RANSOMWARE TASK FORCE

Report Briefing for State/Local Leaders

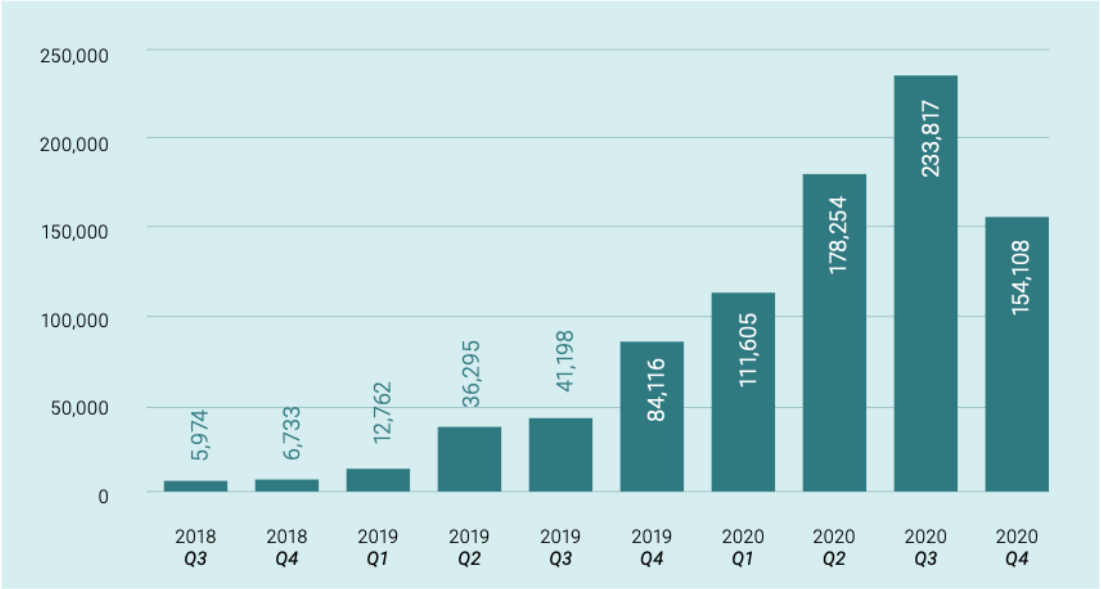
Combating Ransomware: A Comprehensive Framework for Action

Megan Stifel
Global Policy Officer
Capacity & Resilience Program Director
Global Cyber Alliance
Co-Chair, Ransomware Task Force

John A. Davis
Retired U.S. Army Major General
VP, Public Sector
Palo Alto Networks
Co-Chair, Ransomware Task Force

The Rise of Ransomware

FIGURE 1 **Average ransom in USD**



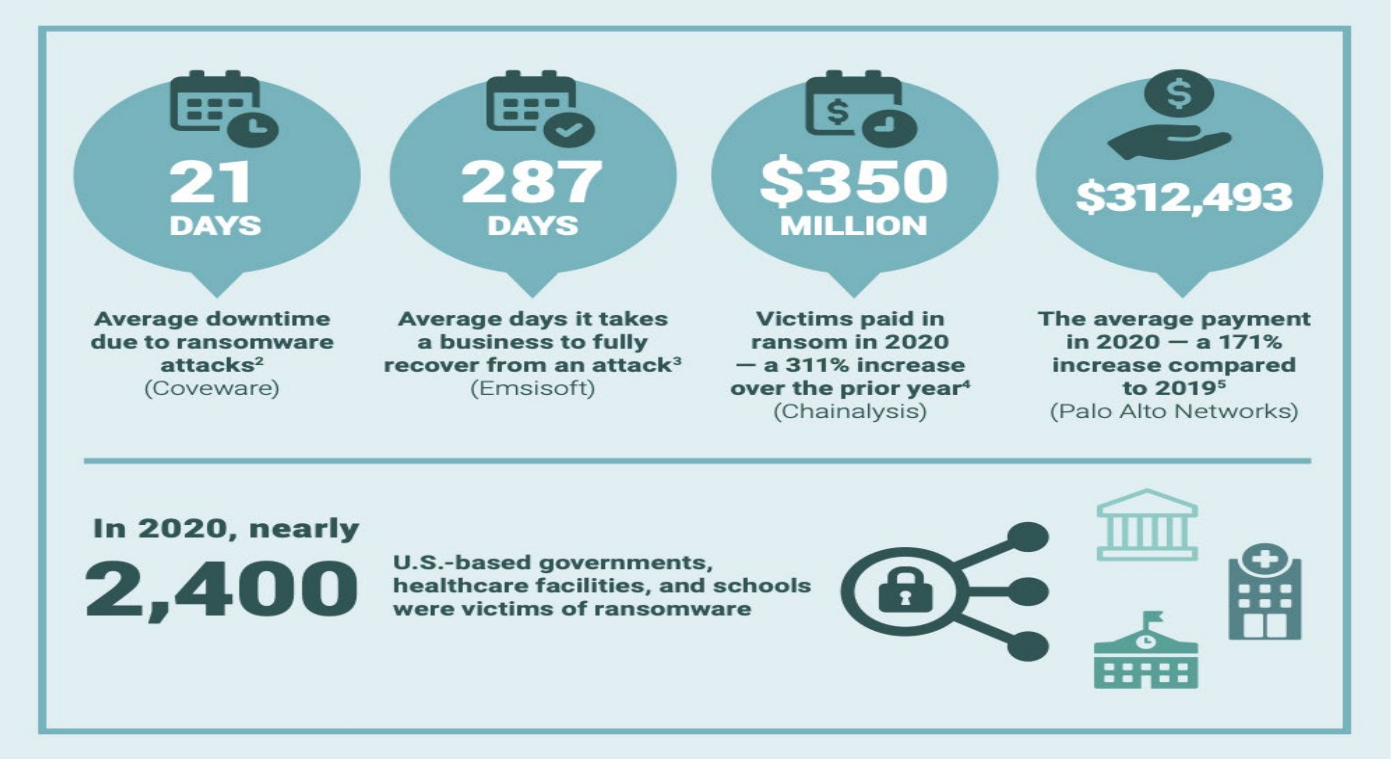
From The Coveware Quarterly Ransomware Report

Ransomware Targets:

- ➔ Hospitals
- ➔ Schools
- ➔ Local police
- ➔ Local governments
- ➔ Small businesses
- ➔ Large corporations

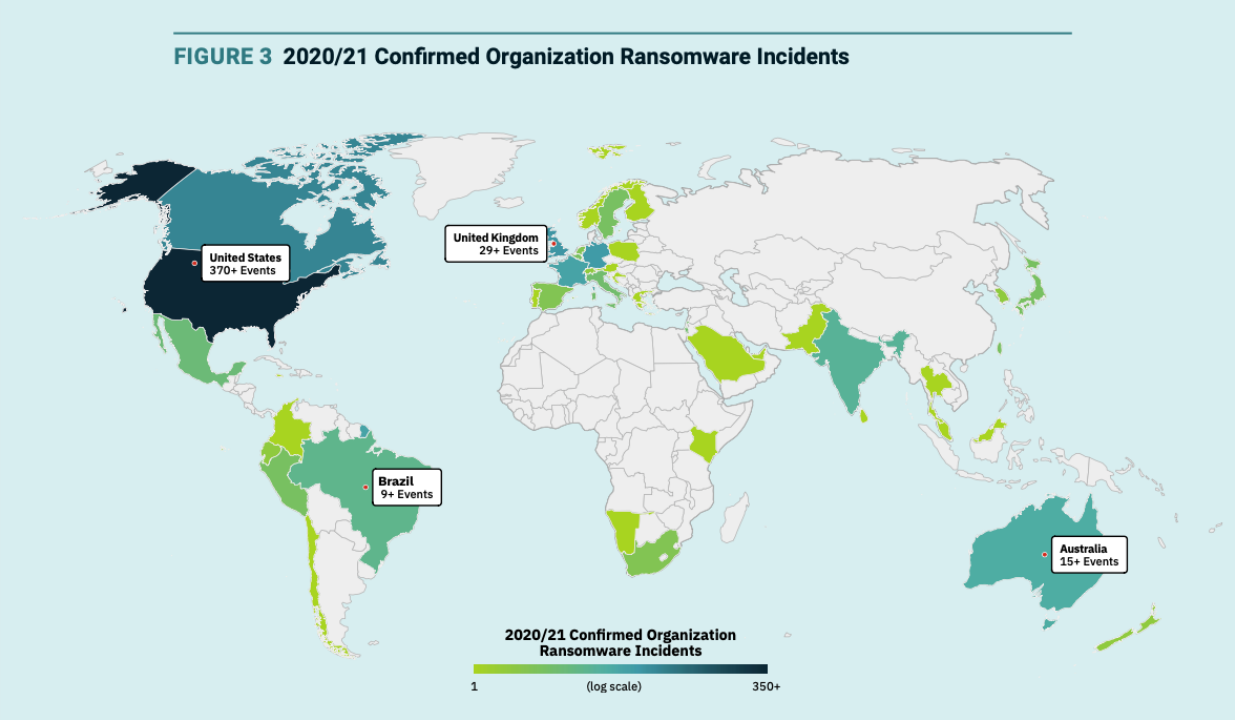
RANSOMWARE TASK FORCE

THE IMPACT OF RANSOMWARE



RANSOMWARE TASK FORCE

A Global problem



RANSOMWARE TASK FORCE

The Ransomware Task Force

- 60+ experts from industry, government, law enforcement, civil society, and international organizations worked hand-in-hand
- Met Jan —April to centralize expertise from different sectors, create comprehensive solutions

Notable Sectors Included:

- ➔ Incident Responders, Threat Intelligence
- ➔ Cyber Insurance Providers, Brokers
- ➔ Healthcare Entities
- ➔ Cryptocurrency Analysis Firms / Exchanges
- ➔ International Law Enforcement
- ➔ Financial Regulators
- ➔ Cybersecurity Providers
- ➔ Corporations including Microsoft, Amazon
- ➔ CTA, GCA, other civil society organizations

RANSOMWARE TASK FORCE

RTF Framework

1. *Deter Ransomware Attacks*

2. *Disrupt the ransomware business model*

3. *Help organizations prepare*

4. *Respond to ransomware attacks more effectively*

RANSOMWARE TASK FORCE

Priority recommendations

1. The United States should lead by example and **execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign**, coordinated by the White House. This must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.

RANSOMWARE TASK FORCE

Priority recommendations

2. Coordinated, international diplomatic and law enforcement efforts must **proactively prioritize ransomware through a comprehensive, resourced strategy** , including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.

RANSOMWARE TASK FORCE

Priority recommendations

3. Governments should establish Cyber Response and Recovery Funds to **support ransomware response** and other cybersecurity activities; **mandate that organizations report ransom payments** ; and require organizations to consider alternatives before making payments.

RANSOMWARE TASK FORCE

Priority recommendations

4. An internationally coordinated effort should **develop a clear, accessible, and broadly adopted framework** to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to **drive adoption**.

RANSOMWARE TASK FORCE

Priority recommendations

5. The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading “desks” to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.

RANSOMWARE TASK FORCE

The Ransomware Task Force: NEXT STEP

- Will not continue in its current form, although the group will likely stay connected for a time
- Different Task Force members will work together in smaller groups to implement the recommendations

Roll out Activities To Date And Planned:

- ➔ On-going media engagement
- ➔ Launch event on April 29th
- ➔ US Congressional Hearing May 5th
- ➔ CTA Webinar on May 6th
- ➔ GCA Twitter Chat on May 12th
- ➔ Brief to UK Government June 21st
- ➔ White House briefing June 24th
- ➔ Brief to Canadian Government July 6th
- ➔ Brief to NIST July 14th
- ➔ Brief to Australian Government July 26th
- ➔ Brief to Netherlands Government July TBD

RANSOMWARE TASK FORCE

RANSOMWARE TASK FORCE LEADERSH

RTF Co-Chairs

***Megan Stifel**, Global Cyber Alliance*

***John Davis**, Palo Alto Networks*

***Michael Phillips**, Resilience*

Executive Director

***Philip Reiner**, Institute for Security and Technology*

RTF Working Group Co-Chairs

***John Davis**, Palo Alto Networks*

***Megan Stifel**, Global Cyber Alliance*

***Michael Phillips**, Resilience*

***Kemba Walden**, Microsoft*

***Jen Ellis**, Rapid7*

***Chris Painter**, The Global Forum on Cyber Expertise*

***Michael Daniel**, Cyber Threat Alliance*

***Philip Reiner**, Institute for Security and Technology*

RANSOMWARE TASK FORCE

RANSOMWARE TASK FORCE Membersh

Joel de la Garza, *a16z*
Temi Adebambo, *Amazon Web Services*
David Forcsey, *Aspen Digital*
Jeff Troy, *Aviation ISAC*
Rich Friedburg, *Blackbaud*
Austin Berglas, *BlueVoyant*
Lewis Robinson, *Center for Internet Security*
Roger Francis, *CFC Underwriting*
Don Spies, *Chainalysis*
Pamela Clegg, *CipherTrace*
Brad Garnett, *Cisco*
Matt Olney, *Cisco*
Peter Lefkowitz, *Citrix*
Bill Siegal, *Coveware*
James Perry, *CrowdStrike*
Stéphane Duguin, *The CyberPeace Institute*
Yonatan Striem-Amit, *Cybereason*
Neil Jenkins, *Cyber Threat Alliance*
Andy Thompson, *CyberArk*
Ari Schwartz, *Cybersecurity Coalition*
John Banghart, *Cybersecurity Coalition*
Ryan Weeks, *Datto*
Patrice Drake, *Deloitte*
Keith Mularski, *Ernst & Young*
Stacy O'Mara, *FireEye*
Nick Bennett, *FireEye*
Jill Fraser, *Jefferson County, CO*
Mark Orsi, *K12 SIX*

RANSOMWARE TASK FORCE

RANSOMWARE TASK FORCE Membersh

Kent Landfield, *McAfee*
Ginny Badanes, *Microsoft*
Kaja Ciglic, *Microsoft*
Ping Look, *Microsoft*
Jennifer Coughlin, *Mullen Coughlin LLC*
John Guerriero, *National Governors Association*
Justin Herring, *New York Department of Financial Services (NYDFS)*
Adrian McCabe, *Palo Alto Networks*
Sam Rubin, *Palo Alto Networks*
Sean Morgan, *Palo Alto Networks*
Bob Rudis, *Rapid7*
Scott King, *Rapid7*
Tod Beardsley, *Rapid7*
Allan Liska, *Recorded Future*
Katie Nickels, *Red Canary*
Adam Flatley, *Redacted*
Davis Hake, *Resilience*
Michael Convertino, *Resilience*
Chris Lynam, *Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)*
Jeff Bonvie, *Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)*
Kevin Gronberg, *SecurityScorecard*
Richard Perlotto, *The Shadowserver Foundation*
Beau Woods, *Stratigos Security*
James Shank, *Team Cymru*
Michael Garcia, *Third Way*

RANSOMWARE TASK FORCE

RANSOMWARE TASK FORCE Membersh

Ciaran Martin, *University of Oxford Blavatnik School of Government*
Eleanor Fairford, *U.K. National Cyber Security Centre (NCSC)*
U.K. National Crime Agency (NCA)
Bridgette Walsh, *U.S. Cybersecurity and Infrastructure Security Agency (CISA)*
U.S. Federal Bureau of Investigation (FBI)
Jonah Hill, *U.S. Secret Service (USSS)*
Bobby Chesney, *U.T. Austin Strauss Center*

RANSOMWARE TASK FORCE

RANSOMWARE TASK FORCE Staff

Sarah Powazek, *RTF Program Manager, IST*
Alexander Riabov, *Communications Manager, IST*
Leah Walker, *Future Digital Security Leader Fellow, IST*
Chuck Kapelke, *Writing Support*
Kathryn Pledger, *Pledger Designs*
Emma Hollingsworth, *Global Cyber Alliance*

RANSOMWARE TASK FORCE

QUESTIONS

RANSOMWARE TASK FORCE

Legislative opportunities

Action 2.1.1. Develop new levers for voluntary sharing of cryptocurrency payment indicators
Action 2.1.2. Require cryptocurrency exchanges, crypto kiosks, and over -the-counter (OTC) trading “desks” to comply with existing laws
Action 2.2.3: Clarify lawful defensive measures that private -sector actors can take when countering ransomware
Action 3.3.1: Update cyber-hygiene regulations and standards
Action 3.3.2: Require local governments to adopt limited baseline security measures
Action 3.3.3: Require managed service providers to adopt and provide baseline security measures
Action 3.4.2: Expand Homeland Security Preparedness grants to encompass cybersecurity threats
Action 3.4.3: Offer local government/SLTTs/critical NGOs conditional access to grant funding for compliance with the Ransomware Framework (2.1.1)
Action 3.4.4: Alleviate fines for critical infrastructure entities that align with the Ransomware Framework
Action 3.4.5: Investigate tax breaks as an incentive for organizations to adopt secure IT services
Action 4.1.1: Create ransomware emergency response authorities
Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments (incentivize non -payment of ransoms)
Action 4.1.3: Increase government resources available to help the private sector respond to ransomware attacks
Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment
Action 4.3.2: Require organizations to review alternatives before making payments
~~Action 4.3.3: Require organizations to conduct a cost -benefit assessment prior to making a ransom payment~~

RANSOMWARE TASK FORCE