PRESENTED BY:

GODFREY & KAHN S.C.

WIPFLI

Gallagher

Insurance | Risk Management | Consulting

FEI Northeastern Wisconsin

STATE OF THE CYBER MARKET

October 1st, 2021

Gallagher

Insurance | Risk Management | Consulting

Cyber & Technology Practice

Gallagher | CYBERRISK

State of the Market

Today's Evolving Landscape

Gallagher

Insurance | Risk Management | Consulting

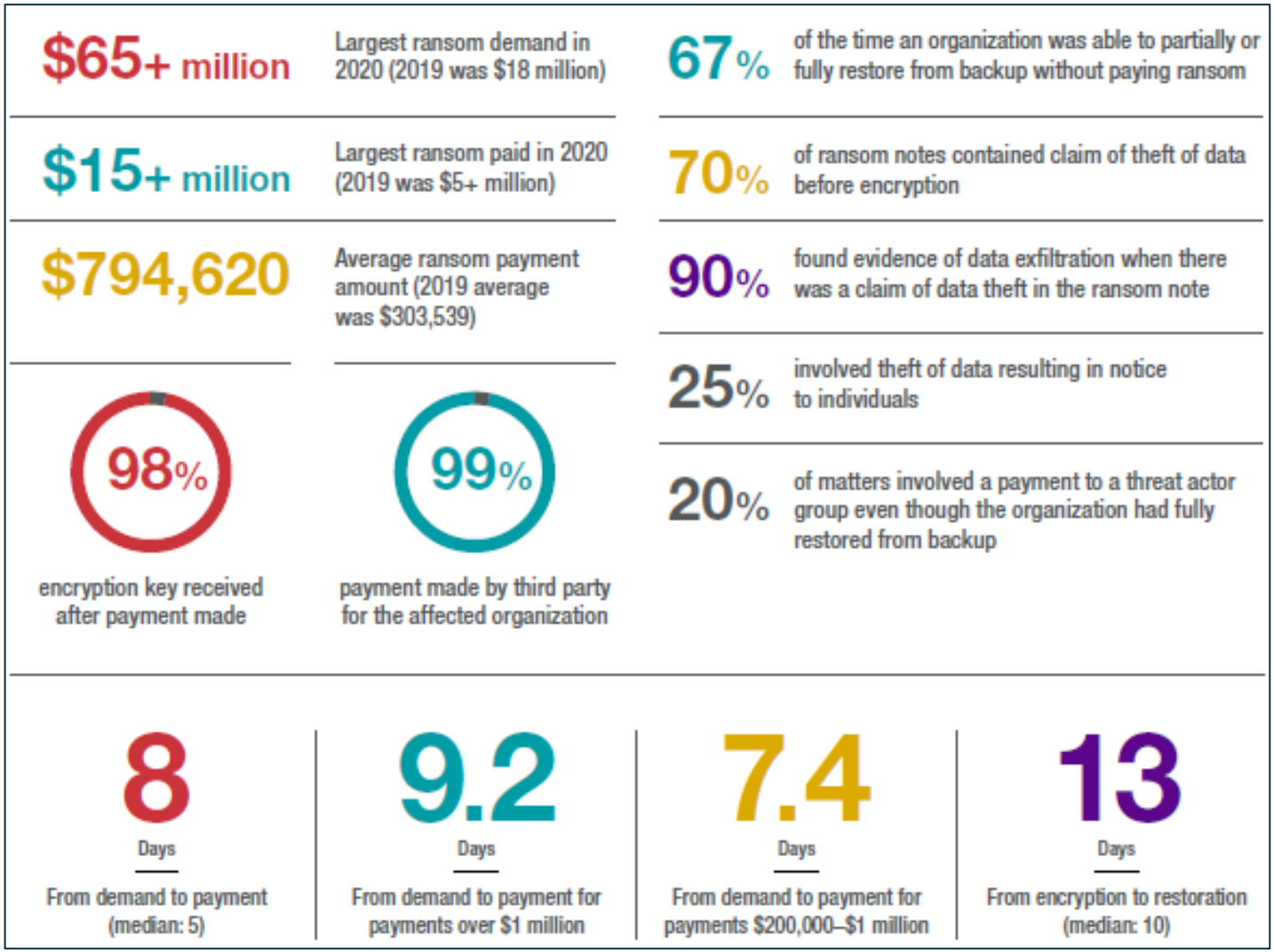
Current Threats & Trends

Cyber Insurance Market Disruption

- **Accellion FireWall Vulnerability**
  - Vulnerability related to File Transfer Appliance (FTA) used to transfer large, sensitive files; hackers using vulnerability to extort organizations
- **Microsoft Exchange Server Zero Day Vulnerability**
  - Too early to determine full impact; estimated 30,000 affected businesses in United States; email logs and credentials targeted
- **Solar Winds (Orion) Supply Chain Attack**
  - Cyber criminals implemented code that created backdoor into Solar Winds clients' network (Estimated 18,000 affected businesses; 400 *Fortune 500* organizations)
- **Blackbaud Ransomware**
  - Cloud based fundraising software; cyber criminals were able to gain access to Blackbaud customers' networks
- **Kaseya Ransomware**
  - Estimated 500 - 1800 companies exposed to a supply chain ransomware attack leveraging a vulnerability in the Kaseya VSA software against multiple MSPs and their customers.
- **Ransomware Trends**
  - 2020 was the worst year on record for ransomware/cyber extortion payments
  - AIG, Chubb, XL among top carriers restricting coverage and shifting risk appetite
  - Colonial Pipeline and JBS among recent critical infrastructure ransomware attacks. CNA $40M extortion payment and Molson Coors hack estimated to cost the company ~$140M. All in first half of 2021.

FEI Northeastern Wisconsin

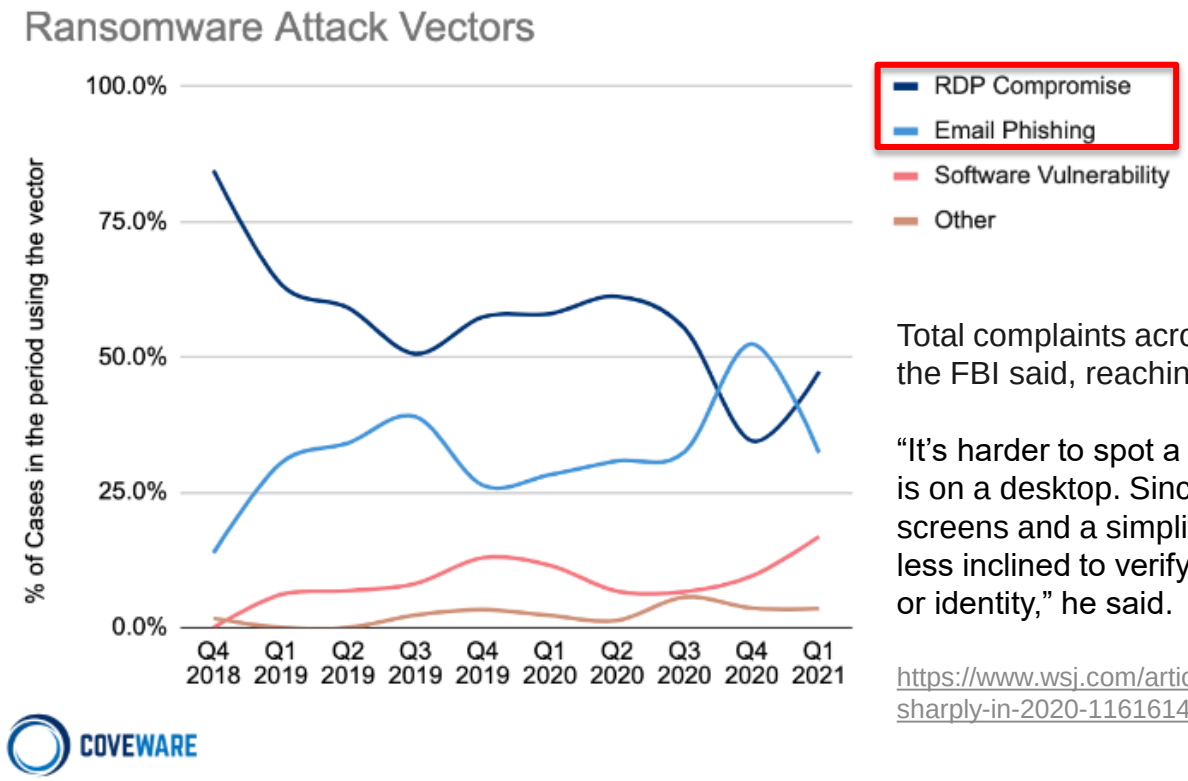
2020 Ransomware Statistics



[4] Baker Hostetler 2020 Data Security Incident Response Report

FEI Northeastern Wisconsin

Ransomware – Attack Vectors



Total complaints across all categories rose by 69%, the FBI said, reaching a record 791,790.

"It's harder to spot a phishing attack on mobile than it is on a desktop. Since mobile devices have smaller screens and a simplified user experience, people are less inclined to verify the sender's real email address or identity," he said.

https://www.wsj.com/articles/fbi-says-phishing-scams-rose-sharply-in-2020-11616146202?mod=djemCIO

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

Loss Prevention & Claims

Claims Trends: Cyber Regulatory Landscape

State Privacy Law

- All 50 States have a Data Breach Notification Law, now several states are expanding into regulating how data is used and collected
- Existing state privacy laws have been broadened to expand the scope of protected information, tighten notification timelines, and impose data-security requirements, including but not limited:
  - California: Passed the unprecedented California Consumer Privacy Act of 2018 which will go into effect in July. The law as currently written provides GDPR-like protects for Californians, including: strict disclosure requirements, ability to opt out of information being shared with third parties, data access, knowledge and portability rights and a right to be forgotten.
  - Washington: Amended its breach notification statute in March 2020 by greatly expanding their def. of personal (includes just the last four digit of SSN), shortening the notice period to 30 days and requiring regulator notice even for small breaches.
  - Nevada: Provides residents the ability to opt out of data sales. Organizations that violate any of the privacy and security requirements may be subject to a penalty up to $5,000 per violation.
  - Arizona: Protected information now includes private electronic keys (ex. username + password) and refined notice within 45 days of discovery
  - Colorado: Now requires notice to affected individuals within 30 days of discovery
  - Louisiana: Companies now must implement & maintain "reasonable security procedures" and refined notice within 60 days of discovery
  - 10+ States: currently contemplating the implementation of privacy / security law changes similar to onerous requirements of CCPA and GDPR.

Biometric Information

- Regulation of **Biometric Information**
  - Illinois, Texas, Washington and now Vermont are jurisdictions that regulate the collection and use of biometric information
- Illinois' Biometric Information Privacy Act (BIPA) allows for a private right of action.

International

- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
  - First nation-wide mandatory breach notification requirement with penalties per offense for non-compliance.
- EU's General Data Protection Regulation (GDPR)
  - Applies to any organization that collects, processes or stores the information of EU residents
    - Broad Definition of Protected Information ; Simply having an EU-facing website that installs tracking cookies can put an organization in the scope of GDPR
    - Includes strict data management and breach prevention requirements such as right to erasure and data portability
    - Allows for penalties to be assessed against non-compliant organizations up to 4% of global annual "turnover" (re: gross income)
    - Extensive business practice requirements and action can be brought for failure to comply, regardless of if data has been affected

Other Items of Note

- **Multiple laws can apply at the same time** and the organization is expected to comply with each applicable regulation. The application of laws is usually dependent upon **the residency of the affected individual**
- Many laws establish that transfer of information to a 3rd party **does not constitute the transfer of liability**
  - The "originating" organization is considered the "Data Owner" and therefore responsible for notification if compromised while in the care of a 3rd party. There are **numerous inconsistencies** among Privacy Laws
  - Differences in **defining** "protected information"
    - **Typically** includes a Name + social security number, state ID or Driver's License number, and financial account number with access code
    - Some states **are broader** than others and include biometric information, health insurance and medical information, and e-mail addresses/usernames with passwords – CCPA expands this definition
  - Reporting requirements **vary.** Example: Some states require the Attorney General be notified, others don't have these stipulations

Gallagher

Insurance | Risk Management | Consulting

2021 Cyber Insurance Marketplace

Work From Home / Remote Workforce

IT Supply Chain Attacks

- Solarwinds
- Acellion
- Microsoft Exchange
- Blackbaud

Ransomware

- Average Ransom Payment
- Exfiltration
- Phishing increases

Privacy Regulations

- GDPR
- CCPA / CPRA
- BIPA
- VDCPA
- Others in the works

Rate Increases

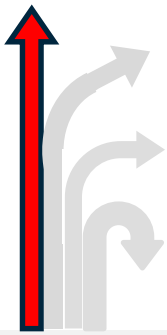
50 - 100% + for above avg controls
100 - 300% for below avg controls

Coverage Restrictions

Ransomware + Dependent Business Interruption
Increased retentions
Reduction of capacity

Overall Market Conditions: Cyber Liability

Gallagher
Insurance | Risk Management | Consulting



Rate Expectations

- **Hard (60% - 100% for above avg risks; 100% - 300% for below avg risks)** – The cyber/tech market is **in a hard market** due to increased claims frequency, severity and acute concerns of systemic cyber events.
- **Ransomware** losses continue to exceed projections and the **SolarWinds** supply chain event shocked the market.
- Positive results may be achieved through **broad marketing effort** with the communication of **robust cybersecurity controls.**

Technical Underwriting

- **"Live" underwriting becoming more common.**
- **Ransomware Supplemental Applications required – specific controls related to ransomware prevention and mitigation.**
- **Carriers require specific controls before releasing terms or binding coverage. Carriers vary on those specific mandatory controls but there are commonalities.**
- **Showcase improvements and investment in NETSEC and INFOSEC initiatives.**

Critical Cybersecurity Controls

- **MFA for remote access and privileged access and stringent privileged account management (PAM)**
- **Segmented and frequent backups (< 31 days), with a demonstrated ability to quickly restore within DRP/IRP.**
- **Prompt implementation of security patches/updates to operational technology and stringent change management.**
- **Endpoint Detection and Response tools (EDR).**

Coverage Restrictions Trends

- Ransomware sub-limits
- Ransomware coinsurance percentages (50%)
- Dependent Business Interruption coinsurance percentages (50%)
- Broad SolarWinds Exclusions
- Aggregate capacity restrictions
- Market segment and revenue class restrictions

Doesn't apply to all carriers or all market segments. It's difficult to predict if these coverage positions will hold through 2021-2022

"High Hazard" Industries

- **Public Entities and Municipalities**
- Education
- **Law Firms & Other Professional Firms**
- Healthcare

Plan, Invest, and Communicate

FEI Northeastern Wisconsin

Critical Cybersecurity Controls

- Multifactor Authentication (MFA) for remote access, privileged access and email access
- Endpoint Detection and Response tool (EDR) and/or Next Generation Anti-Virus (NGAV) with the ability to isolate and contain host machines
- Disaster Recovery/Incident response plan in place in the event of a cyber-incident that is tested and updated <yearly with key stakeholders
- Prudent backup, patching and encryption policies for sensitive data and critical applications (Less than 7 days for critical, less than 30 for all other at a minimum)
- Offsite, air gapped and encrypted backups necessary for many carriers to offer cover
- Demonstrated capacity to apply critical security patches immediately, particularly in response to high profile zero day exploits (Microsoft Exchange, Kaseya, Accellion, etc.)

https://www.ajg.com/us/news-and-insights/2021/apr/cyber-insurance-fight-against-ransomware/

FEI Northeastern Wisconsin

Critical Cybersecurity Controls (Cont'd)

- Domain/service account restrictions across the environment and separate from day to day accounts
- Articulate privileged access account security measures and/or integrated PAM tool
- Password management (preferably through a vault or randomizer with limited access and check in/out)
- Provide detailed asset footprint of particular service accounts with domain credentials, the services they provide and how they are monitored throughout and between trees/forests
- EOL (End of Life/unsupported) software segregated from the network and plans to decommission timely
- Remote access via VPN with MFA implemented especially through RDP with network level authentication and honeypots.

https://www.ajg.com/us/news-and-insights/2021/apr/cyber-insurance-fight-against-ransomware/

Thank You