



**Baker
McKenzie.**

Global Cybersecurity and Ransomware Preparedness

ACC San Francisco Bay Area

San Francisco | March 23, 2022

Palo Alto | March 24, 2022



Speakers



Lothar Determann
Partner
lothar.determann
@bakermckenzie.com



Jessica Nall
Partner
jessica.nall
@bakermckenzie.com



Cyrus Vance
Partner
cyrus.vance
@bakermckenzie.com



Jonathan Tam
Partner
jonathan.tam
@bakermckenzie.com



Bilyana Lilly, PhD
Information Warfare,
Russia, Ransomware
Deloitte

Agenda

1

Recent Trends In Cyber Incidents
And Ransomware

2

Security Vulnerabilities: A Technical
Primer

3

Privacy Laws Obligations

4

Incident Preparedness

5

Panel Discussion

6

Post-breach Litigation: Class
Actions And Regulatory
Proceedings

7

Q&A

The background of the slide is a city skyline at night, with various skyscrapers visible. A semi-transparent blue filter is applied over the entire image. A green wireframe mesh, resembling a topographical map or a data network, is overlaid on the city. The mesh consists of numerous points connected by thin lines, creating a series of peaks and valleys. The overall aesthetic is high-tech and digital.

1

Recent Trends

NYC Response to Cyber Threats

THE WALL STREET JOURNAL.

OPINION | COMMENTARY

New York Launches a Cybercrime Brigade

A new citywide initiative aims to coordinate digital law-enforcement efforts.

By Cy Vance Jr. and James P. O'Neill
April 1, 2019 7:08 pm ET

In a little more than a month last year, cybercriminals temporarily debilitated Atlanta's computer systems, disrupted Baltimore's 911 emergency system, and forced Colorado's Department of Transportation offline. Atlanta's cyberattack alone cost taxpayers an estimated \$17 million, according to a city report. These attacks transpired amid a yearlong barrage of international cybercrimes against hospitals, governments, banks and utilities that exposed the personal information of millions of people, shut down large server networks, and caused significant financial loss.

It is clear to us in law enforcement that these threats are an issue of public safety. If a hospital, water system or energy grid goes down, people could die. When critical services like transportation and government offices can't function, it affects the

THE WALL STREET JOURNAL.

◆ WSJ NEWS EXCLUSIVE

New York City Opens Cyberattack Defense Center

The initiative brings together government agencies and business groups to share intelligence and respond to digital threats

New York City has become the first major American metropolitan area to open a real-time operational center to protect against cybersecurity threats, regional officials said.

Set in a lower Manhattan skyscraper, the center is staffed by a coalition of government agencies and private businesses, with 282 partners overall sharing intelligence on potential cyber threats. Its members range from the New York Police Department to [Amazon.com](https://www.amazon.com) Inc. and International Business Machines Corp. to the Federal Reserve Bank and several New York healthcare systems.

NYC CCSI Participating Sectors



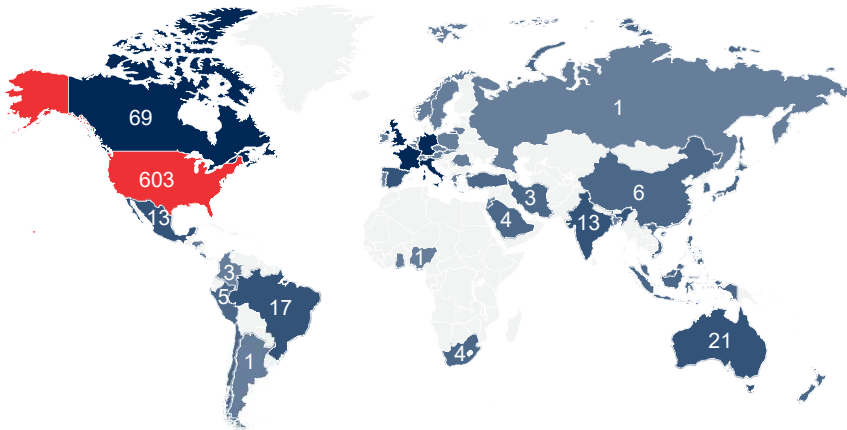


2

Security Vulnerabilities: A Technical Primer

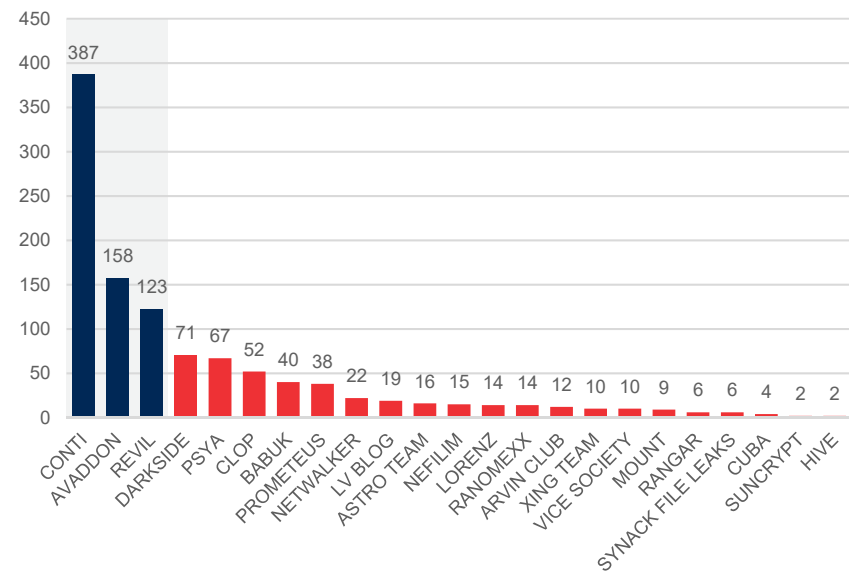
Who are the threat actors and who do they target?

US-based companies are most targeted.



The **US** is the most targeted country with **54.9%** of total victims. The top **10** targeted countries constitute **84%** of total victims.

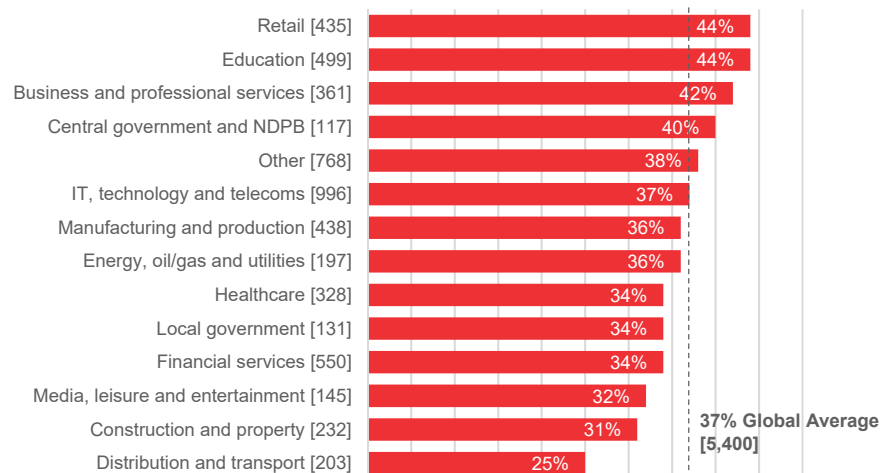
The top 3 groups – Conti, Avaddon and REvil – are responsible for **60%** of total victims



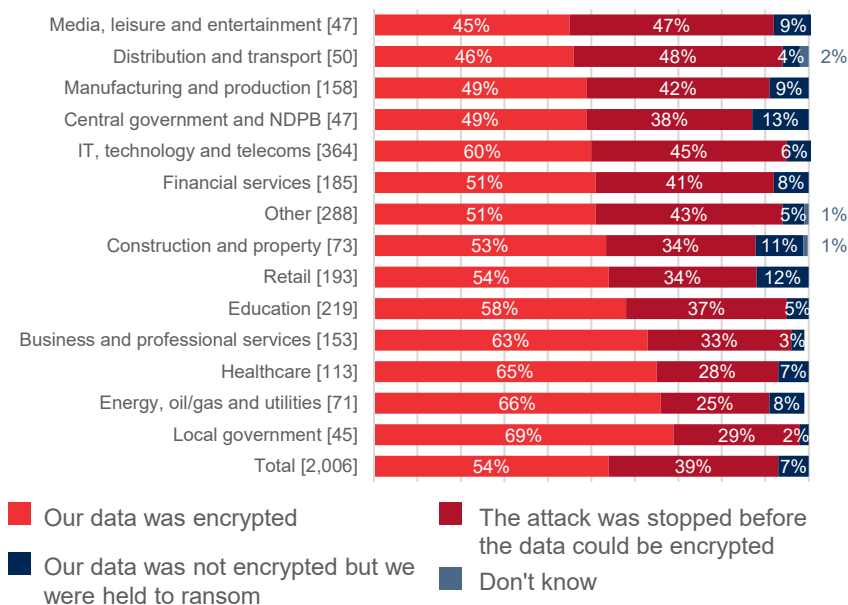
Source: [Ransomware attack statistics 2021 - Growth & Analysis | Cognyte](#)

Ransomware impact by industry

Propensity to be hit by ransomware varies by industry.



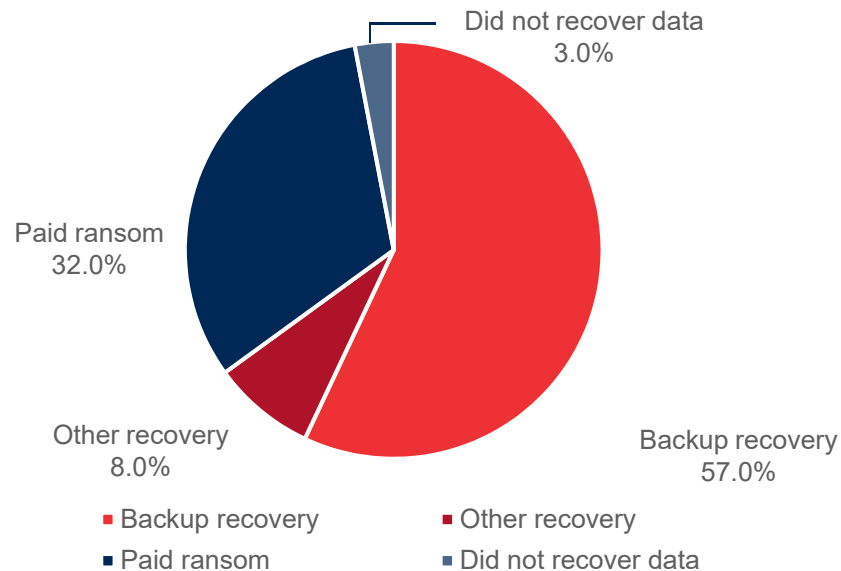
Ability to stop ransomware varies by industry.



Source: Sophos Report, available at: [sophos-state-of-ransomware-2021-wp.pdf](https://www.sophos.com/usa/pressroom/press-releases/2021/sophos-state-of-ransomware-2021-wp.pdf).

Data restoration and recovery

How Companies Recover Data After a Ransomware Attack









| 2020 | 2021 | |
|------|------|-----------------------------------|
| 26% | 32% | Paid ransom to get data back |
| 56% | 57% | Used backups to get data back |
| 12% | 8% | Used other means to get data back |
| 94% | 96% | Total that got data back |

Paying the ransom only gets you some of your data



Source: Sophos Report, available at: [sophos-state-of-ransomware-2021-wp.pdf](https://www.sophos.com/en-us/press-room/articles/sophos-state-of-ransomware-2021-wp.pdf).

Common cyber attack vectors

| | | |
|--------------------------|---|---|
| Phishing | <ul style="list-style-type: none">Fraudulent attempt to steal personal information |  |
| Malware | <ul style="list-style-type: none">Codes with malicious intent that typically steals/destroys data |  |
| Remote Desktop Protocols | <ul style="list-style-type: none">Used by employees and other authorized users to access server infrastructure remotely |  |
| Compromised Credentials | <ul style="list-style-type: none">Weak or compromised passwords may allow an attacker to access a target system |  |
| Denial-of-Service | <ul style="list-style-type: none">Focuses on disrupting the service to a network |  |
| Digital Supply Chain | <ul style="list-style-type: none">Exploits vulnerabilities in business software or managed service providers (MSPs) |  |

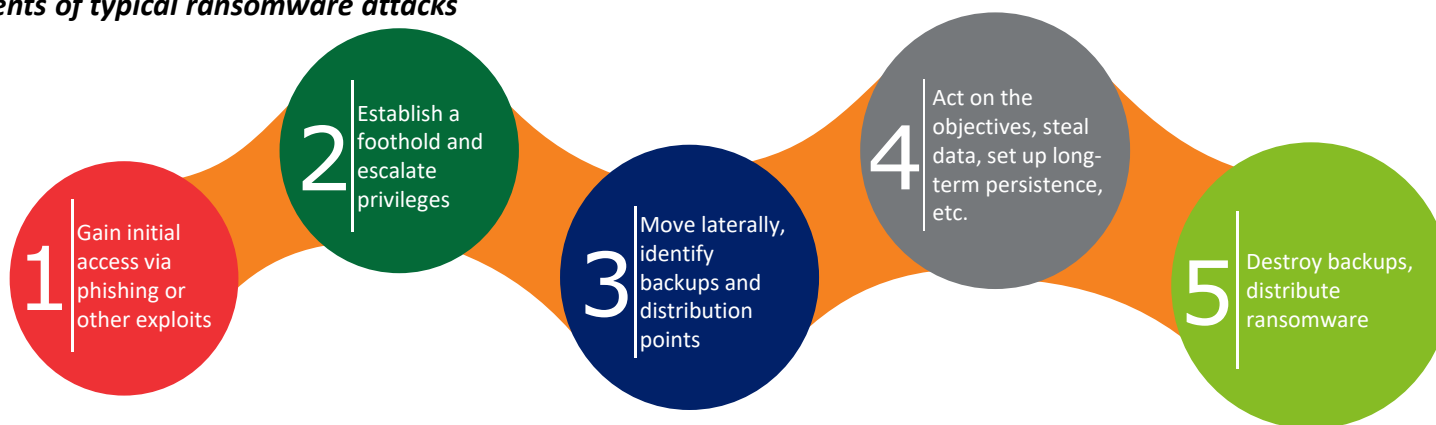
Cyber attack surface



Ransomware attack: A multi-faceted threat

Attacks have evolved from being a cyber nuisance to complex multi-faceted extortion campaigns driven by cyber criminals, encompassing data theft and business disruption in addition to ransom.

Key components of typical ransomware attacks



Ransomware groups leverage **Ransomware-as-a-Service** platforms, **access brokers**, data release (**double extortion**) and other types of cyber operations such as Distributed Denial of Service (DDoS), and supply-chain attacks



Cybercriminals are **destroying backups**, increasing the effectiveness of ransom attacks and confounding recovery; **cloud solution backups** may see an increase in ransomware incidents



Attackers may leverage access to an organization to **ransom partners, supply chain, and connected third parties**; ongoing conflict likely to inspire **more ransomware attacks**

Ransomware is the most prevalent emerging business risk

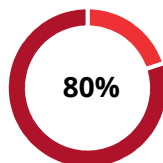
Ransomware attacks now pose not only a cybersecurity risk, but also an enterprise-wide risk, threatening business continuity and operations.

GROWING THREAT

4,000

Ransomware attacks occur daily

80% of Companies who paid the ransom experienced another attack



191 days

The average number of days an organization takes to identify a breach



8.7% increase

In the average number of cases that are exfiltrating and dropping ransomware

FINANCIAL TURMOIL

\$265 BILLION

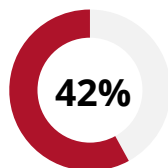
Ransomware attacks will cost its targets \$265 billion by 2031



Victims paid \$350 million in ransom in 2020

104% increase

In the average ransom payment amount from Q4 2019



42% of companies with cyber insurance did not have all losses covered by insurance

BUSINESS IMPACTS

19 days

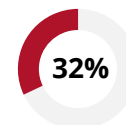
The average time of system outages



92% of companies who paid ransom do not get all their data restored



53% of companies reported that their brand suffered



32% of companies lost C-level talent as a direct result of a ransomware incident

26%

26% of organizations report a requirement to close operations for some period of time

Sources: Sophos State of Ransomware | 2021; 2021 Cyber Security Statistics; The Ultimate List Of Stats, Data & Trends | PurpleSec; Security Trends: Data Breach Statistics from 2018 and Predictions for 2019 (securitymetrics.com); Attackers use botnets to break into networks faster (cybereason.com); Global Ransomware Damage Costs Predicted To Exceed \$265 Billion By 2031 (cybersecurityventures.com); Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force (securityandtechnology.org)

Draft - For Discussion Only

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Ransomware lessons learned

The lessons learned listed below represent some of the more common items identified with ransomware events

Access Management

Failure to implement least user privilege (LUP) can facilitate an adversary's ability to escalate throughout the environment and allow defenders less time to detect a ransomware attack before it takes place

Untested and/or Unused IR Plans

Lack of clear roles and responsibilities and leveraged incident response processes result in confusion and chaos during a ransom incident hindering an organization's ability to effectively respond

Recovery Capabilities

Lack of or untested backups of critical systems and configurations can hinder an organization's ability to effectively recover from a ransomware incident, resulting in the loss of critical data and resources

Security Controls

Lack of security controls can leave an organization vulnerable to ransomware attacks, increasing the opportunity for an adversary to exploit critical systems

Environment Visibility

Lack of visibility and knowledge about the network an organization secures hinders the ability to fully scope an environment for ransomware and can impact containment procedures allowing an adversary's footprint to spread

Processes and Procedures

Failure or lack of processes and procedures hinder a response team's effort in containing, eradicating and recovering from a ransomware incident increasing the time taken to effectively restore business operations

Technology Stack

Inability to detect an adversary at each point of the kill chain can hinder an organization's efforts to mitigate threats before ransom can take place

Cyber Wargaming

Lack of interactive cybersecurity exercises to evaluate and improve cyber incident response preparedness through broad simulation attacks prevents an organization from understanding how to operate as an effective team to identify ransomware and understand its environment



3

Privacy Law Obligations

Post-attack remediation

Notifications and Responding to Inquiries



Notification obligations

- Regulators
- Enforcement authorities
- Customers
- Individuals



Customer inquiries



Individual inquiries



Regulator / Enforcement authority inquiries

- SEC focus on public companies, especially post *Solarwinds*
- Additional requirements for financial services companies
- Interest from state authorities



Notification obligations: key jurisdictions

| | Regulator / DPA | Data Subject | Additional Sector-Specific Requirements |
|-----------|---|---|---|
| US | <input checked="" type="checkbox"/> <i>*state law</i> | <input checked="" type="checkbox"/> <i>*state law</i> | <input checked="" type="checkbox"/> |
| Canada | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Mexico | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Brazil | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| UK | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Germany | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| India | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Japan | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Australia | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Notification obligations: regulators and law enforcement



Notification obligations: implications



Notification triggers are highly jurisdiction-specific



Specific rules regarding the **timing, content and form** of notification



“without unreasonable delay”



Substantial potential **penalties**



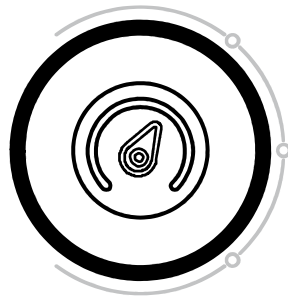
4

Incident Preparedness

Managing risks



Cybersecurity compliance

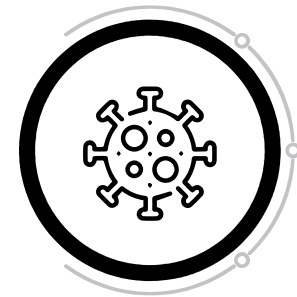


Risk allocation

- Contractual Provisions
- Insurance Policy



Company policy Personnel training



Planning in light of COVID-19

- Crisis management
- Work from home arrangements

Pre-attack preparation

Action Items



Data Security Incident Response Plan and Trainings



Avoidance

- Back-up systems segregated sufficiently?
- Operational recovery plan practiced?
- Back-up communications solutions in place?
- Business continuity plan?
- "Crown jewels" assessments



Engagement of Response Providers

- Baker McKenzie
- Forensic Investigators
- eDiscovery Providers
- Public Relations / Crisis Management
- Credit Monitoring / Identity Theft Protection / Call Center
- Ransom Negotiators / Payors



Insurance

- Review and understand scope of cyber insurance coverage





Pre-attack preparation

Decision Points



Moral / PR / Corporate Decisions

- Is the company against paying ransoms?
- PR considerations
- Different approaches for different business segments?



Operational Issues

- Who pays and how (e.g., from what accounts)?
- Insurance requirements?
- Who/how to engage with attacker?



Regulatory Issues

- Diligence requirements for payments
- OFAC guidance
- SEC and market regulators



Law enforcement notification strategy

The background of the slide features a blurred city skyline at night, likely New York City, with prominent skyscrapers. Overlaid on this is a complex, glowing green wireframe structure that resembles a network or a topographical map. The overall color palette is dominated by deep blues and greens.

5

Panel Discussion



6

Post-breach Litigation

Post-breach Litigation

Who may sue and where?

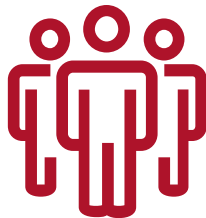
State Attorneys General



Individual Data Subjects



Class plaintiffs



Multi District Litigation



Questions



The background of the slide features a dark blue, blurred cityscape at night. Overlaid on this is a complex, glowing green and white geometric network of lines and dots, resembling a digital or data visualization. The Baker McKenzie logo is positioned in the upper left corner.

Baker McKenzie.

Baker & McKenzie LLP is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2022 Baker & McKenzie LLP

bakermckenzie.com