Business Email Compromise & Ransomware Threats – Best Practices

April 29, 2022

Michelle Tucker,
VP, Security Outreach Manager

Huntington
Welcome.®

Disclaimer

This presentation is intended for educational purposes only and does not replace independent professional judgment. Statements of fact and opinions expressed are those of the individual participants and, unless expressly stated to the contrary, are not the opinion or position of Huntington National Bank or its affiliates. Huntington does not endorse or approve, and assumes no responsibility for, the content, accuracy of completeness of the information presented. Professional assistance must be consulted prior to acting on any of the content in this presentation.

The Huntington National Bank is Member FDIC.

Welcome.

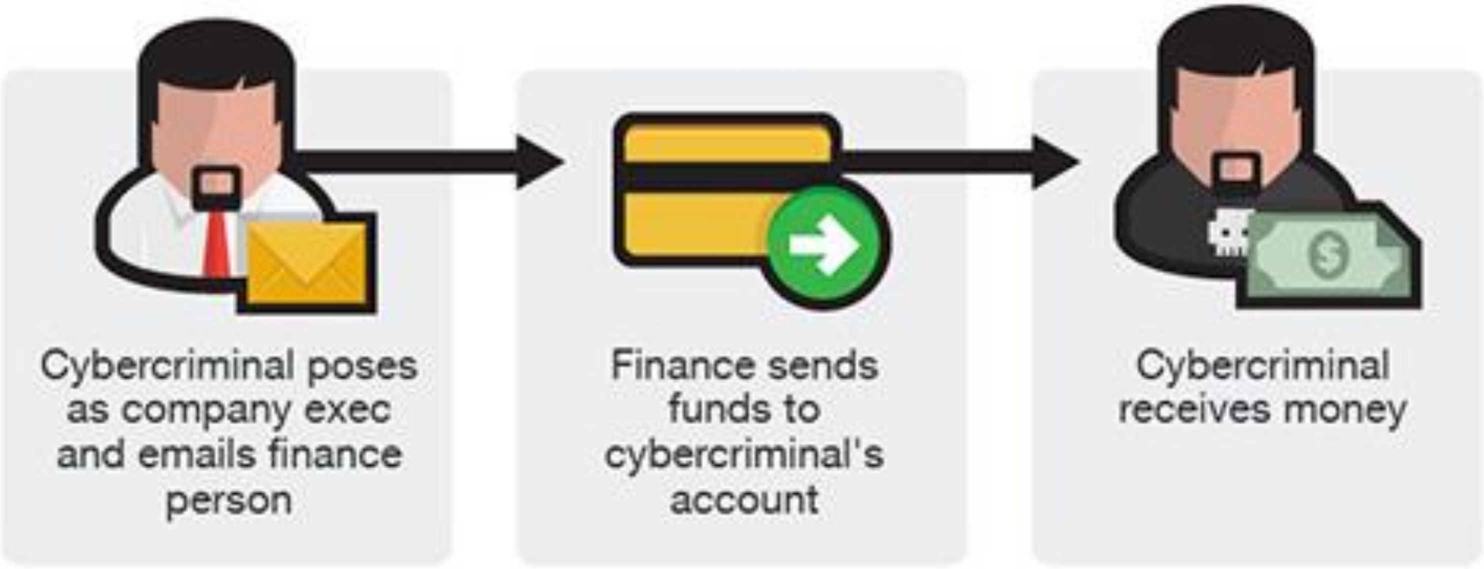
Agenda

- Business Email Compromise – Best Practices
- Ransomware Prevention – Best Practices
- Q&A

Huntington
Welcome.

Business E-mail Compromise (BEC)

Fraudulent communications luring employees to take actions which generally results in the movement of funds or disclosure of information



Cybercriminal poses as company exec and emails finance person

Finance sends funds to cybercriminal's account

Cybercriminal receives money

Is it really email compromise?

BEC VS. Phishing

Phishing generally involves the sending of fraudulent e-mails with the intent of luring a user to click a link or open a document, while **BEC** is typically a fraudster spoofing a user's email address to send fraudulent emails on their behalf.

Phishing typically results in:

- Compromise of the system: malware or ransomware
- Compromise of credentials: usernames, passwords, etc.

BEC typically results in:

- Disclosure of sensitive and/or personal information
- Movement of funds

BEC prevention training shares the common safeguards used with anti-phishing education courses

BEC Tactics

- Sense of urgency
- Timing – often near close of business on Friday
- Use of current crisis as topic or to increase urgency
- Increase in target development and sophistication
  - Gathering intelligence
  - Open source, social media
  - Social Engineering

Source: https://www.bankinfosecurity.com/bec-campaign-targets-hr-departments-report-a-13997
https://www.databreachtoday.com/ta505-apt-group-returns-new-techniques-report-a-13678

BEC: Case Study – Invoicing, Electronic Payment

Construction invoicing (St. Ambrose Catholic Parish)

1. Parish email server compromised
2. Fraudsters monitor communications
3. Valid invoice submitted to parish for payment
4. Fraudster spoofs message, as construction firm, to parish requesting a change in payment wire instructions

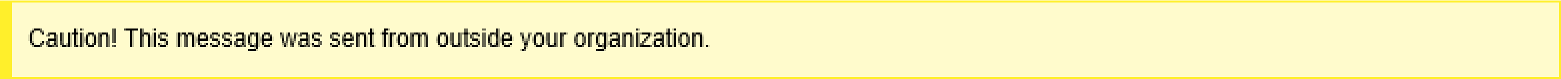
$1.75M LOST

Source: https://threatpost.com/bec-hack-cons-catholic-church/144212/
https://www.cleveland.com/crime/2019/04/email-hackers-steal-175-million-from-st-ambrose-catholic-parish-in-brunswick.html
https://www.news5cleveland.com/news/local-news/oh-cuyahoga/saint-ambrose-catholic-parish-victim-of-sophisticated-business-email-scheme-fbi-says
https://www.scmagazine.com/home/security-news/cybercrime/st-ambrose-catholic-parish-in-brunswick-ohio-was-hit-with-a-business-email-compromise-scam/

Detecting BEC - Red Flags:

The E-mail Bait

- E-mail address variation (user or domain name)
- Misspelling
- Sense of urgency in the request
- Change in email tone
- Removal of addressees on the email chain (cc or other addresses)



Caution! This message was sent from outside your organization.

Detecting BEC - Red Flags:

Procedural Clues

- Requests outside of normal procedures
- Change in payment instructions
- Change in vendor
- Changes to phone number
- Beneficiary changes (from account to account)
- Name/Account mismatch; Returned wires

Know your customer

- If client phone is never answered or goes directly to VM
- Cultural changes/differences; Changes in customer behavior

Know your suppliers

Best Practices:

People

- Educate your employees – Share BEC threats and scams
- Limit publicly available information
  - Contact, organizational structure, process info

Process

- Well documented processes; Periodically reviewed/updated
- Evaluate all processes for potential fraud trouble spots
- Implement multiple controls
  - Call back procedures for verification (e.g. payment change)
  - Voice Approval
  - Use phone numbers that are on file (not passed in email) for call back
  - Dual authorization – look out for each other!]

Technology

- Independent assessment or “Red team” all processes/controls
- Report and save all emails of suspected BEC
- Use two-factor authentication on accounts that support it. Never disable it
- Disable or monitor the use of email auto-forward
- Protect your brand/domain – monitor for spoofed domain; Implement DMARC, BIMI

Source: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

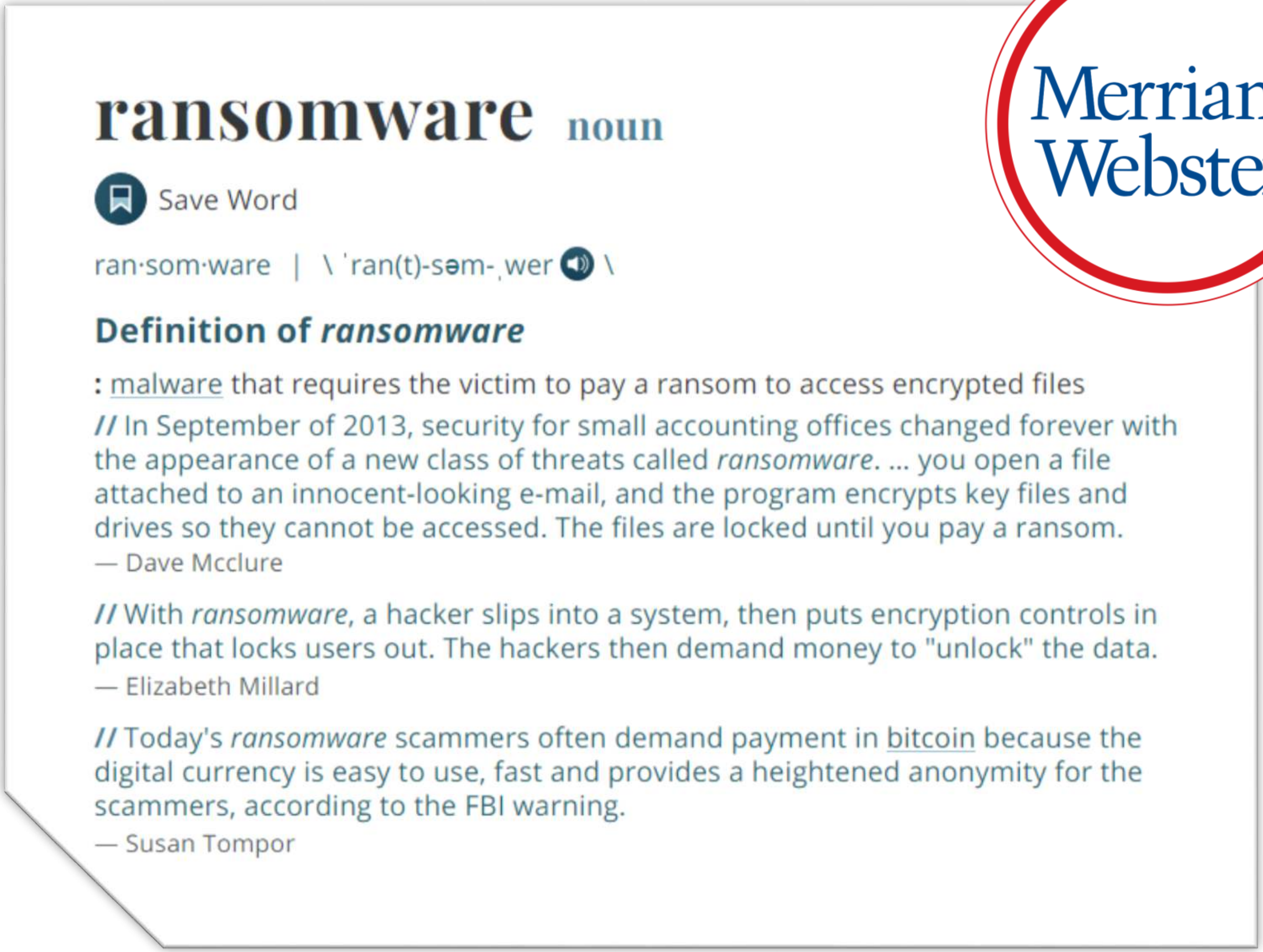
What to do if you suspect BEC

If you or your company fall victim to a BEC scam, it's important to act quickly:

- Contact your financial institution immediately to request that they contact the financial institution where the transfer was sent.
- Report the crime to your FBI Field Office.
- File a complaint with the FBI's Internet Crime Complaint Center.
- Contact your Cybersecurity Insurance Carrier and engage forensic and remediation services

Source: https://www.fbi.gov/contact-us/field-offices
https://www.ic3.gov/default.aspx

Ransomware - Definition



ransomware noun

Save Word

ran·som·ware | \ ˈran(t)-səm-ˌwer \

Definition of *ransomware*

: malware that requires the victim to pay a ransom to access encrypted files

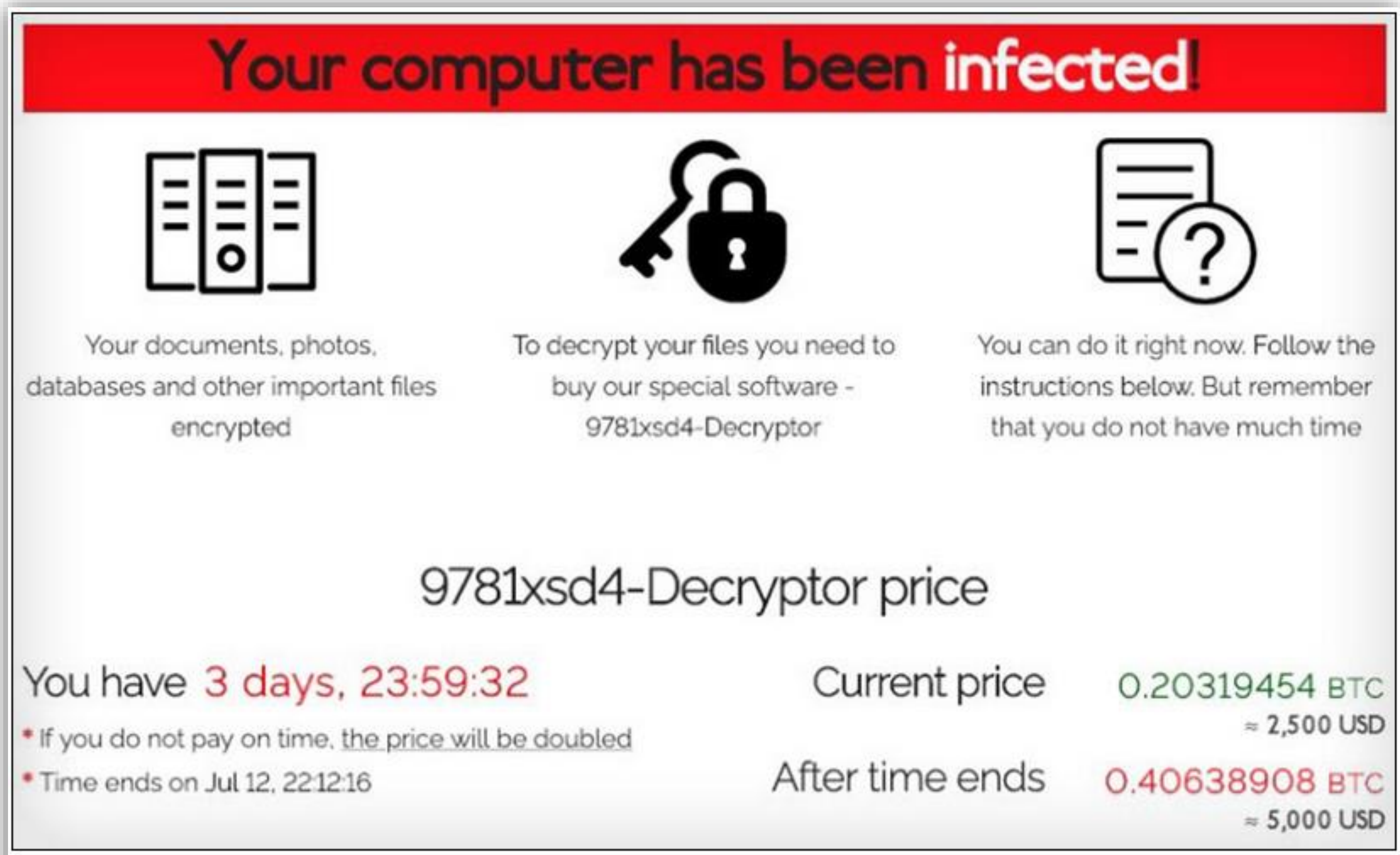
// In September of 2013, security for small accounting offices changed forever with the appearance of a new class of threats called *ransomware*. ... you open a file attached to an innocent-looking e-mail, and the program encrypts key files and drives so they cannot be accessed. The files are locked until you pay a ransom.
— Dave Mcclure

// With *ransomware*, a hacker slips into a system, then puts encryption controls in place that locks users out. The hackers then demand money to "unlock" the data.
— Elizabeth Millard

// Today's *ransomware* scammers often demand payment in bitcoin because the digital currency is easy to use, fast and provides a heightened anonymity for the scammers, according to the FBI warning.
— Susan Tompor

Merriam-Webster®

Source: https://www.merriam-webster.com/dictionary/ransomware?src=search-dict-hed
Logo -



Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - 9781xsd4-Decryptor

You can do it right now. Follow the instructions below. But remember that you do not have much time

9781xsd4-Decryptor price

You have 3 days, 23:59:32

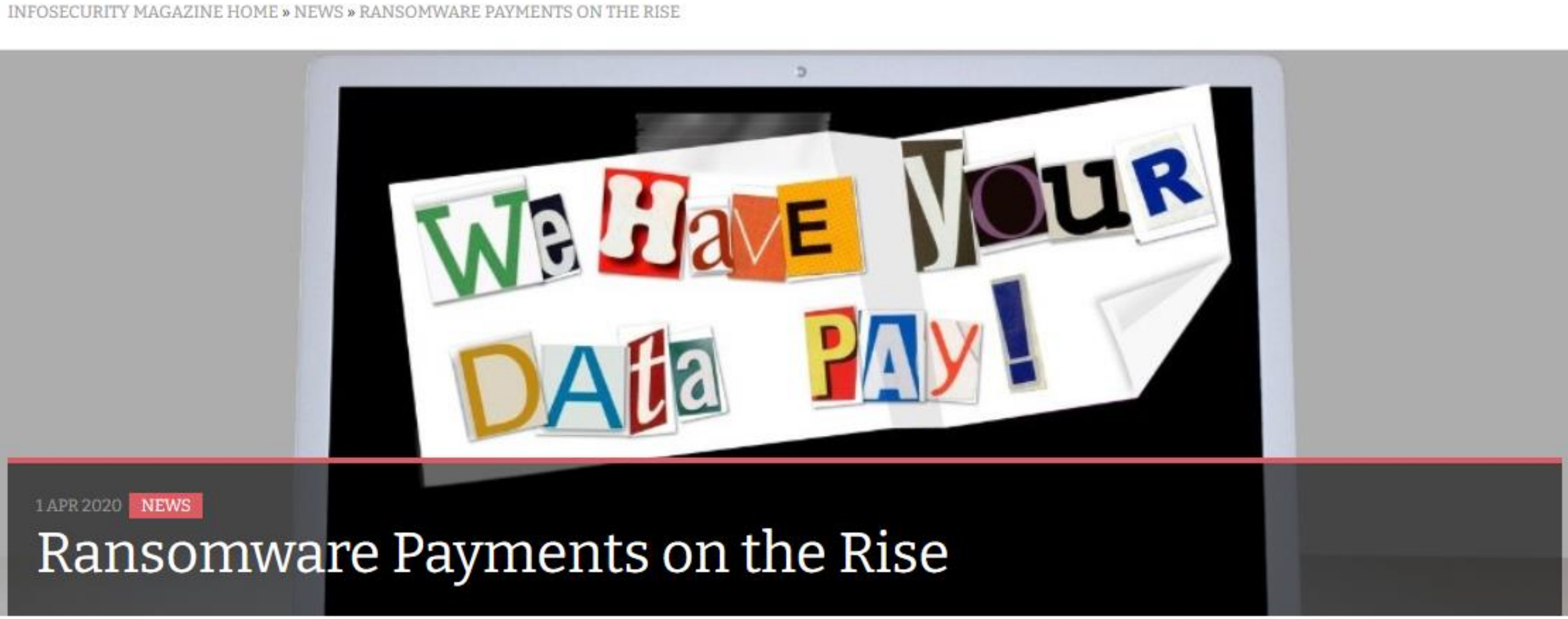
* If you do not pay on time, the price will be doubled

* Time ends on Jul 12, 22:12:16

Current price 0.20319454 BTC ≈ 2,500 USD

After time ends 0.40638908 BTC ≈ 5,000 USD

Sodinokibi/REevil self-service decryptor page, reachable by the anonymizing Tor browser (Source: Secureworks)

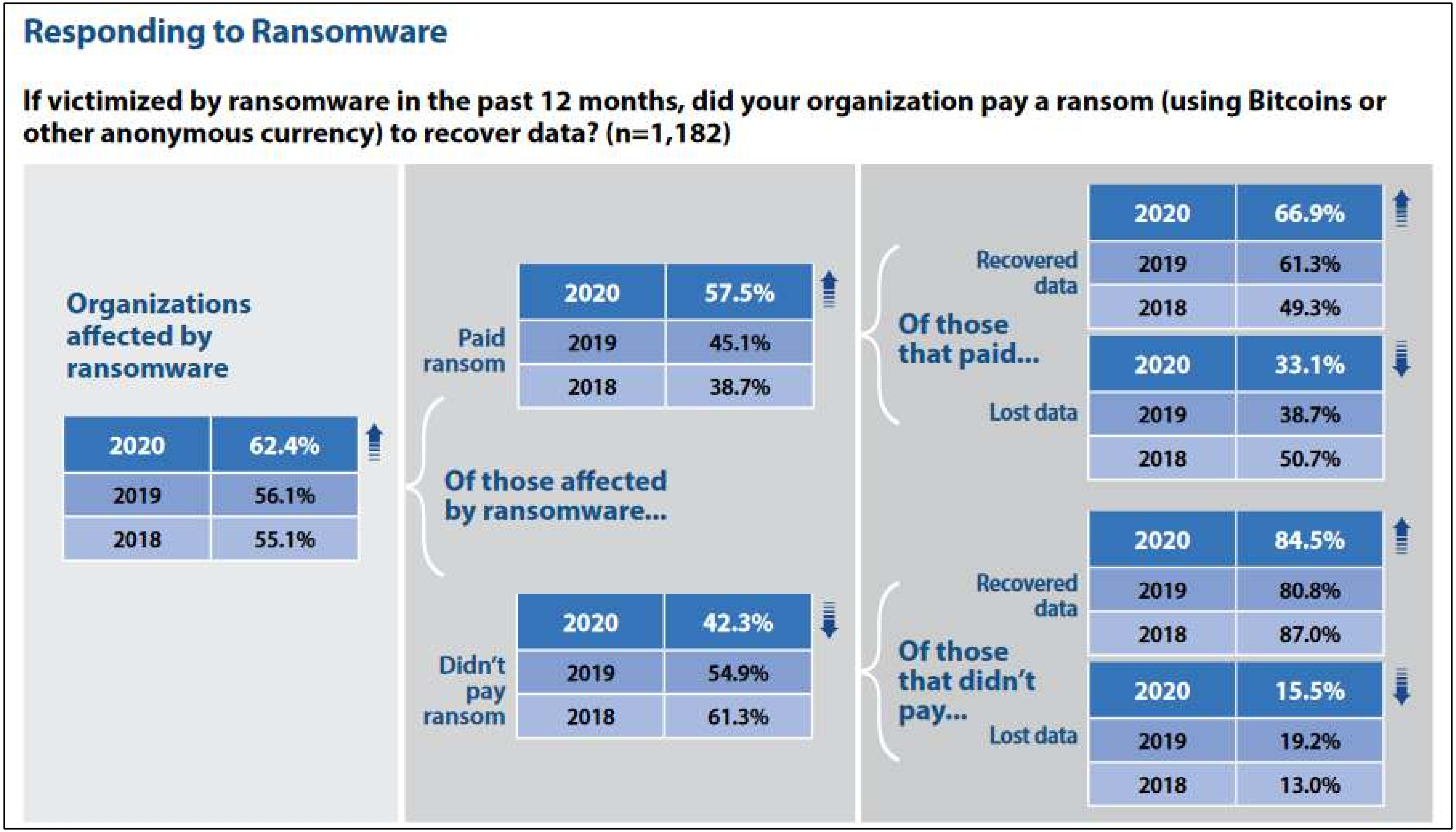


INFOSECURITY MAGAZINE HOME » NEWS » RANSOMWARE PAYMENTS ON THE RISE

1 APR 2020 NEWS

Ransomware Payments on the Rise

Source: https://www.infosecurity-magazine.com/news/rise-in-ransomware-payments/



Responding to Ransomware

If victimized by ransomware in the past 12 months, did your organization pay a ransom (using Bitcoins or other anonymous currency) to recover data? (n=1,182)

Organizations affected by ransomware

2020	62.4%	↑
2019	56.1%	
2018	55.1%	

Of those affected by ransomware...

Paid ransom

2020	57.5%	↑
2019	45.1%	
2018	38.7%	

Didn't pay ransom

2020	42.3%	↓
2019	54.9%	
2018	61.3%	

Of those that paid...

Recovered data

2020	66.9%	↑
2019	61.3%	
2018	49.3%	

Lost data

2020	33.1%	↓
2019	38.7%	
2018	50.7%	

Of those that didn't pay...

Recovered data

2020	84.5%	↑
2019	80.8%	
2018	87.0%	

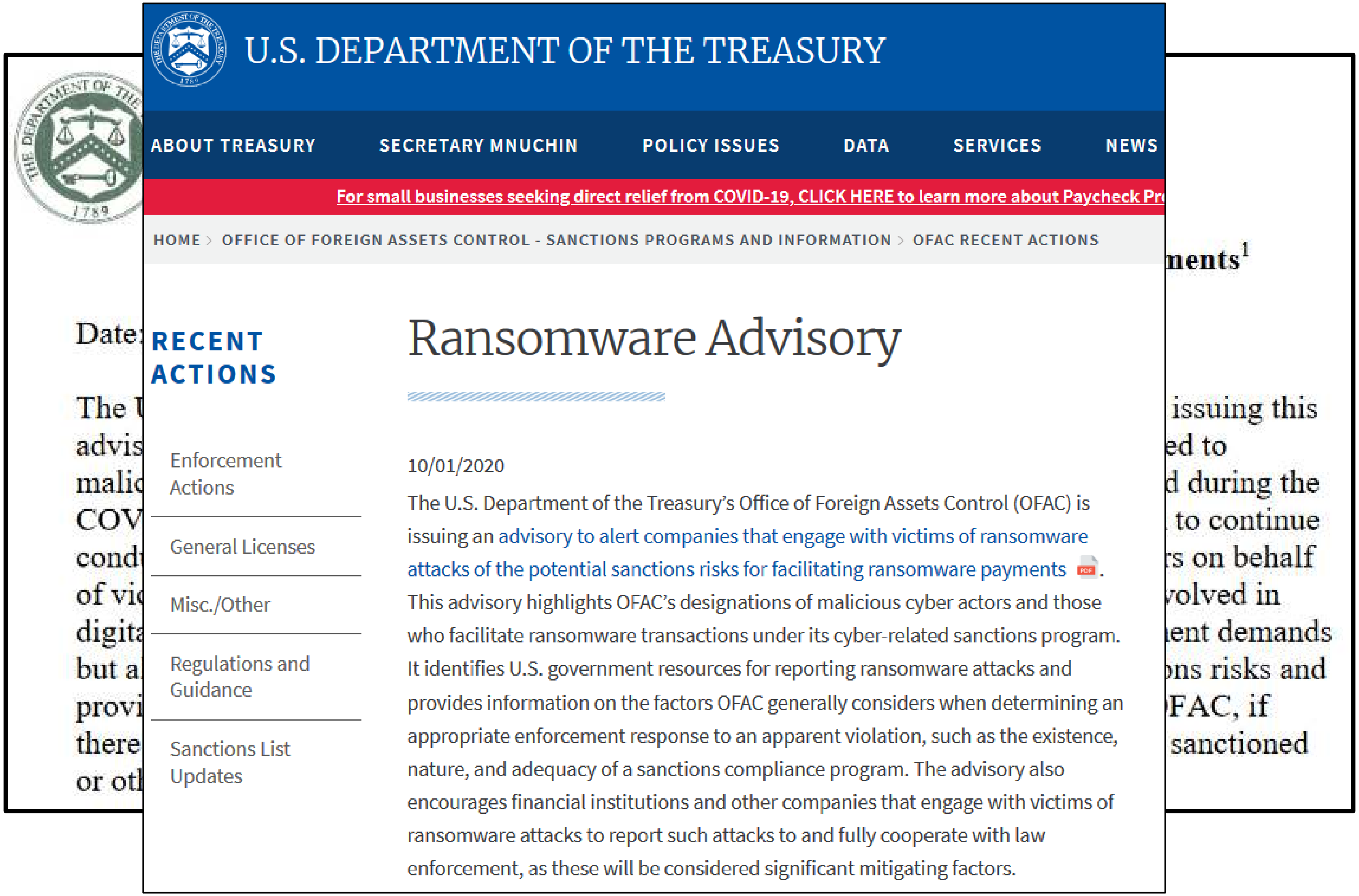
Lost data

2020	15.5%	↓
2019	19.2%	
2018	13.0%	

Source: https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf

As if getting your data back wasn't bad enough …

- Hush Money
- Name and Shame
- Leak Prevention
- Auction Prevention
- Deletion Promise



U.S. DEPARTMENT OF THE TREASURY

ABOUT TREASURY
SECRETARY MNUCHIN
POLICY ISSUES
DATA
SERVICES
NEWS
For small businesses seeking direct relief from COVID-19, CLICK HERE to learn more about Paycheck Pr
HOME › OFFICE OF FOREIGN ASSETS CONTROL - SANCTIONS PROGRAMS AND INFORMATION › OFAC RECENT ACTIONS
RECENT ACTIONS
Enforcement Actions
General Licenses
Misc./Other
Regulations and Guidance
Sanctions List Updates

Ransomware Advisory

10/01/2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments. This advisory highlights OFAC's designations of malicious cyber actors and those who facilitate ransomware transactions under its cyber-related sanctions program. It identifies U.S. government resources for reporting ransomware attacks and provides information on the factors OFAC generally considers when determining an appropriate enforcement response to an apparent violation, such as the existence, nature, and adequacy of a sanctions compliance program. The advisory also encourages financial institutions and other companies that engage with victims of ransomware attacks to report such attacks to and fully cooperate with law enforcement, as these will be considered significant mitigating factors.

ments[1]

Date:

The U
advis
malic
COV
cond
of vi
digit
but a
provi
there
or ot

issuing this
ed to
d during the
to continue
s on behalf
volved in
ent demands
ns risks and
FAC, if
sanctioned

Source: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001

Ransomware – Increasing Threat

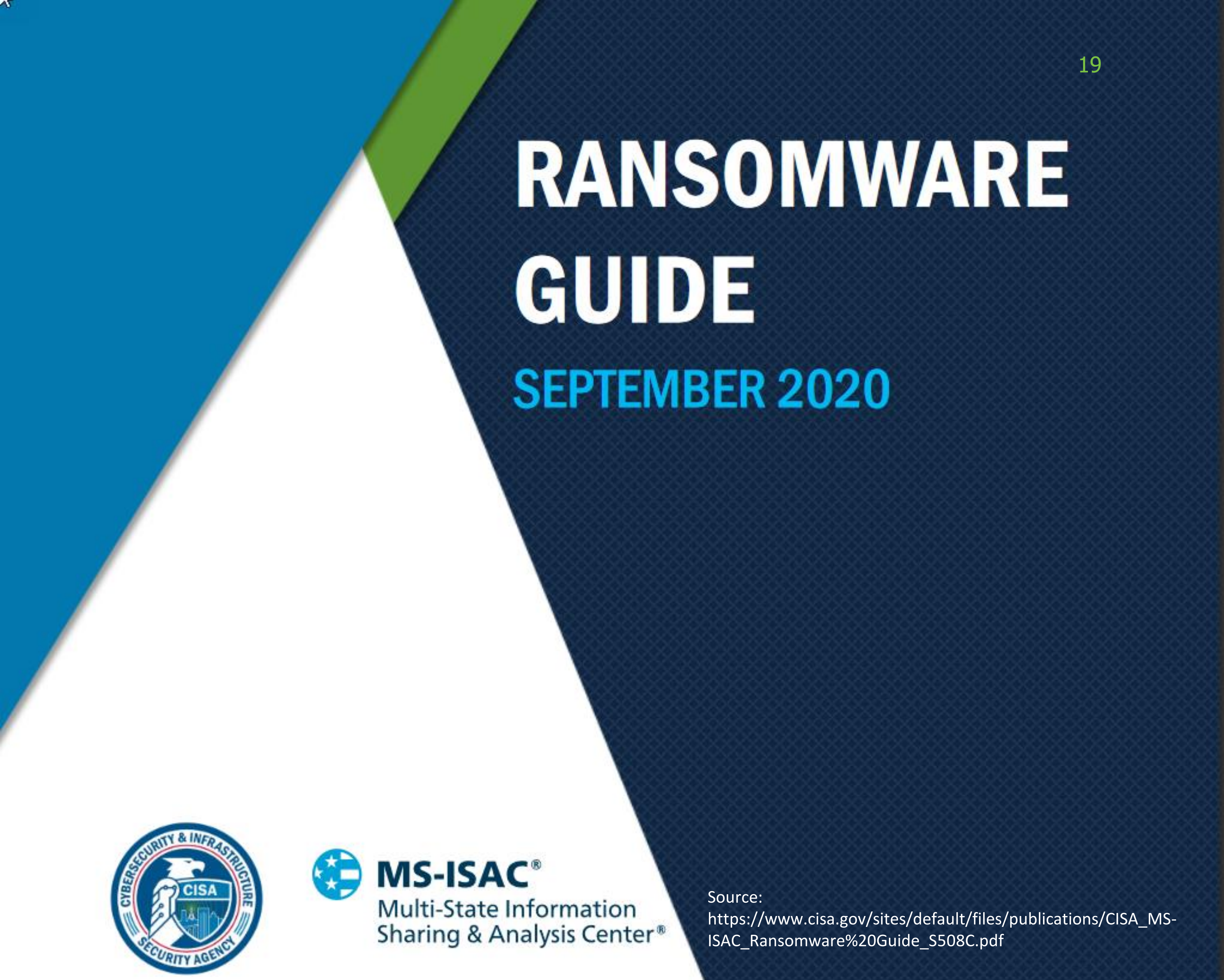
Huntington

- 7 per hour (and increasing)
- 65,000 attacks last year (2020) costing $1.4B
  - Only those that were reported
- Average Down Time – 21 days
- Average Days to recover - 287
- $350M paid in ransom (2020)
- Average Ransome Payment $312,493 (2020)
- Cybercrime damage in 2021 estimated to be $6T

Recent Ransomware Attacks

- Howard University – Sep 2021 – unknown
- Accenture – Aug 2021 - $50M
- Kaseya (1500 organizations) – Jul 2021 - $70M
- Ireland Health Service Executive – May 2021 - $20M
- Colonial Pipeline – May 2021 - $4.4M
- Brenntag – May 2021 – $7.5M
- Acer – May 2021- $50M
- JBS Foods – May 2021 - $11M
- Washington DC Police - May 2021 - $4M
- AXA – May 2021 – Unknown
- Ireland's Health Service Executive (HSE) – May 2021 - Unknown
- Quanta – Apr 2021 - $50M
- NBA – Apr 2021 – Unknown
- CNA – Mar 2021 – $40M
- Acer – Mar 2021 - $50M
- Buffalo Public Schools – Mar 2021 - Unknown
- CD Projekt – Feb 2021 -
- KIA Motors – Feb 2021 -

Source: https://cybersecurityventures.com/annual-cybercrime-report-2017/
https://securityandtechnology.org/wp-content/uploads/2021/06/IST-Ransomware-Task-Force-Report.pdf



RANSOMWARE GUIDE

SEPTEMBER 2020

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA

MS-ISAC®

Multi-State Information Sharing & Analysis Center®

Source: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Cybersecurity Ransomware Prevention

- Backups
- Create/Update Incident Response Plan
- Educate users to prevent falling victim to phishing
- Patch Operating Systems and Applications 💻
- Network Segmentation 💻

- Remove/Block unnecessary and outdated protocols/services (e.g., RDP, SMB) 💻
- Disable MS Office macros 💻
- Ensure antivirus and anti-malware software is operating and up to date 💻
- Use application “allowlisting” to authorize only legitimate software 💻

Source: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cybercriminals-actively-exploiting-rdp-to-target-remote-organizations/

Cybersecurity Ransomware Prevention

Third-Party Cybersecurity

- Infection vector may come from connected Third-Party Providers
- Know your Third-Party Providers
- Evaluate their cybersecurity
- Evaluate contract language; liability
- Managed Service Providers (MSPs)
  - Limit access to your systems to minimum necessary (least privilege)
  - Treat all Third-Party connections as untrusted

Source: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

What to do if you are a victim

If you or your company fall victim, it’s important to act quickly:

- Contact your Cybersecurity Insurance Carrier and engage forensic and remediation services
- Report the crime to your FBI Field Office
- File a complaint with the FBI’s Internet Crime Complaint Center.
- Contact your financial institution to request that they contact the ensure that ransom payment does not violate OFAC sanctions

Source: https://www.fbi.gov/contact-us/field-offices
https://www.ic3.gov/default.aspx

Cybersecurity Best Practices

Personal Cybersecurity Basics*

1. Raise awareness (Phishing, Social Engineering, …) – know the threats
2. Passwords – NO reuse; Complex; Passphrase; Use a Password Manager
3. Backup data
4. Updated/Current OS and Applications – allow auto-update
5. Antivirus, Firewall, Home network – change default passwords!
6. Terms of Service; Beware of free services – YOU'RE the product
7. Geolocation/Location based services
8. Reputable applications and what they have access to
9. Home IoT Devices – Change default passwords; Security
10. Wi-Fi Security
11. Credit Cards – Transaction Alerts (CNP); Use mobile app locking
12. Credit Reporting Bureaus - Freeze/Lock credit
13. Application Settings - Security & Privacy – periodically review/reset

BE BRILLANT AT THE BASICS

* Start with these, but don't stop there once you've mastered them

Q&A

Thank you.