Current Cybersecurity and Payment Threats: Best Practices & Insurance Strategies to Reduce Risk

October 2021

Don Boian,
Security Outreach Director

Ashley Bauer,
VP P&C Insurance Product Manager

Huntington
Welcome.

Agenda

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

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.

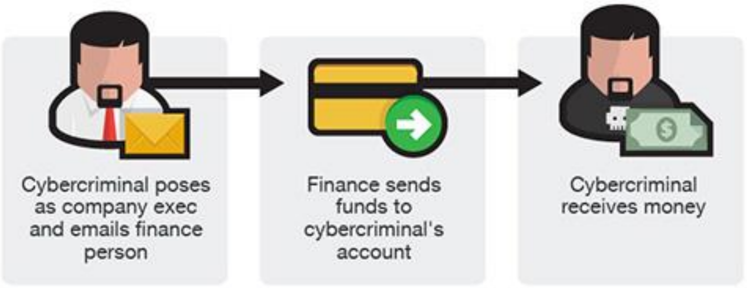
The Huntington National Bank is Member FDIC.

Welcome.

3

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 <u>compromise</u>?

4

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 users 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

5

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

6

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

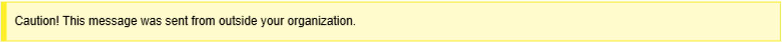
$1.75M LOST

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

| 11 | Huntington

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

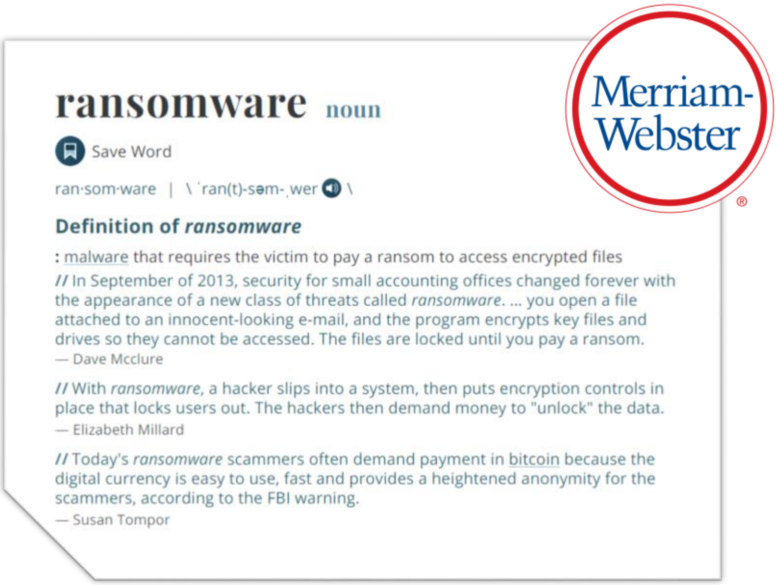
- Contact your financial institution immediately to request that they contact the financial institution where the transfer was sent.
- Report the crime to your FBI Field Office.
- File a complaint with the FBI’s Internet Crime Complaint Center.
- Contact your Cybersecurity Insurance Carrier and engage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

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

11

Ransomware - Definition

| 12 | Huntington



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

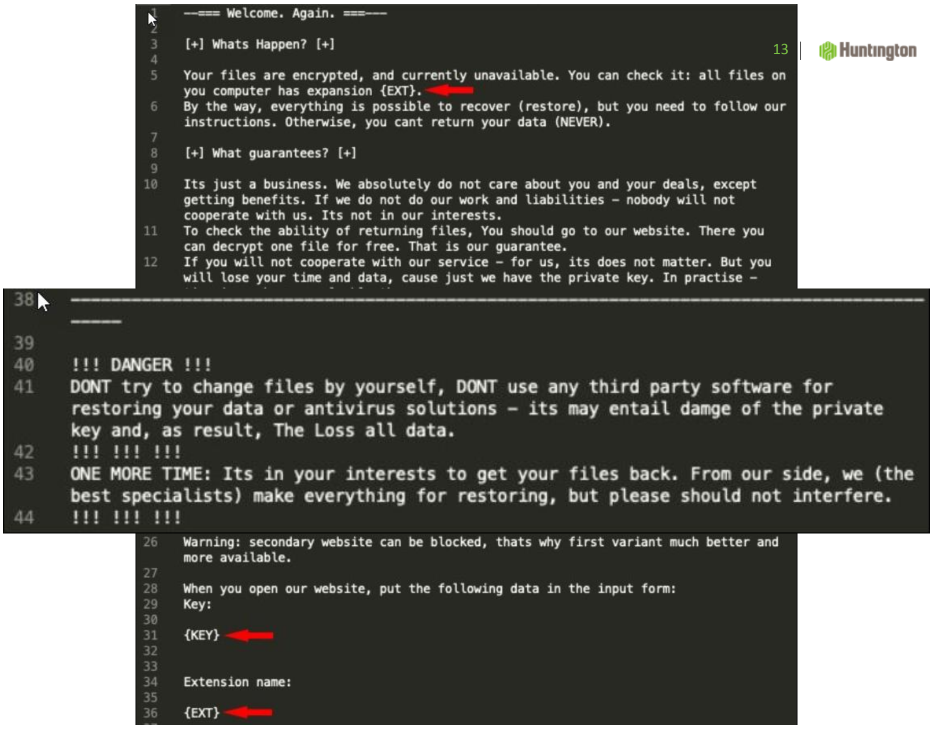
// In September of 2013, security for small accounting offices changed forever with the appearance of a new class of threats called *ransomware*. … you open a file attached to an innocent-looking e-mail, and the program encrypts key files and drives so they cannot be accessed. The files are locked until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

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

12

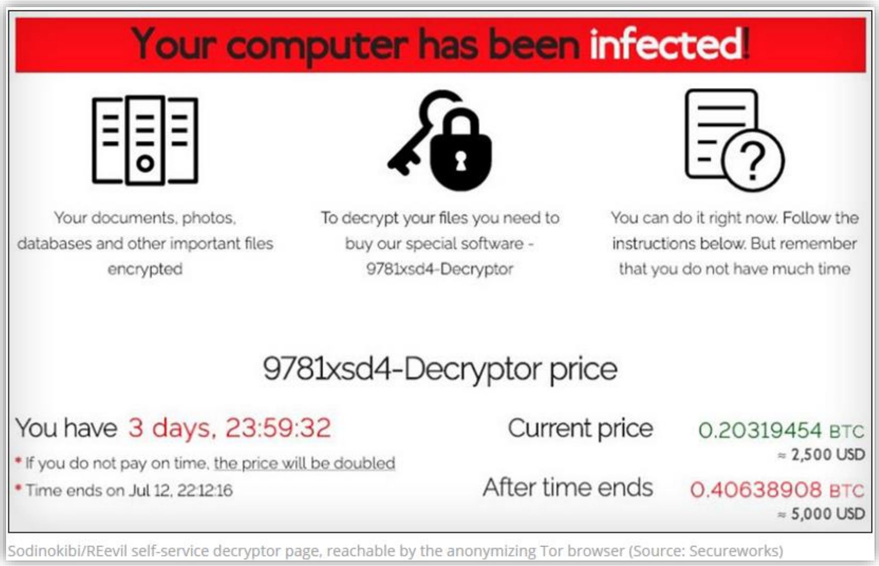


```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on
you computer has expansion {EXT}.
By the way, everything is possible to recover (restore), but you need to follow our
instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except
getting benefits. If we do not do our work and liabilities - nobody will not
cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you
can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you
will lose your time and data, cause just we have the private key. In practise -
```

```
-------------------------------------------------------------------------------
------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for
restoring your data or antivirus solutions - its may entail damge of the private
key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the
best specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!
```

```
Warning: secondary website can be blocked, thats why first variant much better and
more available.

When you open our website, put the following data in the input form:
Key:

{KEY}


Extension name:

{EXT}
```

13



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

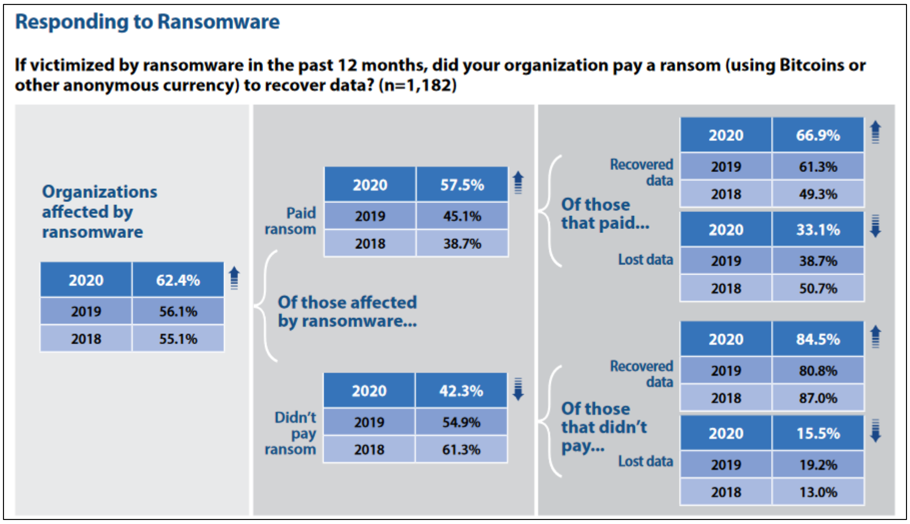
* Time ends on Jul 12, 22:12:16

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)

14



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%	

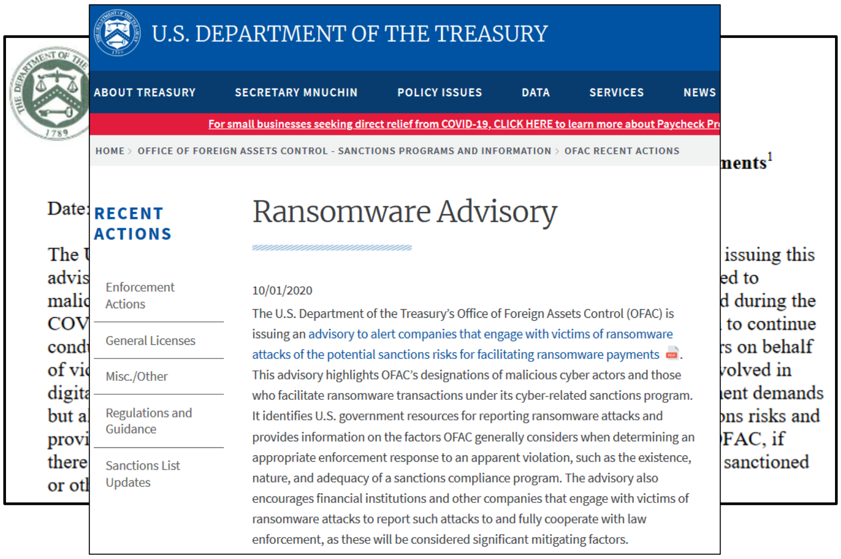
Lost data

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.

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

18

Ransomware – Increasing Threat

- 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

19

20

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

20

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/

21

Cybersecurity Ransomware Prevention

| 22 | Huntington

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

22

| 23 | Huntington

NO MORE RANSOM!
www.nomoreransom.org

23

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

Cyber Liability Insurance

Huntington
Welcome.

Traditional Fraud and Crime Insurance

- Employee Theft
  - Unlawful taking of money, securities, other property by **employees** either on their own or in collusion with others
- Forgery or Alteration
  - Losses customer experiences from forgery or alteration of **their checks**, drafts, promissory notes and similar
  - Includes signing of name of another person or organization with intent to deceive
    - Forged Name
    - Altered Account
- Money Orders, Counterfeit Money
  - Pays for losses insured **accepts** in good faith
    - Money orders issued not paid (altered)
    - Counterfeit money
- Computer and Funds Transfer Fraud
  - Loss from **fraudulent entry** of electronic data or computer program information
  - Change of insured information causing money, securities, property to be transferred or account to be debited or deleted
  - Loss from fraudulent instruction which directs a financial institution to debit insured's account and pay money, securities from account

Cyber Insurance
First Party (Client Expenses) Coverage

Insurance will cover costs the insured faces out of a cyber incident:

Breach Response/Crisis Management

Coverage responds to a network or privacy breach. Coverage includes: breach notification, public relations, forensic consultants, and credit monitoring costs

Cyber Extortion or Loss

Coverage responds to a threat by third party to commit a network security or privacy breach

Business Interruption Extra Expense Loss

Coverage responds to loss of income resulting from a network security breach or a network attack and extra expenses incurred to restore network to original condition

Data Restoration Coverage

Coverage responds to cost to restore data destroyed or altered as a result of a network security breach

Cyber Insurance
Third Party (Liability) Coverage

Insurance will cover claim expenses and damages the insured is legally obligated to pay to others as a result of the following:

Network Security Liability

Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Network Security Breach or Failure

Privacy Liability

Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Privacy Breach of PII, PHI or Corporate Confidential Information

Regulatory Coverage

Provides coverage for actions or proceedings and fines/penalties against the Insured by a regulatory agency resulting from a violation of a Privacy Law

Website Media / Multimedia

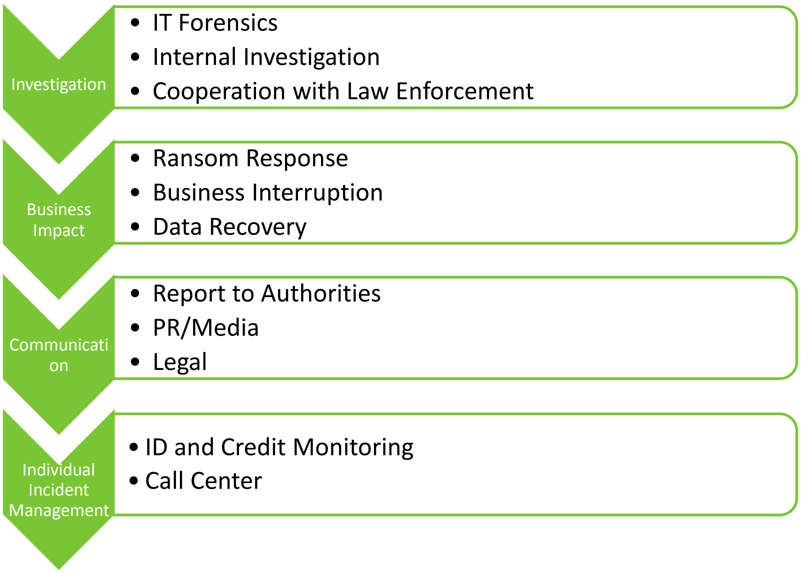
Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Media Peril of content on the Insured's Internet Site or may cover general Media Perils

Professional Liability

Provides coverage for acts, errors or omissions in the rendering or failure to render professional services to a client of the Insured

Incident Response

Insurance will cover costs the insured faces out of a cyber incident:

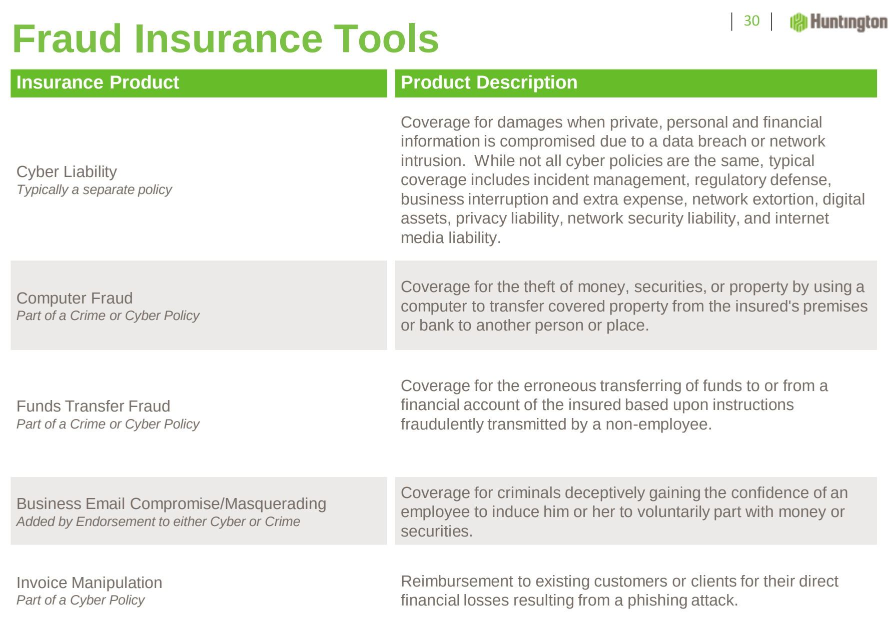


Investigation
- IT Forensics
- Internal Investigation
- Cooperation with Law Enforcement

Business Impact
- Ransom Response
- Business Interruption
- Data Recovery

Communication
- Report to Authorities
- PR/Media
- Legal

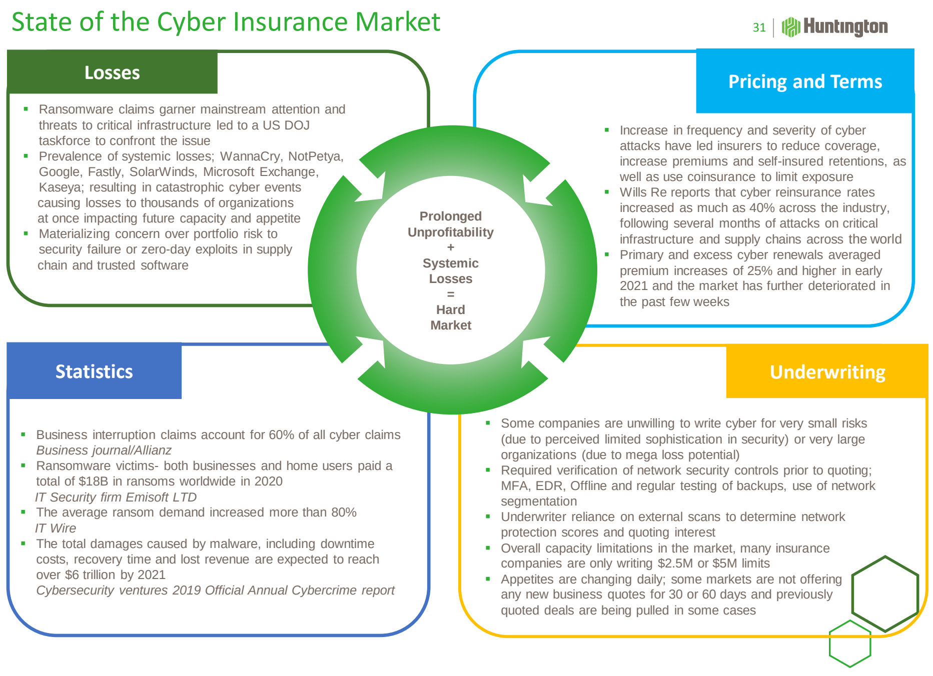
Individual Incident Management
- ID and Credit Monitoring
- Call Center



Fraud Insurance Tools

Insurance Product	Product Description
Cyber Liability *Typically a separate policy*	Coverage for damages when private, personal and financial information is compromised due to a data breach or network intrusion. While not all cyber policies are the same, typical coverage includes incident management, regulatory defense, business interruption and extra expense, network extortion, digital assets, privacy liability, network security liability, and internet media liability.
Computer Fraud *Part of a Crime or Cyber Policy*	Coverage for the theft of money, securities, or property by using a computer to transfer covered property from the insured's premises or bank to another person or place.
Funds Transfer Fraud *Part of a Crime or Cyber Policy*	Coverage for the erroneous transferring of funds to or from a financial account of the insured based upon instructions fraudulently transmitted by a non-employee.
Business Email Compromise/Masquerading *Added by Endorsement to either Cyber or Crime*	Coverage for criminals deceptively gaining the confidence of an employee to induce him or her to voluntarily part with money or securities.
Invoice Manipulation *Part of a Cyber Policy*	Reimbursement to existing customers or clients for their direct financial losses resulting from a phishing attack.

30



State of the Cyber Insurance Market

Losses

- Ransomware claims garner mainstream attention and threats to critical infrastructure led to a US DOJ taskforce to confront the issue
- Prevalence of systemic losses; WannaCry, NotPetya, Google, Fastly, SolarWinds, Microsoft Exchange, Kaseya; resulting in catastrophic cyber events causing losses to thousands of organizations at once impacting future capacity and appetite
- Materializing concern over portfolio risk to security failure or zero-day exploits in supply chain and trusted software

Pricing and Terms

- Increase in frequency and severity of cyber attacks have led insurers to reduce coverage, increase premiums and self-insured retentions, as well as use coinsurance to limit exposure
- Wills Re reports that cyber reinsurance rates increased as much as 40% across the industry, following several months of attacks on critical infrastructure and supply chains across the world
- Primary and excess cyber renewals averaged premium increases of 25% and higher in early 2021 and the market has further deteriorated in the past few weeks

Prolonged Unprofitability
+
Systemic Losses
=
Hard Market

Statistics

- Business interruption claims account for 60% of all cyber claims
  Business journal/Allianz
- Ransomware victims- both businesses and home users paid a total of $18B in ransoms worldwide in 2020
  IT Security firm Emisoft LTD
- The average ransom demand increased more than 80%
  IT Wire
- The total damages caused by malware, including downtime costs, recovery time and lost revenue are expected to reach over $6 trillion by 2021
  Cybersecurity ventures 2019 Official Annual Cybercrime report

Underwriting

- Some companies are unwilling to write cyber for very small risks (due to perceived limited sophistication in security) or very large organizations (due to mega loss potential)
- Required verification of network security controls prior to quoting; MFA, EDR, Offline and regular testing of backups, use of network segmentation
- Underwriter reliance on external scans to determine network protection scores and quoting interest
- Overall capacity limitations in the market, many insurance companies are only writing $2.5M or $5M limits
- Appetites are changing daily; some markets are not offering any new business quotes for 30 or 60 days and previously quoted deals are being pulled in some cases

31

Q&A

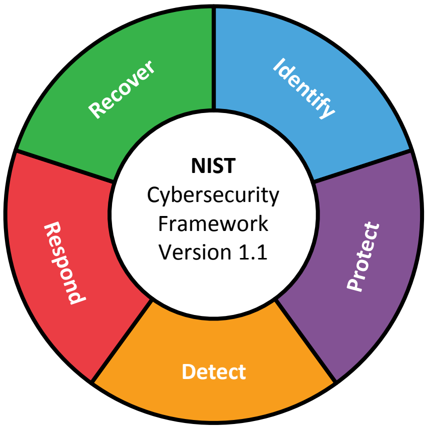
Thank you.

32

Cybersecurity Best Practices

33

The NIST Cybersecurity Framework



Source: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

34

Corporate Cybersecurity Basics*

Identify	• Inventory sensitive data (know where it is stored and processed, know what 3rd parties have your sensitive data) • Inventory systems and software (necessary for Vulnerability Mgt, etc) • Establish policies and procedures around Cybersecurity (WiFi, breach, etc) • Independently assess your security and that of your 3rd parties
Protect	• Employee training/awareness (Phishing, BEC, Social Engineering, Fraud, …) • Updated/Current OS and Applications (patch management) • Practice good password management; Use Multi-factor Authentication • Implement E-mail security (DMARC, SPF, DKIM), external banner, block spam/junk • Backup data (conduct, maintain and test)
Detect	• Monitor your logs for anomalies (or outsource it – MSSP) • Antivirus, Endpoint encryption, Data Loss Prevention - software up to date • Increase network defensive barriers (Firewalls, IDS, IPS, …) • Checks and Balances in ALL processes (Segregation of duties, least privilege, invoice/payment processing, …) • Plan (and exercise) for the worst (malware, outage, breach, …)
Respond	• Establish and practice crisis management policies and procedures
Recover	• Cybersecurity Insurance – Purchase and/or update policies & know your coverage

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

BE BRILLANT AT THE BASICS

35

36

Appendix

37

Personal Cybersecurity Basics*

| 38 | Huntington

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. WiFi 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

38

References

| 39 | Huntington

- **Huntington - Privacy & Security**
  - https://www.huntington.com/Privacy-Security
- **FBI**
  - Internet Crime Complaint Center (IC3)
    - https://www.ic3.gov/default.aspx
  - Public Service Announcements
    - https://www.ic3.gov/media/default.aspx
- **Federal Trade Commission**
  - Cybersecurity for Small Business
    - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
  - Identity Theft
    - http://www.identitytheft.gov/
- **NIST Cybersecurity Framework**
  - https://www.nist.gov/cyberframework/framework
- **Center for Internet Security**
  - https://www.cisecurity.org/
- **Cloud Security Alliance**
  - https://cloudsecurityalliance.org/

39

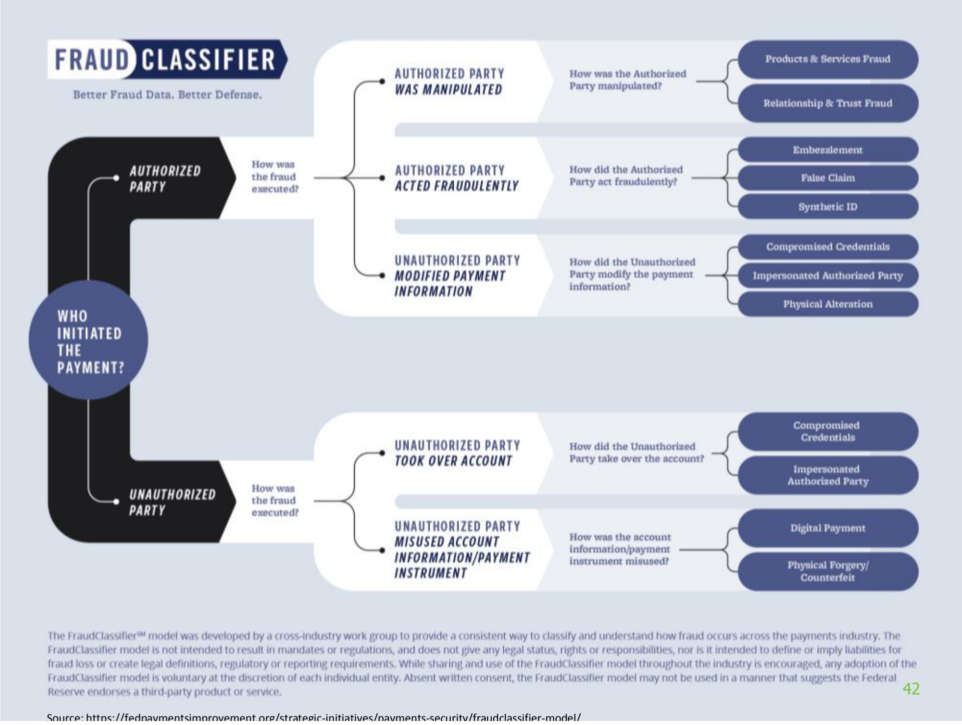
References

- **Credit Reporting Agencies**
  - Equifax (888)766-0008 http://www.equifax.com/CreditReportAssistance
  - Experian (888)397-3742
    - Fraud - https://www.experian.com/fraud
    - Freeze - https://www.experian.com/freeze/center.html
  - TransUnion (800)680-7289
    - Fraud – https://www.transunion.com/solution/fraud-detection
    - Freeze - https://www.transunion.com/blog/identity-protection/credit-freeze-vs-credit-lock
- **Federal Trade Commission – Complaint**
  - http://www.ftc.gov/complaint
- **National Automated Clearing House Association**
  - https://www.nacha.org/case-studies/business-email-compromise-and-vendor-impersonation-fraud-what-you-need-know

References – Cybersecurity Careers & Education

- **Careers in Cybersecurity – CyberSeek**
  - https://www.cyberseek.org/heatmap.html
  - https://www.cyberseek.org/pathway.html
- **National Institute of Standards and Technology (NIST)**

  National Initiative for Cybersecurity Education (NICE) Framework
  - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
- National Initiative for Cybersecurity Careers and Studies (NICCS)
  - https://niccs.us-cert.gov/
- STOP. THINK. CONNECT.
  - https://www.stopthinkconnect.org/
- FBI – Safe Online Surfing
  - https://sos.fbi.gov/en/



FRAUD CLASSIFIER

Better Fraud Data. Better Defense.

WHO INITIATED THE PAYMENT?

AUTHORIZED PARTY

How was the fraud executed?

AUTHORIZED PARTY *WAS MANIPULATED*

How was the Authorized Party manipulated?

- Products & Services Fraud
- Relationship & Trust Fraud

AUTHORIZED PARTY *ACTED FRAUDULENTLY*

How did the Authorized Party act fraudulently?

- Embezzlement
- False Claim
- Synthetic ID

UNAUTHORIZED PARTY *MODIFIED PAYMENT INFORMATION*

How did the Unauthorized Party modify the payment information?

- Compromised Credentials
- Impersonated Authorized Party
- Physical Alteration

UNAUTHORIZED PARTY

How was the fraud executed?

UNAUTHORIZED PARTY *TOOK OVER ACCOUNT*

How did the Unauthorized Party take over the account?

- Compromised Credentials
- Impersonated Authorized Party

UNAUTHORIZED PARTY *MISUSED ACCOUNT INFORMATION/PAYMENT INSTRUMENT*

How was the account information/payment instrument misused?

- Digital Payment
- Physical Forgery/ Counterfeit

The FraudClassifier℠ model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for fraud loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the FraudClassifier model throughout the industry is encouraged, any adoption of the FraudClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the FraudClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

42

Source: https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

42