



SOUTHERN LEGISLATIVE CONFERENCE



# Cybersecurity: Impacts, Implications, and Action for State Governments

*Mark Weatherford  
Chief Strategy Officer  
National Cybersecurity Center*

**The invention of the ship, was also  
the invention of the shipwreck.**



# We have a **PERFECT STORM** in cybersecurity

- Laws and law enforcement are limited, inconsistent, and unenforced
- The speed of innovation is far faster than the speed of security
- Anonymous access to vast resources and information
- 30-40 year old protocols with no security
- Lack of international norms of behavior
- Hacker tools look and act legitimate
- Virtually unlimited interconnectivity
- No national or political boundaries
- Value in everything online
- Billions of clueless victims
- No taxes = no tax evasion



Most companies are out-matched in their ability to combat cyber-attacks from nation states, global criminals and malicious insiders. *In no other arena* are private organizations expected to do battle with the likes of:



### International organized crime

- Customer and credit card account manipulation
- Harvesting PII for identity theft



### Hacktivists

- Political hacktivism and hacking for the *Lulz*
- Cyber-civil disobedience

### Global Nation States

- Cyber espionage and IP theft
- Economic data and competitive intelligence



### Terrorists

- Targeting critical infrastructures
- Maximum lethal impact to society



# Traditional ideas about conflict management **DON'T APPLY** in the cyber domain

- The cyber domain is an independent landscape where *geography is both irrelevant and an advantage*
- It's difficult to differentiate between a *laptop with WiFi access* and a nation-state actor or international cyber-criminal
- Escalation *is not* linear, but rather potentially exponential
- Deterrence *assumes* some sense of adversary rationality
- A noisy attacker doesn't matter *if no one is listening!*



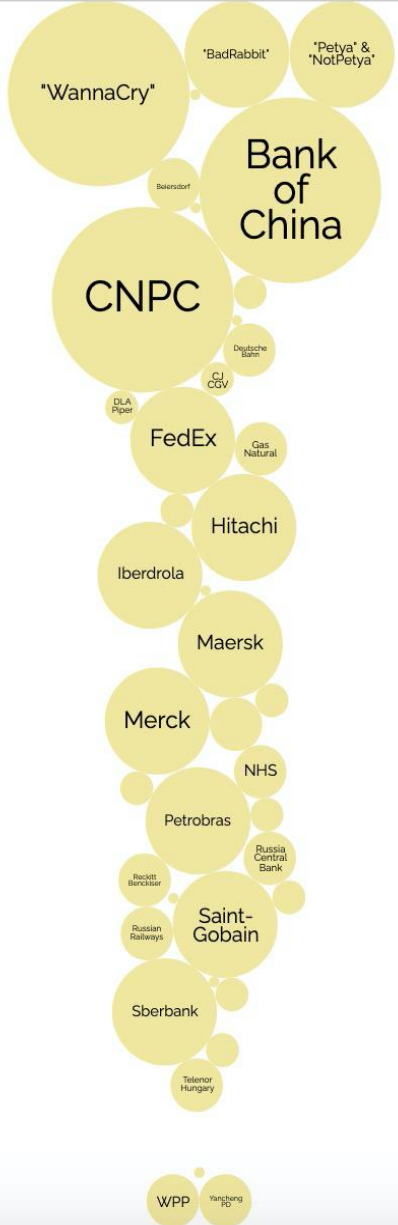
# Ransomware Attacks BETA

size = size of organisation

PRE 2016



2017



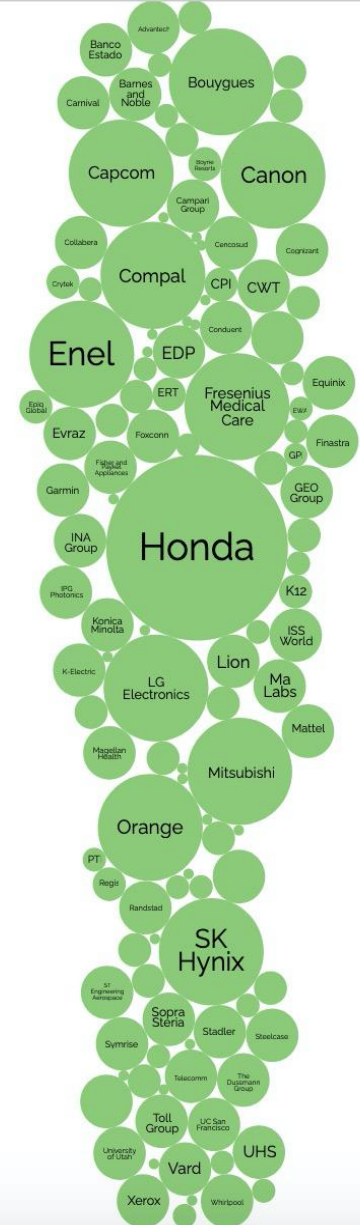
2018



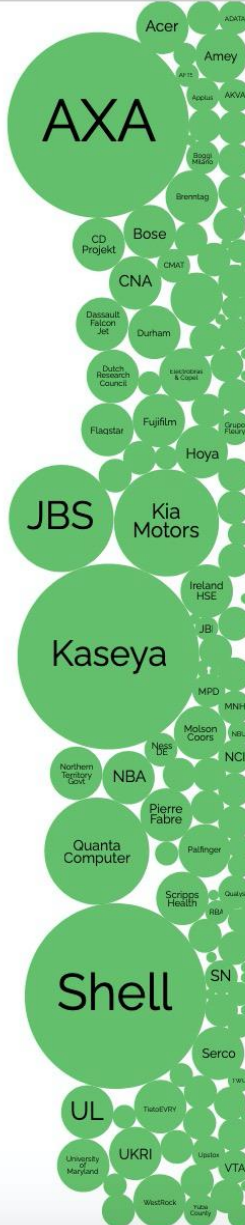
2019



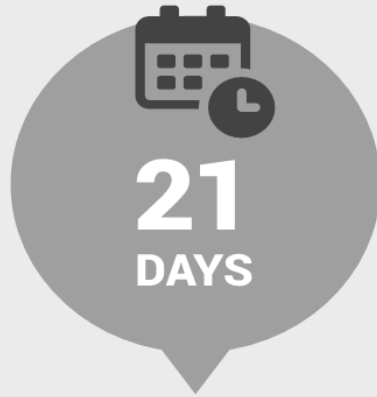
2020



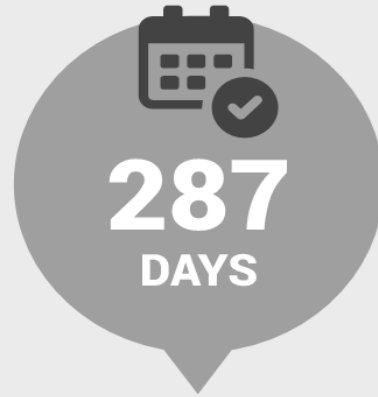
2021



# The scourge of ransomware



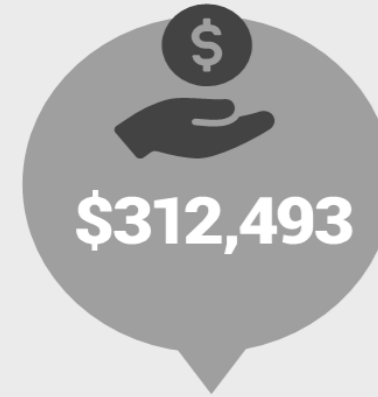
Average downtime due to ransomware attacks<sup>2</sup>  
(Coveware)



Average days it takes a business to fully recover from an attack<sup>3</sup>  
(Emsisoft)



Victims paid in ransom in 2020 – a 311% increase over the prior year<sup>4</sup>  
(Chainalysis)



The average payment in 2020 – a 171% increase compared to 2019<sup>5</sup>  
(Palo Alto Networks)

In 2020, nearly  
**2,400**

U.S.-based governments, healthcare facilities, and schools were victims of ransomware



# 2021 shaping up to be another annus horribilis

- **December 2020.** Over 200 organizations around the world—including multiple US government agencies—were revealed to have been breached by Russian hackers who compromised the software provider **SolarWinds** and exploited their access to monitor internal operations and exfiltrate data.
- **May 2021.** On May 6, the **Colonial Pipeline**, the largest fuel pipeline in the United States, was the target of a ransomware attack. The energy company shut down the pipeline and later paid a \$5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group.
- **May 2021.** The world's largest meat processing company, Brazilian-based **JBS**, was the victim of a ransomware attack. The attack shut down facilities in the United States, Canada and Australia. The attack was attributed to the Russian speaking cybercrime group, REvil.Colonial Winds
- **July 2021.** A massive supply chain ransomware attack by the Russian REvil ransomware gang on **Kaseya** impacted thousands of businesses who use Managed Service Provider services.

# The latest “wake-up call” - Kaseya VSA

- **What is a Managed Service Provider (MSP)?** An MSP is a company that manages networks and computers for companies that are too small to justify having full-time IT staff. MSP's often have hundreds or thousands of customers and do everything from patching computers, to managing backups. MSP's service their customers remotely and administer all their customers' networks at the same time through automated processes.
- **What is a Supply Chain Attack?** A supply chain attack is when the attacker compromises a software supplier in order to provide malicious code to the eventual victim. Supply chain attacks are particularly devastating because it affects both the company's suppliers and their suppliers' suppliers. It is called the n-tier problem.
- **What is Kaseya Virtual System Administrator (VSA)?** Kaseya is vendor of Managed Service Provider software and Kaseya VSA is the automated software tool used by many MSPs to control customer systems.
- **Who is REvil?** The affiliate business model for ransomware is where the corporate overlord provides the technology, branding, and processes the payments for both the affiliates and the victims. The arrangement is to the relationship between a fast-food brand and its franchisees. **REvil** is the Russian McDonalds of the criminal ransomware world with a very high profile.
- **So What Happened in this Incident?** An affiliate of the REvil ransomware gang launched a ransomware supply chain attack against a large number of Kaseya MSP installations, resulting in ransomware infections on the MSPs' customers' computers.
- **What to do about the attackers?** A friend of mine has begun to calling Russia a “Pirate State” because it's highly unlikely the REvil crew will face justice in the Putin regime.

• [Source: https://www.lawfareblog.com/what-happened-kaseya-vsa-incident](https://www.lawfareblog.com/what-happened-kaseya-vsa-incident) July 4, 2021

# State and local governments are outgunned and under-resourced

0 COMMENTS  
[COMMENT NOW](#)

announced a new report called *The Municipalities*.

Login

100% 0%

Like

**to Keep Up**

In its latest report, KnowBe4 looks at the financial costs, reputational effects, level of public trust, and other impacts that cyberattacks have had on municipalities.

Tampa Bay, FL (July 7, 2020) – KnowBe4, the provider of the world's largest security awareness training and sim

announced a new report called *The Municipalities*.

ox File Edit View History Bookmarks Tools Window Help

https://www.americancityandcounty.com/2021/03/22/report-ransomware-

informa

CO-OP SOLUTIONS COMMENTARIES NEWS IN-DEPTH MULTIMEDIA RESOURCES

ADMINISTRATION ECONOMY & FINANCE PROCUREMENT PUBL

AMERICAN CITY & COUNTY

## Report: Ransomware attacks cost local state governments of \$18 billion in 2020

Written by Jason Axelrod 22<sup>nd</sup> March 2021

With local governments, schools and businesses connected, hackers have been at work trying

SECURITY

## Cyber Threats Rise Amid Chaos Resulting from Pandemic

With local governments, schools and businesses using the Internet to stay connected, hackers have been at work trying to exploit weaknesses in computer systems to steal money and personal information.

April 26, 2021 • Christian M. Wade The Eagle-Tribune, North Andover

HELPNETSECURITY News Features Expert analysis Reviews

Help Net Security October 15, 2020

## State and local governments under siege from cyber threats

Top barriers to overcome cybersecurity challenges

- 1 Lack of sufficient cybersecurity budget
- 2 Inadequate cybersecurity staffing
- 3 Legacy infrastructure and solutions to support emerging threats
- 4 Lack of dedicated cybersecurity budget
- 5 Inadequate availability of cybersecurity professionals

Source: 2020 Deloitte-NASCIO Cybersecurity Study.

# What is the role of government in private sector cybersecurity?

- Washington is finally beginning to understand what this means in the federal cybersecurity arena but still assumes they are smarter than the private sector
  - How about at the state and local government level?
- The Internet is (primarily) a private sector domain:
  - Not a government domain
  - Not a defense domain
  - Not a war domain
- What is the appropriate level of response?
  - Diplomacy?
  - Sanctions?
  - Offensive attacks?
  - Who do they support? When? How?
    - Fortune 500 vs Unfortunate 5000

# Legislation – 117<sup>th</sup> Congress

[S.1917](#) - K-12 Cybersecurity Act of 2021

[S.808](#) - Cybersecurity Disclosure Act of 2021

[H.R.4005](#) - Enhancing K-12 Cybersecurity Act

[H.R.3608](#) - Improving Contractor Cybersecurity Act

[H.R.2982](#) - National Guard Cybersecurity Support Act

[H.R.2980](#) - Cybersecurity Vulnerability Remediation Act

[H.R.3138](#) - State and Local Cybersecurity Improvement Act

[H.R.2685](#) - Understanding Cybersecurity of Mobile Networks Act

[S.658](#) - National Cybersecurity Preparedness Consortium Act of 2021

[H.R.3078](#) - Pipeline and LNG Facility Cybersecurity Preparedness Act

[S.2274](#) - Apprenticeship Program on Cybersecurity Training for Veterans

[H.R.117](#) - DHS Cybersecurity On-the-Job Training and Employment Apprentice Program Act

[H.R.2659](#) - United States-Israel Cybersecurity Cooperation Enhancement Act of 2021

.  
.

117 pieces of  
legislation at  
the federal  
level that  
address  
cybersecurity

-July 9, 2021

# Resources for government leaders

## National Cybersecurity Center



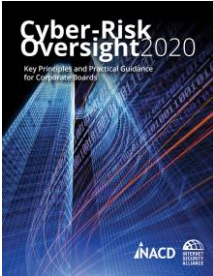
## Center for Internet Security



## Department of Homeland Security



## National Association of Corporate Directors



## Center for Internet Security



## National Governors Association



THE  
ENEMY  
ISN'T  
HACKERS  
IT'S  
APATHY

Mark Weatherford

[mark.weatherford@cyber-center.org](mailto:mark.weatherford@cyber-center.org)