PROGRAM MATERIALS
Program #31104
June 9, 2021

Cyber Risks Are Evolving—And Impacting Your Cyber Insurance

- Paul Moura, Esq. – Cooley LLP
- David Navetta – Cooley LLP

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919

Cooley

Cyber Risks Are Evolving—

And Impacting Your Cyber Insurance

June 2021

Introductions

David Navetta
Partner
Cyber / Data / Privacy
+1 720 566 4153
dnavetta@cooley.com

Paul Moura
Associate
Insurance
+1 212 479 6503
pmoura@cooley.com

Agenda

- Recent trends in cyber attacks
- Business impact
- Insurance for cyber exposures
- Impact on cyber insurance market
- Judicial interpretations of cyber insurance coverages
- Strategies for addressing the cyber market contraction

Trends in cyber attacks

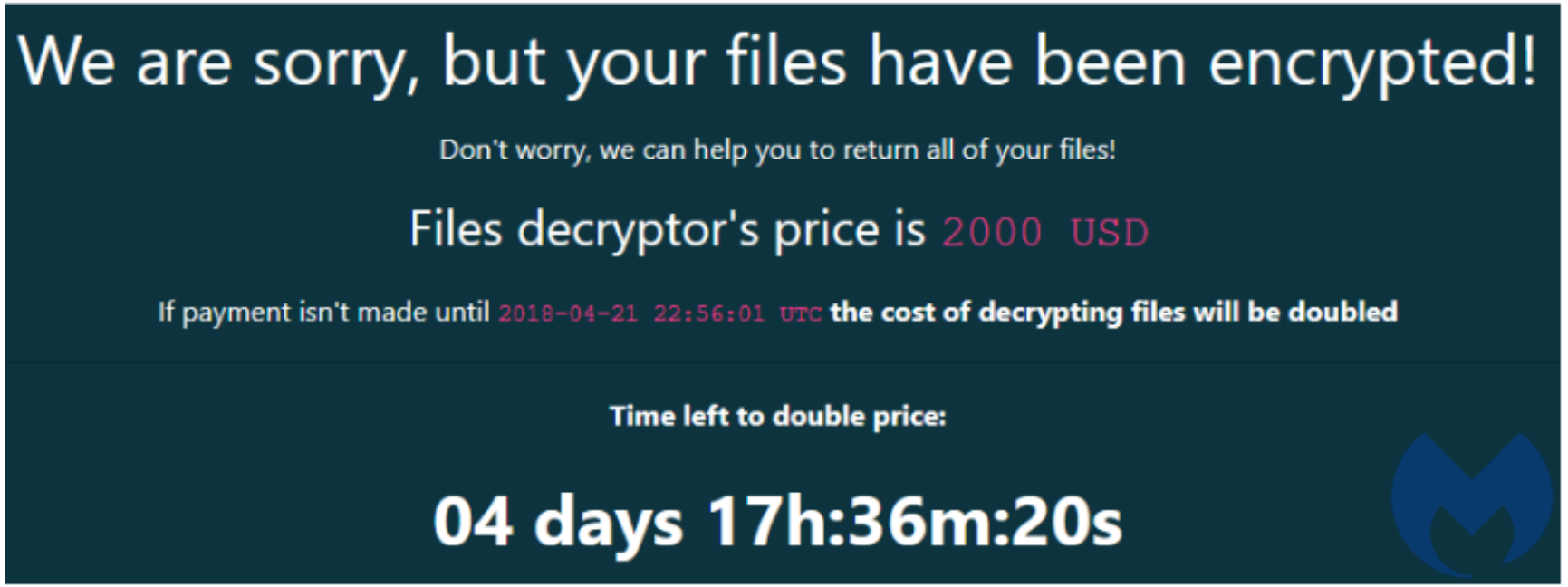
- **Systemic Cyber Risk**
  - 2016: “Bangladesh Bank Robbery”
  - 2017: “WannaCry” ransomware attack
  - 2017: “NotPetya” malware attacks
  - 2018: Amazon Web Services Cloud Disruption Event
  - 2018: Microsoft Office 365 Outage
  - 2020: SolarWinds attack
  - 2021: Microsoft Exchange Server data breach
- **Recent losses**:
  - Maersk ($300M)
  - Norsk Hydro ($40M)
  - City of Baltimore ($18M)

Trends in cyber attacks

- **Characteristics**
  a. **Not drive-by attacks** – intelligence gathering, planning, use of multiple tools and lateral movement (often through admin access)
  b. **Bad timing** – attackers maximize pressure by timing attacks at bad times
  c. **Encryption of backups**
  d. **Entire system disabled** (email, manufacturing, fulfillment, invoicing, delivery)
  e. **Need to wipe and rebuild in real-time** – cannot simply restore or decrypt because of high risk of secondary attack
  f. **Data exfiltration investigation is necessary after initial triage**
  g. **Phishing is often root or contributing cause**

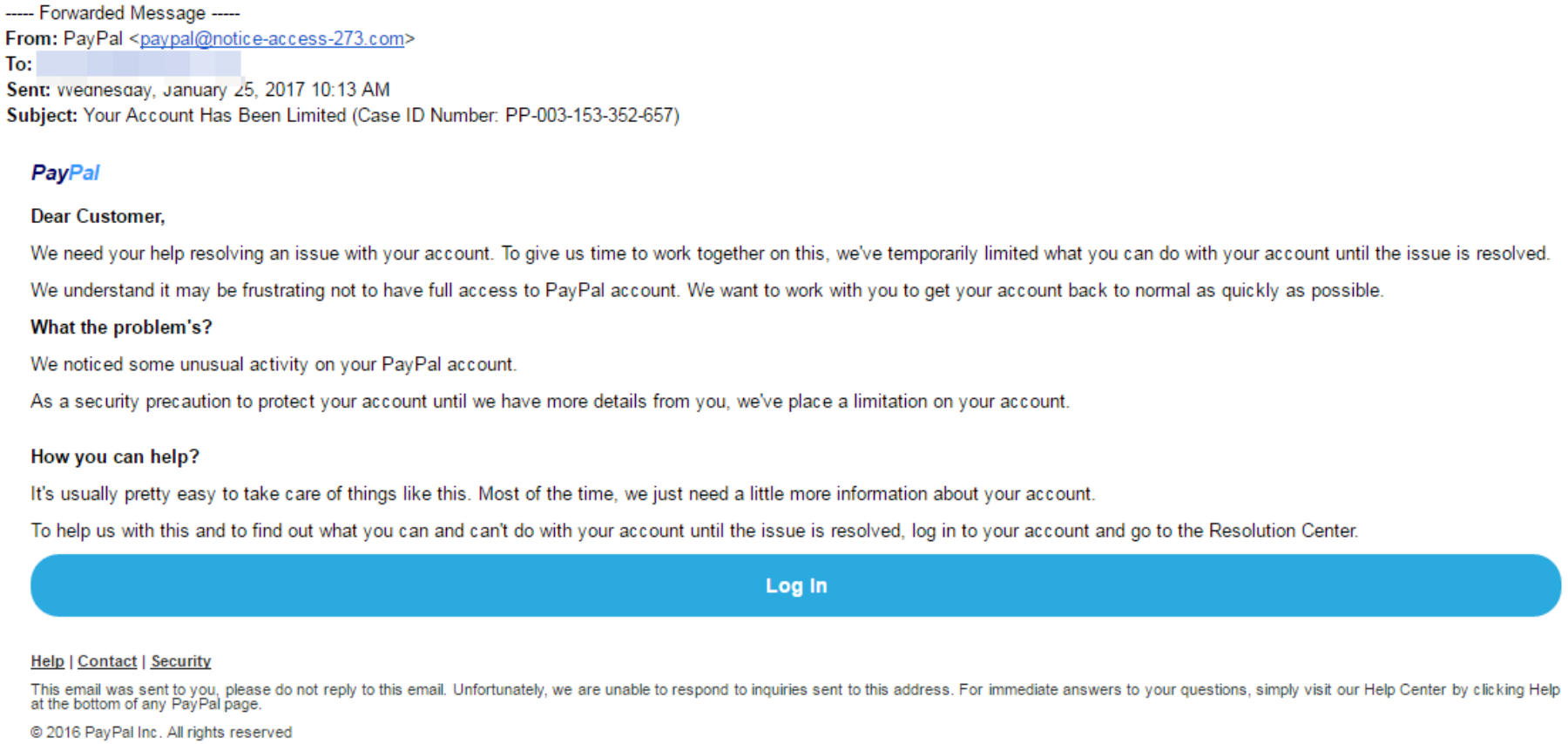
Trends in cyber attacks

- **Ransomware / Encryption / Entire System Disabled**



Trends in cyber attacks

- **Phishing and Social Engineering**



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

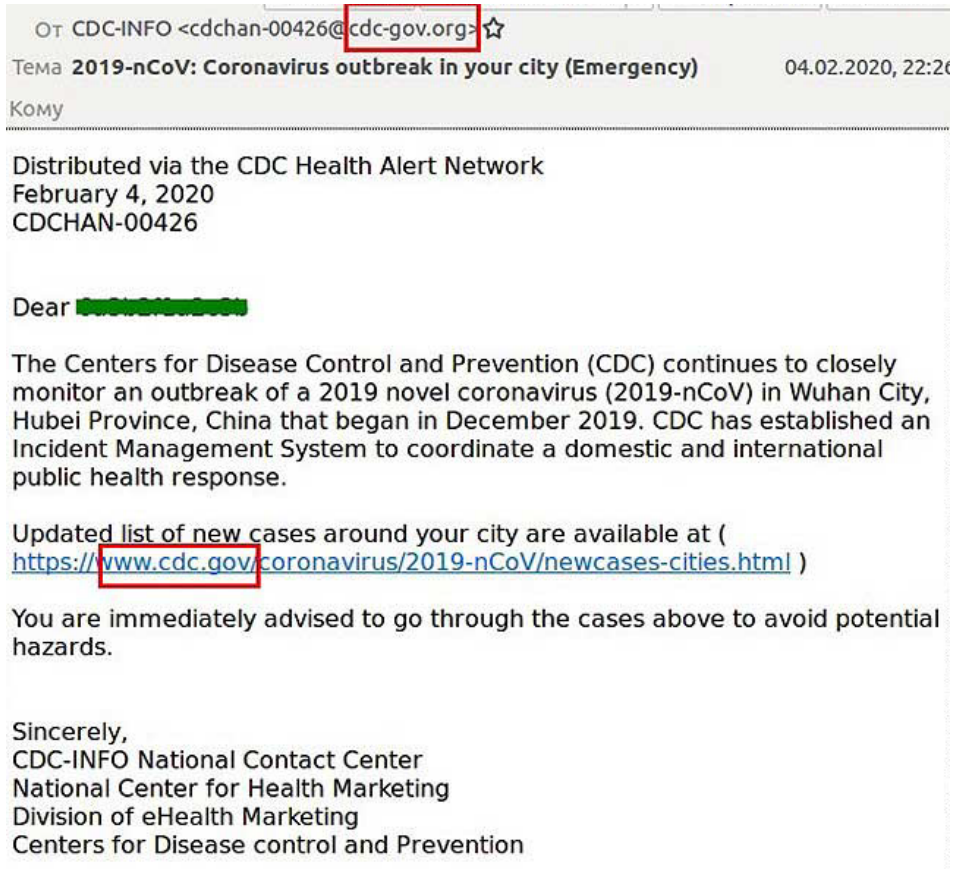
Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

Trends in cyber attacks

- **Phishing and Social Engineering**



От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:2

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

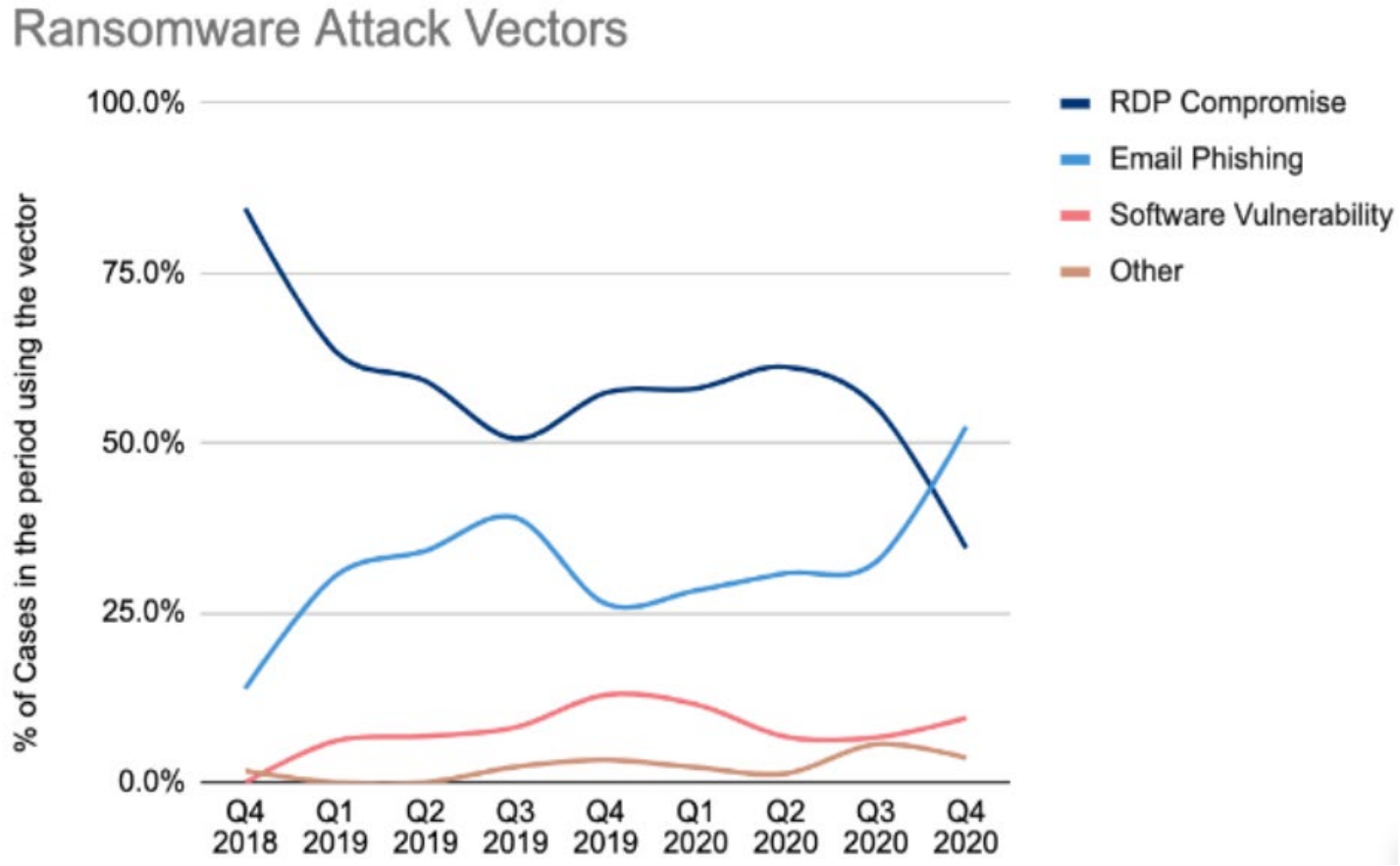
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Trends in cyber attacks



https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

Business impact

- First-party Expenses
  - Forensic investigation
  - Crisis response
  - Public relations
  - Legal expenses
  - Repairs and remediation
  - Lost Business Income
  - Fraud payments
  - Ransom Payments
- Third-party Expenses
  - Lawsuits and consumer claims
  - Government inquiries and investigations
  - Contractual liabilities (including PCI DSS fines)

Business impact

Business Interruption Costs Are the Largest Source of Losses

Average Days of Downtime

21

+11% from Q3 2020

Downtime is still the most costly aspect of a ransomware attack. In Q4 of 2020, the average firm experienced roughly 21 days of downtime, 2 more days than in Q3. Downtime can range on a spectrum from having a business be at a total standstill, to being just mildly affected by non-available machines.

https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

Business impact

Average Ransom Payment

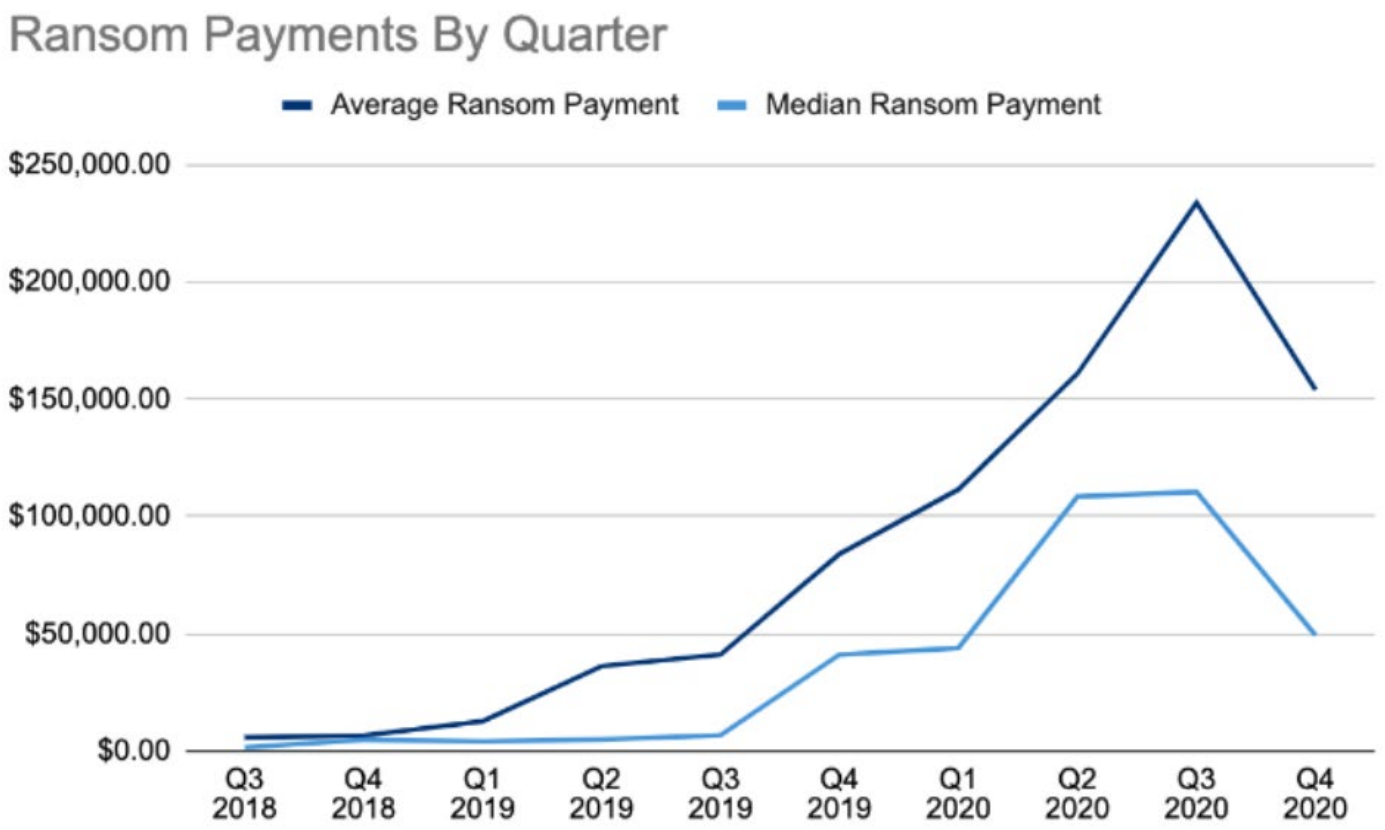
$154,108

-34% from Q3 2020

Median Ransom Payment

$49,450

-55% from Q3 2020



https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

Insurance for cyber exposures

- September 2015: 40% of Fortune 500 companies had cyber insurance
- October 2016: 29% of all US businesses had cyber insurance
- Traditional policies *may* cover cyber-related exposures
  - General Liability
  - Property Policies
  - Crime / Fidelity Policies
    - Financial theft
    - Kidnap, ransom, extortion
- However, most traditional policies are not tailored toward cyber incidents (e.g., “direct loss” requirements)—and more recently, attempt to expressly exclude coverage for cyber-related exposures (i.e., “silent cyber”).

Insurance for cyber exposures

- What does Cyber Insurance Cover?
  - Covered Expenses
    - Forensic investigation and data restoration
    - Legal expenses, PR costs
    - Notification costs, Call centers, Credit monitoring
    - Contractual and Third-party liabilities, PCI DSS fines
  - Covered Claims
    - Security Event (breach event)
    - Privacy Event (disclosure of PII)
    - Wrongful Acts

Insurance for cyber exposures

- Anatomy of a Cyber Policy – No Two Cyber Policies Are Alike

First Party

- Cyber event management (notification/remediation)
- Business interruption
- Data recovery
- Cyber extortion
- Cyber crime

Third-Party

- Network security liability
- Privacy liability
- Media liability
- Technology E&O liability
- IP liability

Impact on cyber insurance market

- Market uncertainties
  - Concerns over systemic and catastrophic cyber risk (*e.g.*, NYDFS guidance)
  - Increases is ransom demands
    - Average of $115,123 in 2019; $312,493 in 2020; 171% year-on-year increase
    - 2020 saw ransom demands up to $30M
  - Increase in system downtimes (21 days in 2020 Q4, up 2 days from Q3)
  - Limits on historical and current data for underwriting cyber risk

Impact on cyber insurance market

- Underwriting trends
  - Demand for cyber insurance is up
  - Premium increases averaging 25%-40%
  - New entrants into cyber insurance market continuing
  - Insurtechs and “Smart” underwriting
- Capacity trends
  - $5 million increasingly common maximum limit (though excess is available)
  - Self-insured retentions increased (large insureds see $1M SIRs)
  - Business interruption waiting periods increased (e.g., up to 18 hours)
  - Time limits on event management expenses (e.g., up to 1 year)
  - Ransomware sub-limits (e.g., 50% sub-limit; co-insurance)

Impact on cyber insurance market

- Scope of coverage – Less flexibility by cyber insurers
  - Enforcing terms stringently
    - “Legally obligated to pay”
    - “Actual” versus “suspected” intrusion
    - Prior knowledge, timely notice, and retroactive dates
    - Application representations
    - Consent requirements, cooperation, and information exchange
    - Subrogation
  - Exclusions
    - Intentional acts
    - Antitrust/deceptive trade practices
    - Warlike activity
    - “Silent Cyber” exclusions in traditional policies

Judicial interpretations of cyber insurance coverages

- Denials by cyber insurers:
  - *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.*, 103 F. Supp. 3d 1297, 1302 (D. Utah 2015) (in evaluating coverage for claims in underlying lawsuit arising from insured's alleged refusal to return electronic data to its customer until customer paid money insured demanded, court ruled no duty to defend due to allegations that insured acted with knowledge, willfulness and malice by refusing to release customer's data, whereas the policy covered errors, omissions, and negligent acts).
  - *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 WL 3055111, at *8 (D. Ariz. May 31, 2016) (Court analyzed a cyber-insurance policy that provided coverage for "direct loss, legal liability, and consequential loss resulting from cyber security breaches," and found that insurer properly disclaimed coverage for fees and assessments that the insured agreed to reimburse its credit/debit card processor as a result of a breach, as this constituted liability assumed by the insured).
  - *National Ink and Stitch, LLC v. State Auto Property & Cas. Ins. Co.*, Case No. SAG-18-2138, 2020 WL 374460, *2-5 (D. Md. Jan. 23, 2020) (ransomware attack prevented access to the insured's data, software, and stored files; Court held there was coverage for the costs of replacing the entire computer system and rejected the insurer's contention that the computer system itself was not covered short of a total inability to function).

Judicial interpretations of cyber insurance coverages

- Cybercrime/Crime Insurance
  - **Computer fraud coverage**:
    - Typically insures against the “direct loss of…money, securities or other property resulting directly from the use of any computer to fraudulently cause a transfer of that property.
  - **Funds transfer fraud:**
    - Protects against loss caused by “an electronic, telegraphic, cable, teletype or telephone instruction” that fraudulently directs a debit or transfer from the insured’s account.

Judicial interpretations of cyber insurance coverages

- Cybercrime/Crime Insurance
  - **"Direct" loss**:
    - *Medidata Sols. Inc. v. Fed. Ins. Co.*, 729 F. App'x 117, 118-19 (2d Cir. 2018) (New York law) (unpublished) (losses that resulted from email spoofing attack were covered by the terms of the policy's computer fraud provision, which covered losses stemming from any "entry of Data into" or "change to Data elements of program logic of" a computer system; coverage afforded because the fraudster entered the insured's email system via spoofed emails which contained a computer code that concealed the fraudster's true identity and simulate the insured's president's address).
    - *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 465, 474-80 (6th Cir. 2018) (Michigan law) (impersonator's spoofing email constituted triggered coverage for computer fraud coverage as the insured suffered a "direct" loss when it mistakenly wired funds to the impersonator).*
    - *Cincinnati Ins. Co. v. Norfolk Truck Center, Inc., 430 F. Supp. 3d 116 (E.D. Va. 2019) (finding coverage under computer fraud Insuring Agreement, where fraudster sent email that led insured to pay legitimate invoice to the wrong payee).*

Judicial interpretations of cyber insurance coverages

- Cybercrime/Crime Insurance
  - **No "direct" loss**:
    - *Apache Corp. v. Great Am. Ins. Co.*, No. 15-20499, 662 F. App'x 252, 258 (5th Cir. 2016) (Texas law) (unpublished) (loss resulting from phishing email that directed insured's payment for invoices to a fraudulent bank account was not covered by the "computer fraud" provision in crime protection insurance policy, because the transfer of funds was caused by other acts, including a telephone call from the fraudster).
    - *Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc.*, No. CV2004062ABPVCX, 2020 WL 6789095, at *6 (C.D. Cal. Nov. 5, 2020) (imposter's conduct does not constitute computer fraud as defined by the policy because the relevant wire transfers were made by an authorized user, not the hacker, and the imposter's fraudulent emails did not directly cause the transfer of any funds).
    - *Mississippi Silicon Holdings, LLC v. AXIS Ins. Co.*, 440 F. Supp. 3d 575, 587 (N.D. Miss. 2020) (no coverage because the subject transfers had actually been authorized; albeit following fraudulent email instructions, and ruling that the policy does not cover authorized or valid electronic transactions).

Strategies for addressing the cyber market contraction

- Carefully review and address coverage sticking points at renewal
  - Limits / Sub-limits / Waiting Periods / Time limits
  - Prior knowledge / Retroactive dates / Applications
  - Over-restrictive language (“legally obligated to pay”, “actual/suspected intrusion”, “direct loss”)
  - Overbroad exclusions (deceptive trade practices, war)
  - Consent requirements and pre-approvals of vendors/counsel
  - Carefully review “silent cyber” exclusions
  - Consider excess cyber coverages

Strategies for addressing the cyber market contraction

- Review indemnity provisions in agreements with business partners and vendors

During the Term and at its own expense, Contractor will maintain the following insurance coverage with insurance carriers rated A- or better by A.M. Best Company:

Cybersecurity and Privacy Insurance. If Contractor will collect, store, process or otherwise access any data related to its customers, then Contractor will maintain network security and privacy liability insurance with coverage limits of not less than US$1,000,000 per claim, that includes coverage for: (A) Contractor's unauthorized disclosure of, or failure to properly handle, personal or other confidential data; and (B) financial loss, including any related defense expense, resulting from Contractor's wrongful acts.

Strategies for addressing the cyber market contraction

- Review indemnity provisions in agreements with business partners and vendors
  - Problems with a bare “cyber insurance” insurance requirement
  - More than just “limits”—consider retentions, sub-limits, refreshing limits, waiting periods
  - Consider enumerating cyber coverage parts
  - Consider utilizing master insurance schedules reflecting minimum insurance requirements (incl. re: coverage grants and exclusions)
  - Leverage your insurance brokers

Questions?

Cooley