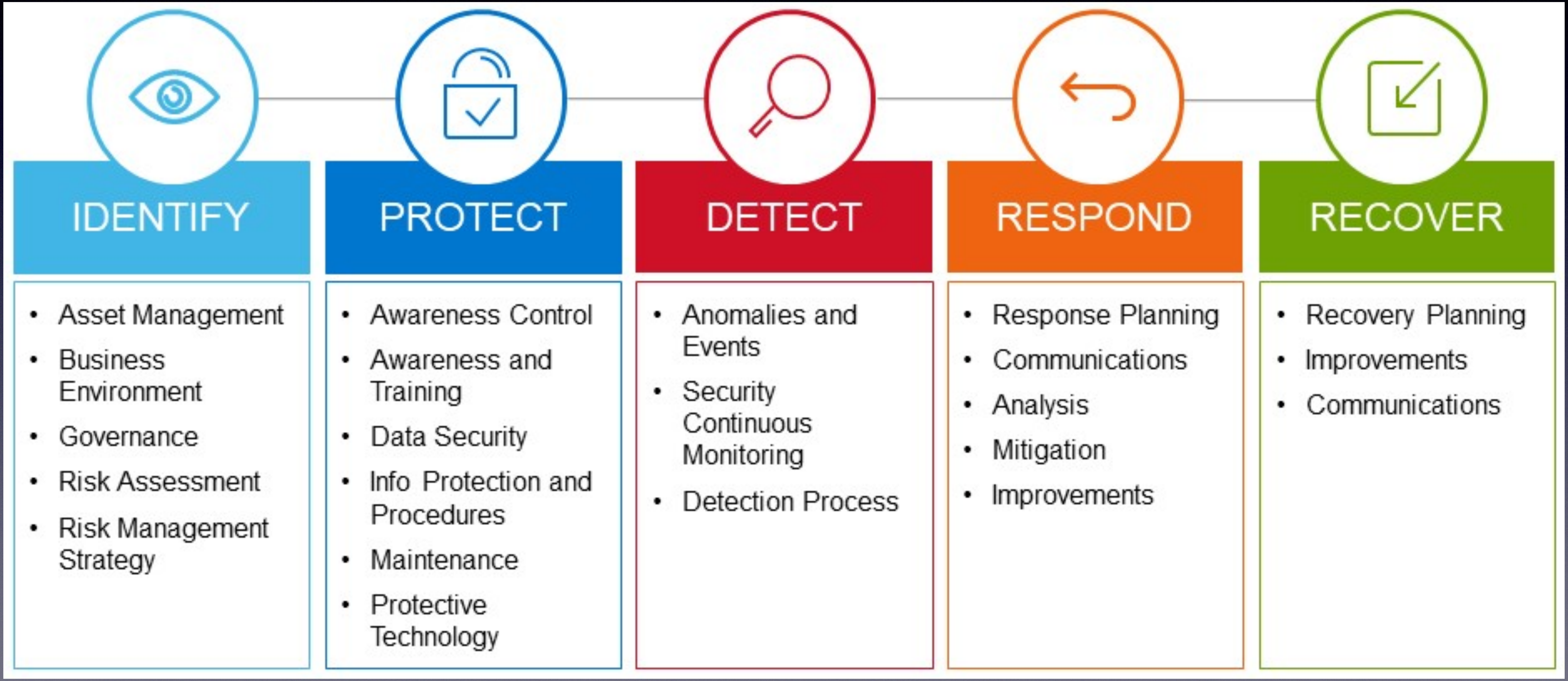
https://www.survey-security.com/download/ransomware-malware-scanner.exe

Please respond back to let us know 1) you have run it and 2) if your system was clean/infected.

Thanks,

IT Department

Big Picture, Little Details



IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Awareness Control
- Awareness and Training
- Data Security
- Info Protection and Procedures
- Maintenance
- Protective Technology

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvements
- Communications

Questions?

Contact me anytime with questions or concerns regarding your cybersecurity posture!

Cam Murphy
Cybersecurity Professional
jcmurph@mac.com
www.linkedin.com/in/Cam-Murphy