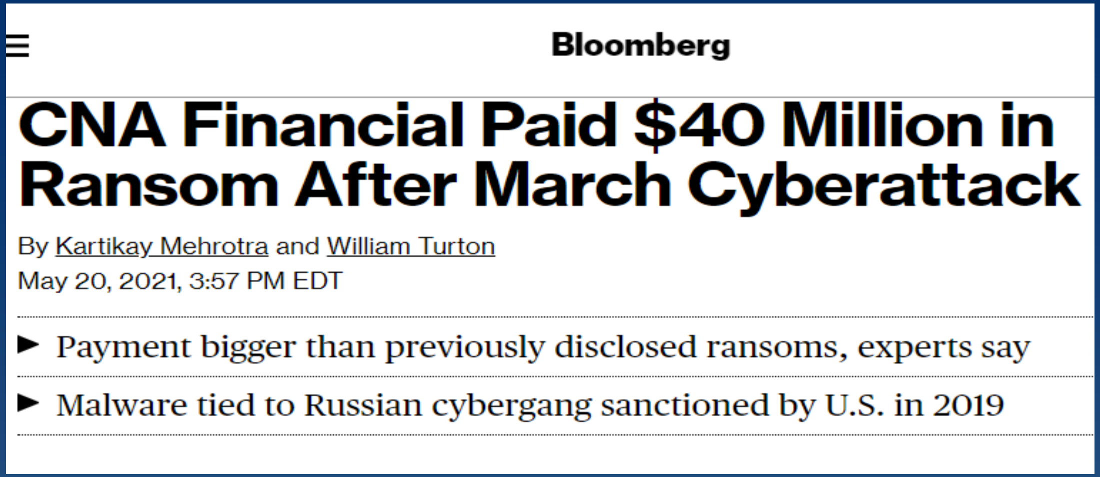
State of Ransomware – October 2021

Overview

1. State of Ransomware
2. Types of Losses
3. Claims Handling Best Practices
4. Incident Response Players
5. Pre-breach Commandments

State of Ransomware

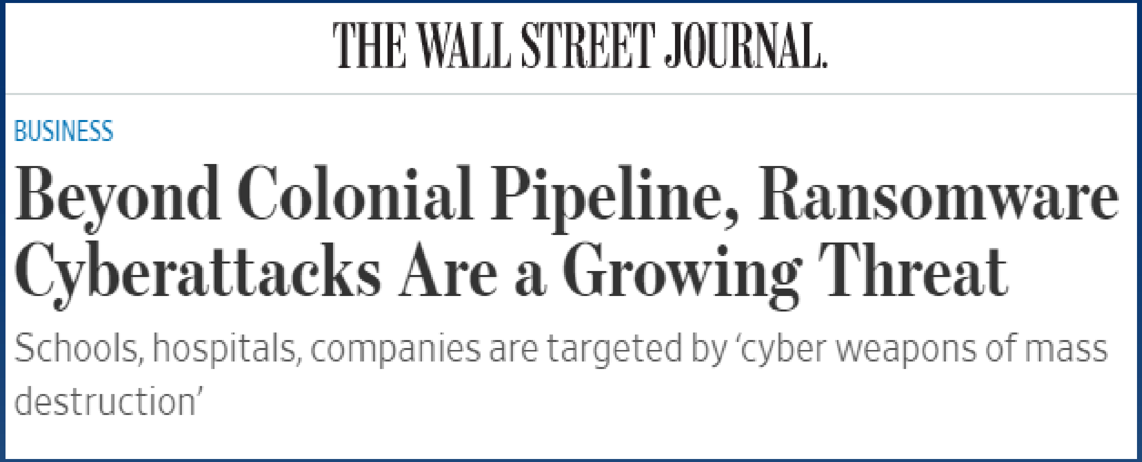


Bloomberg

CNA Financial Paid $40 Million in Ransom After March Cyberattack

By Kartikay Mehrotra and William Turton
May 20, 2021, 3:57 PM EDT

- Payment bigger than previously disclosed ransoms, experts say
- Malware tied to Russian cybergang sanctioned by U.S. in 2019

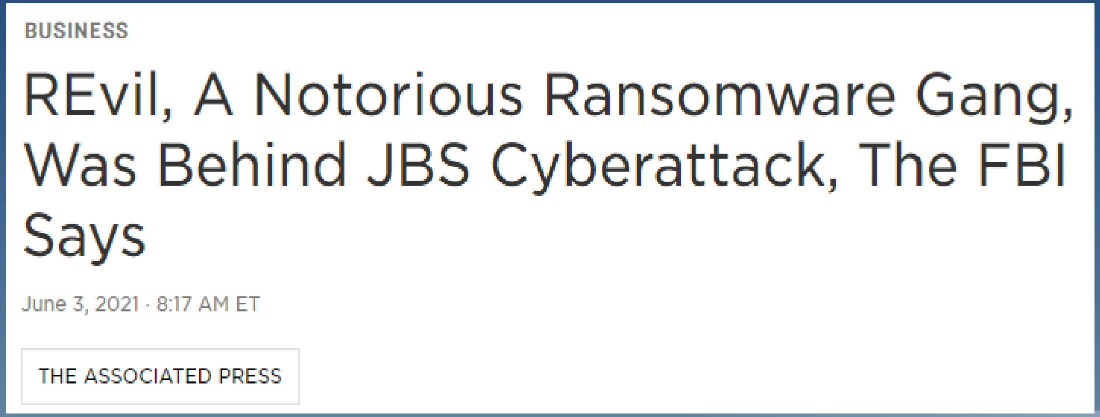


THE WALL STREET JOURNAL.

BUSINESS

Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Threat

Schools, hospitals, companies are targeted by 'cyber weapons of mass destruction'

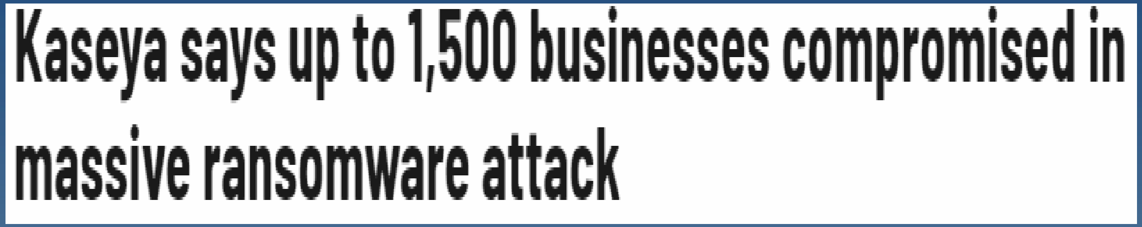


BUSINESS

REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says

June 3, 2021 · 8:17 AM ET

THE ASSOCIATED PRESS



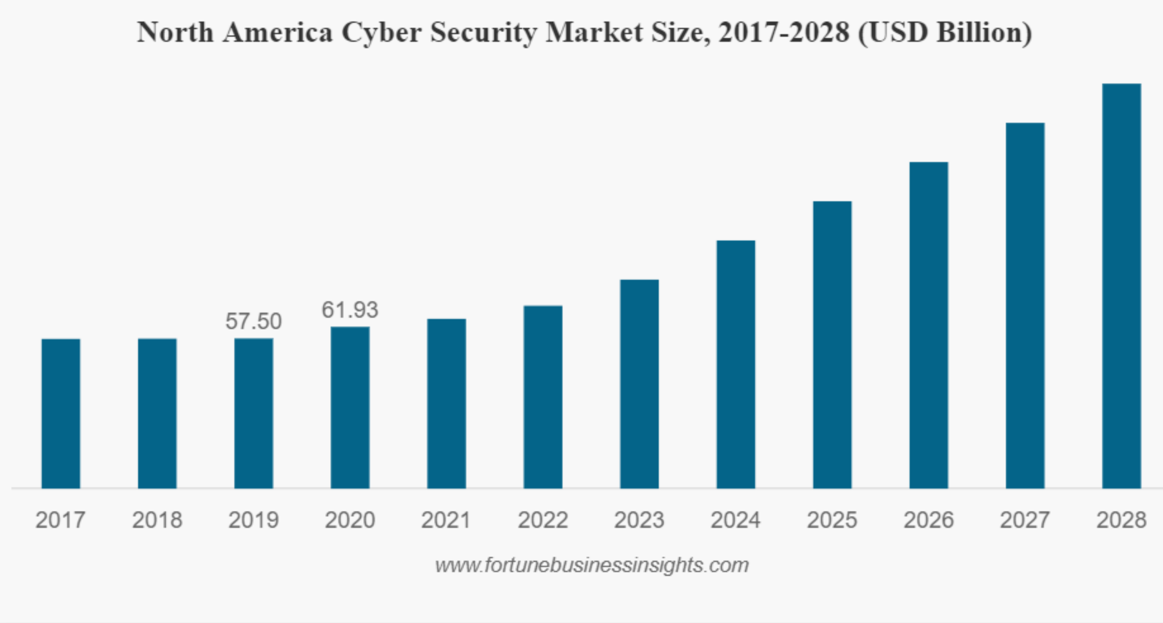
Kaseya says up to 1,500 businesses compromised in massive ransomware attack

State of Insurance Coverage

1. Start: Silent cyber

2. Then: Sublimit on commercial and PL policies

3. Now: Standalone and tower coverage



WILSON ELSER

Overview – Claims Handling Best Practice

- Secure network
- Engage breach counsel
- Iron out incident response plan
  - Who is doing what?
  - Are all the bases covered?
  - Preapproval process clear?
- Data privacy and breach compliance

Overview – Ransomware

1. Threat actor gains foothold
2. Traverses within network environment
3. Anti-forensics and persistence
4. Potential data exfiltration
5. Malicious encryption
6. Demand ransom payment in exchange for:
   - Decryption tool; and/or
   - Promise to delete and not leak/sell any exfiltrated data
7. Data leak and potential harassment

Types of Losses (Immediate)

- Business interruption
  - Loss of revenue
  - Third-party claim exposure
  - Liquidity issues
- Ransom services and potential payment
- IT restoration
  - Triage
  - Wipe and rebuild as needed
  - Reimage
- Forensics
  - Endpoint detection and response (EDR)
    - Licensing and active monitoring
  - Forensic investigation
    - 5-20 hours per server, at around $300/hr and 4 servers = $24k
  - Report writing
- Data recovery
  - Express evaluation and then recovery
- Crisis communications

Types of Losses

- Breach counsel
  - Triage advisory
  - Initial and continuing notifications
  - Crisis communications assistance
  - Handle third-party and regulatory contact
- Third-party claim exposure
  - Private cause of action?
  - Article III jurisdiction?
  - What kind of data?
  - Who is downstream (or upstream)?

- Specialized investigations
  - Response to regulatory inquiry
  - PCI DSS
- Notification
  - Common panel vendor minimum of $2k
  - NCOA, letter mailing, credit monitoring, and optional call center
  - Enrollment rates fluctuate:
    - .05% - 3.5% retail events
    - 4% - 9.5% health care related events
    - 7%-12% banking/CPA/Financial firms
    - 12% - 20% instances of fraud

Initial Considerations

- Current status of environment
  - If not secure, then disconnect
  - Get EDR
- Coverage and subrogation
  - Time sensitive preapprovals needed
- Client industry
  - HIPAA and the FTC Act
  - GLBA
  - Government
  - FERPA
- Is critical data backed up
- Client's existing in-house IT capabilities
  - IT provider or MSP assistance?
  - Is onsite assistance needed?
- Sensitivity of any exfiled data
- Ransomware gang / variant / strain
- **Preserve forensic evidence**

Incident Response Players

- The Insured / victim company
- MSP or IT provider
- Broker
- Carrier
- Incident response team:
  - Breach counsel
  - Forensics and ransom communications
  - IT restoration
  - Crisis communications
  - Data recovery

Players – the Insured / victim company

- Will need quicker responses than most other claims
- Ensure email has been cleared/secured
- May need client involvement of both decision-making stakeholder and internal IT professional
- Companies vary on their existing IT capabilities
  - Entirely outsourced to a third-parties
  - Single internal officer who leans on third-parties
  - Handful of internal resources, using third-parties as needed
  - Robust and complete internal capabilities

Players – Managed Service Provider (MSP) or IT company

- IT provider is generally:
  - Formally “on retainer” with a Master Service Agreement; or
  - Ad hoc local IT company
- MSP is usually the first call
- Check threat intel. Is variant is known to exploit remote monitoring and management (RMM) tools?
- Determine MSP scope to tailor response and avoid duplication
- Ease outside firm into engagement with potentially defensive MSP
- Get proposed hours and rates up front
- Contract language varies on services provided and limitation of liability

Players – Data Privacy (“Breach”) Counsel

- Immediately commence attorney-client relationship
  - Protects communications from disclosure if there are third party claims
  - (Should) maintain confidentiality of forensic findings
- Iron out and optimize incident response plan
- Recommend appropriate vendors
- Make any immediate statutory, contractual, or proactive notifications
- Guide incident response plan through conclusion
- Make additional notifications as forensics concludes
- Handle any third party or regulatory activity or actions

Players – Forensics and Ransom Communications

- License and deploy EDR
- Obtain forensic evidence
  - Images, logs, and related artifacts
- Ransom communications
  - OFAC attestation letter
  - Can monitor leak site
  - Note: Know carrier reimbursement policy
- Provide forensic report upon request
  - Executive summary
  - Comprehensive report.

- Clear email environment
- Conduct investigation, with two primary goals:
  1. Root cause analysis (RCA) to determine the “threat vector”, i.e. how compromise occurred
  2. Extent of sensitive data access and/or exfiltration. Specifically, opining on:
     - i. Manual unauthorized activity within environment
     - ii. The presence of any persistence
     - iii. Any exfiltration or obfuscation

Players – Incident Response Team

- IT restoration
  - Assist with triage and forensic imaging
  - Remediate and rebuild network infrastructure as appropriate
  - Restore and reimage data
- Data Recovery
  - Attempting to recover data direct from damaged or corrupted hardware
  - Increased cost for express service

- Crisis Communications / PR
  - In cases of:
    - High-profile client without internal marketing or PR department
    - Publicized event or local media attention
    - Customer-facing or PCI DSS

Pre-breach Commandments

1. Employee phishing training
2. Secure cloud backups
3. Multi-factor authentication (MFA)
4. Network segregation and data minimization
5. No open RDP ports
6. EDR with a security operations center (SOC), if in budget
6. Written information security program/plan (WISP)
   - Employee rules for data hygiene
   - Who is responsible for what?
   - Vendor configurations and RMM
   - Other statutory boxes to check
7. Sufficient and applicable insurance!

State of Ransomware – November 2021