



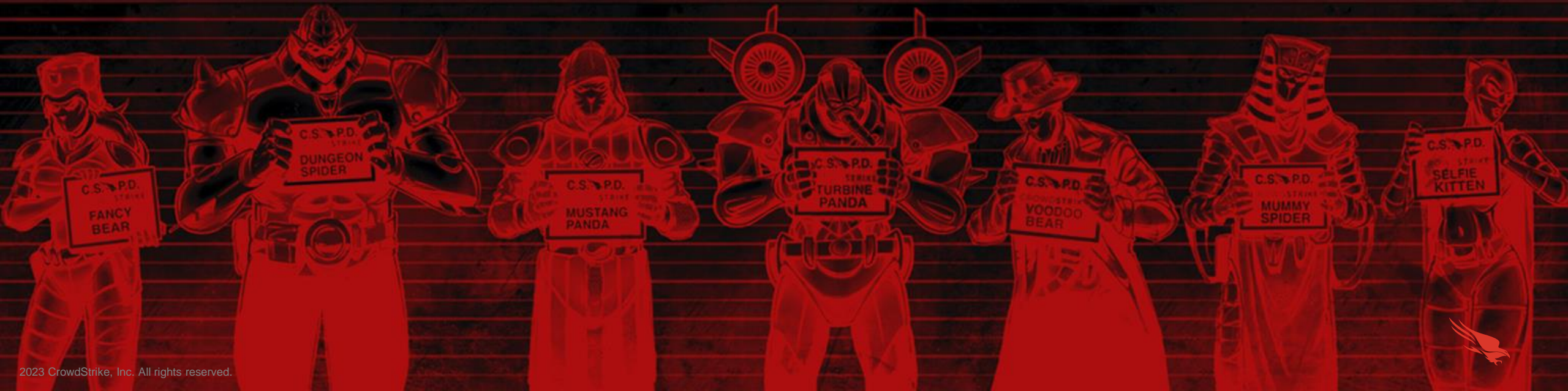
Threats to Local Governments and the Way Forward

Debbi Blyth

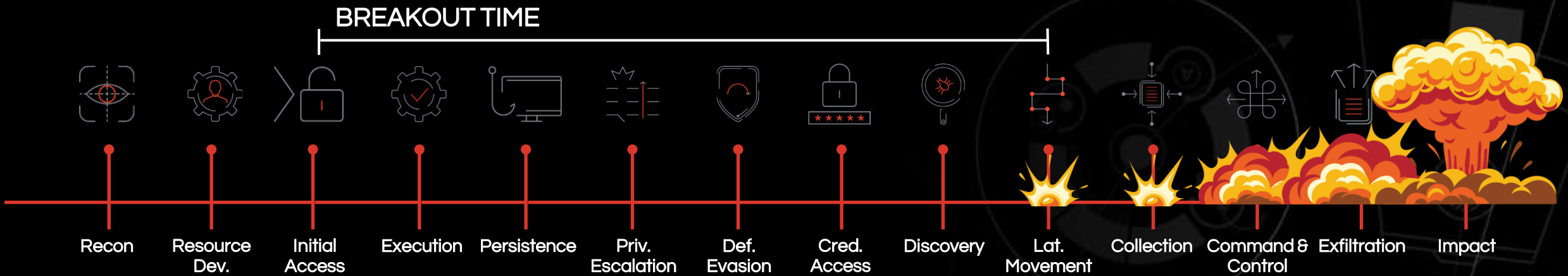
Former CISO for the state of Colorado
Executive Strategist with CrowdStrike

AGENDA

- ATTACK TRENDS
- CHALLENGES COMMON TO LOCAL GOVERNMENTS
- THE WAY FORWARD



Speed: Criminal Breakout Time



MITRE ATT&CK PHASE



Attack Trends

SPEED



**The Adversary
is Faster!**

COMPLEXITY



**Signatures
Don't Work!**

THE SHORTCUT



**Stolen
Credentials**



Speed: Evolution of Criminal Breakout Time



9H 42M

eCriminal Breakout Time in 2018



1H 38M

eCriminal Breakout Time in 2021



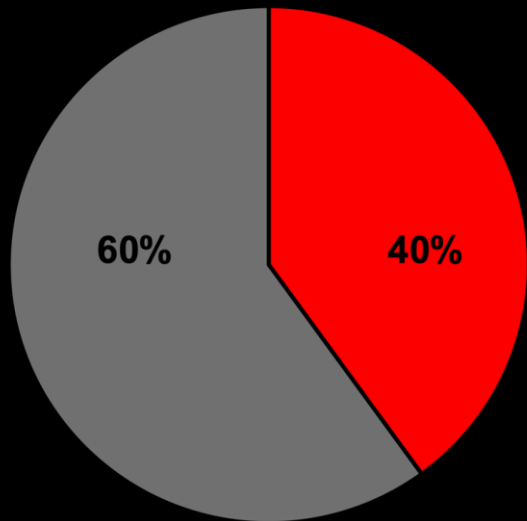
1H 24M

eCriminal Breakout Time in 2022

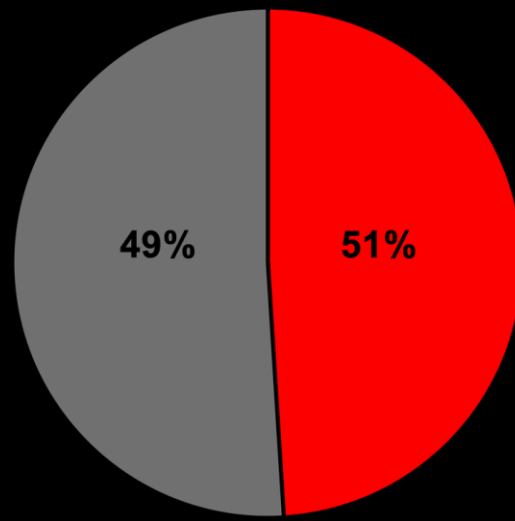
<https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/>



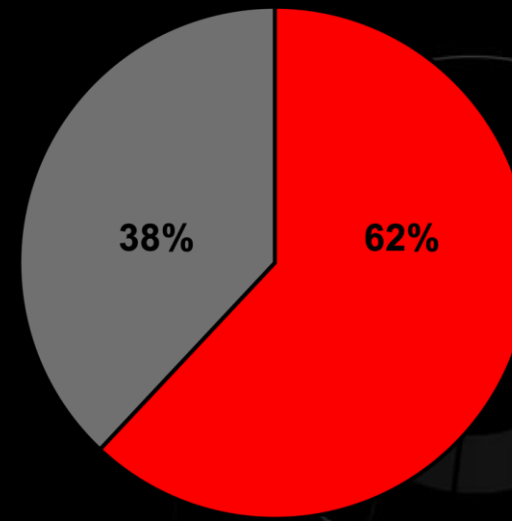
Complexity: Malware versus Malware-Free Attacks



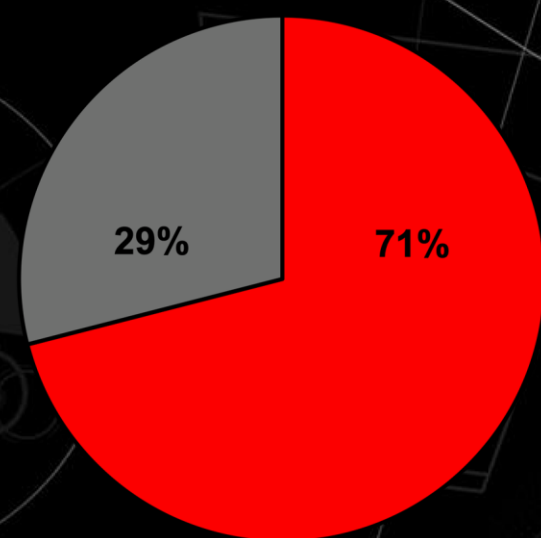
Malware vs. Malware-Free Attacks in 2019



Malware vs. Malware-Free Attacks in 2020



Malware vs. Malware-Free Attacks in 2021



Malware vs. Malware-Free Attacks in 2022

Malware 

Malware-Free 

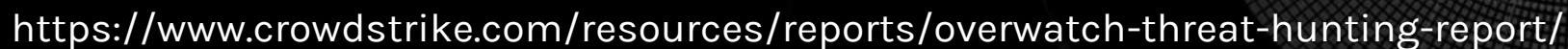
<https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/>



MALWARE
29%

YOU NEED COMPLETE BREACH PREVENTION

MALWARE-FREE
71%



DBIR

Data Breach Investigations Report

2008

2022

The Shortcut: Stolen Credentials

Compromised Credentials is the Most Common Cause of a Data Breach

80% of breaches of internet-facing systems due to stolen credentials

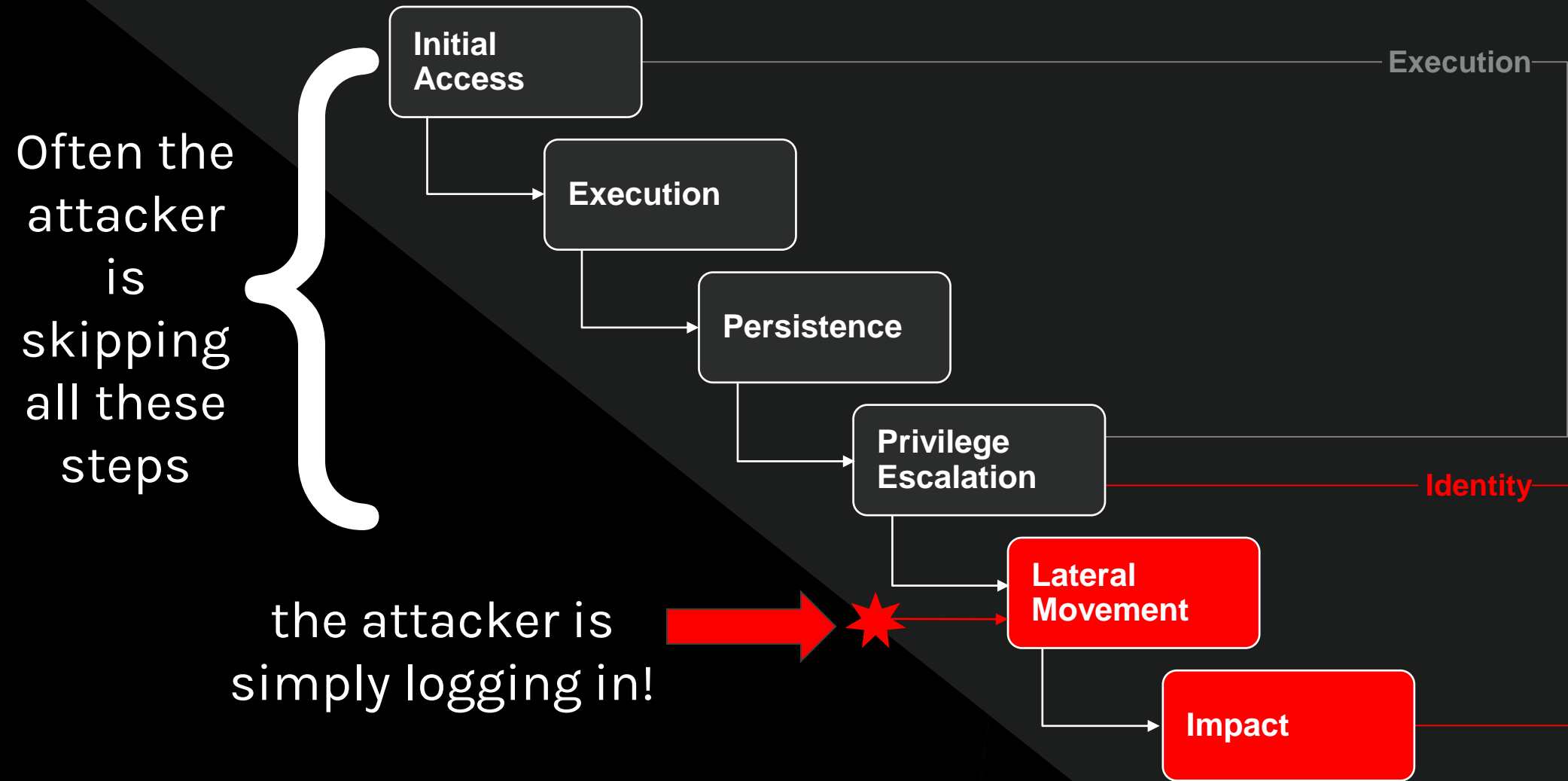
~30% Increase in Stolen Credentials since 2017

2022 Data Breach Investigations Report

<https://www.verizon.com/business/resources/reports/dbir/>



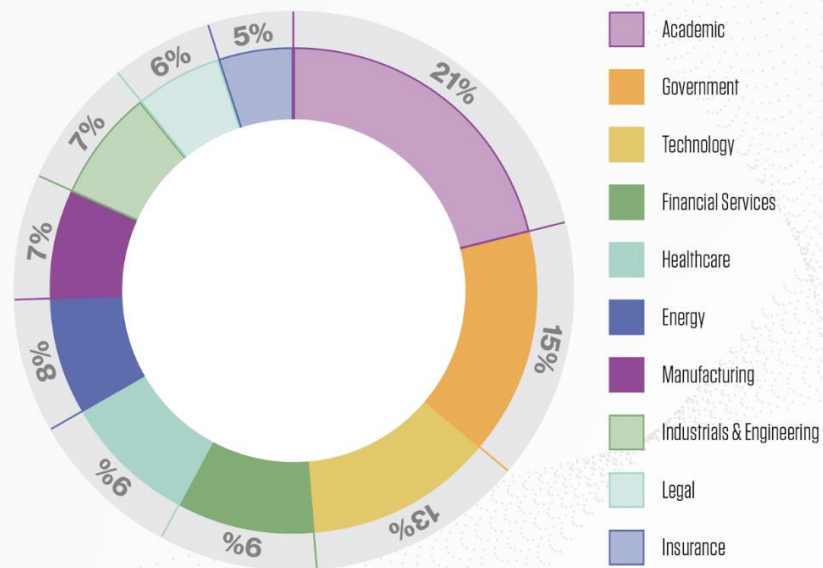
The Shortcut: Stolen Credentials



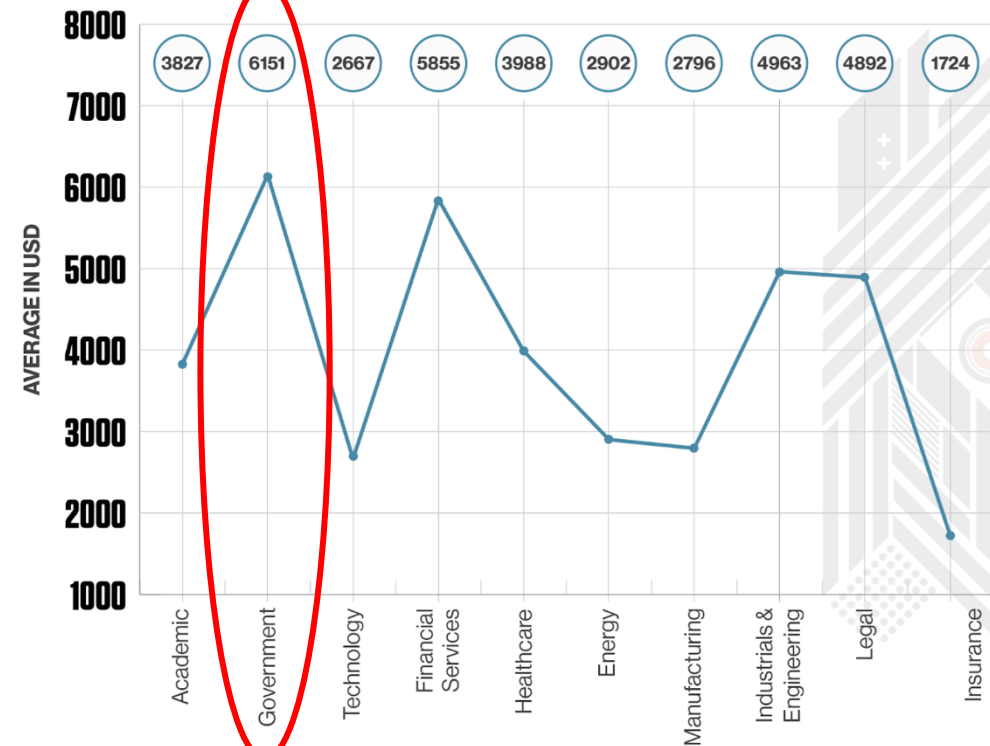


The Shortcut: Stolen Credentials

Top 10 Targeted Sectors



Average Asking Price for Top 10 Targeted Sectors



<https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/>



Challenges Faced by Local Governments



Local Government Challenges: Ransomware and Data Extortion



82% increase in ransomware
related data leaks in 2021

reported by CrowdStrike 2022

Top Government Targets:

Academia
Local Governments

reported by the FBI 2022



Local Government Challenges: Difficulty Obtaining Cyber Liability Insurance

In 2020 Cyber Liability Insurance Companies Lost Money



Many Are Denied
Coverage



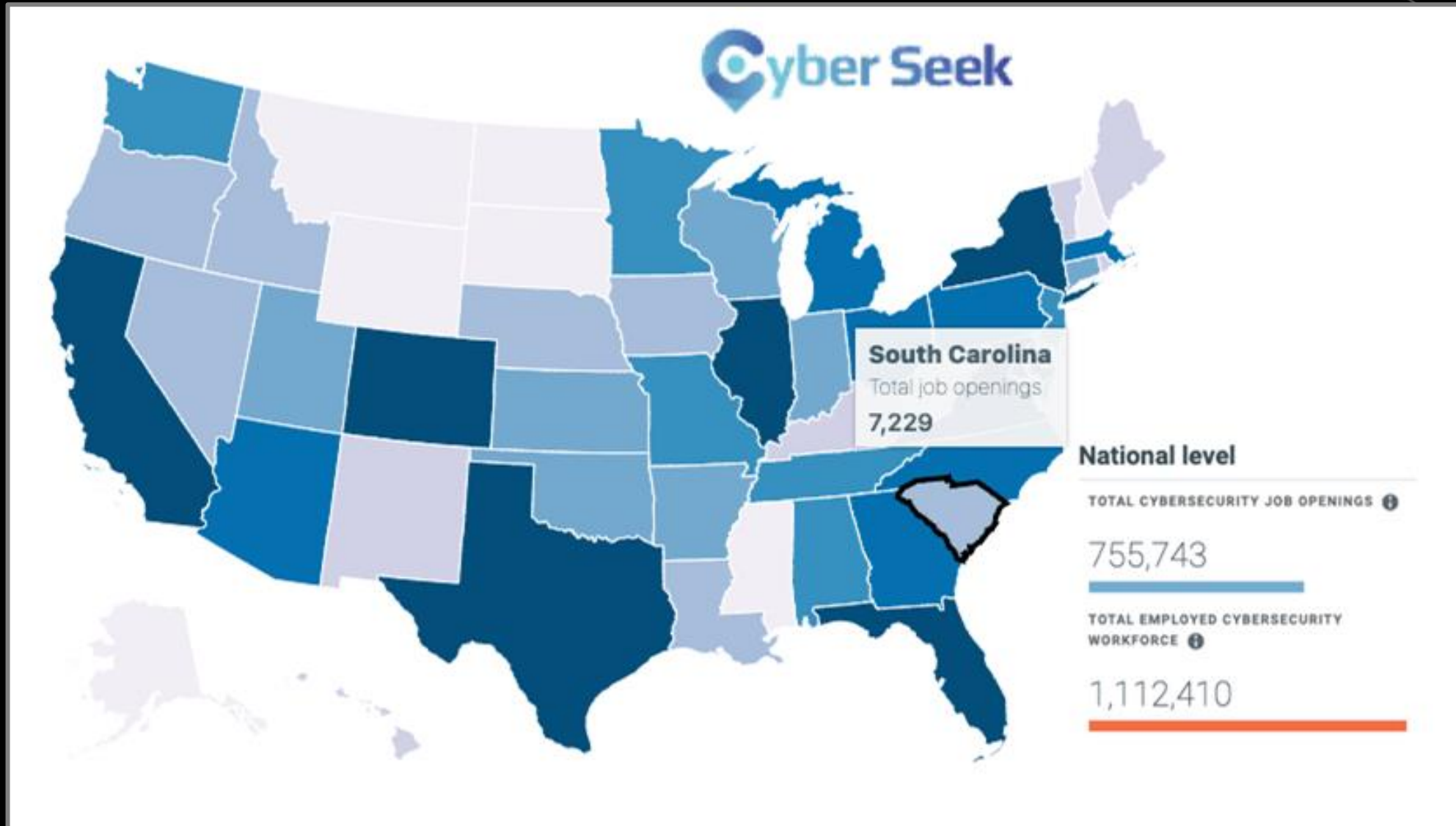
Premiums Went
Up



Key Security Controls
are Validated



Local Government Challenges: Cybersecurity Workforce Shortage

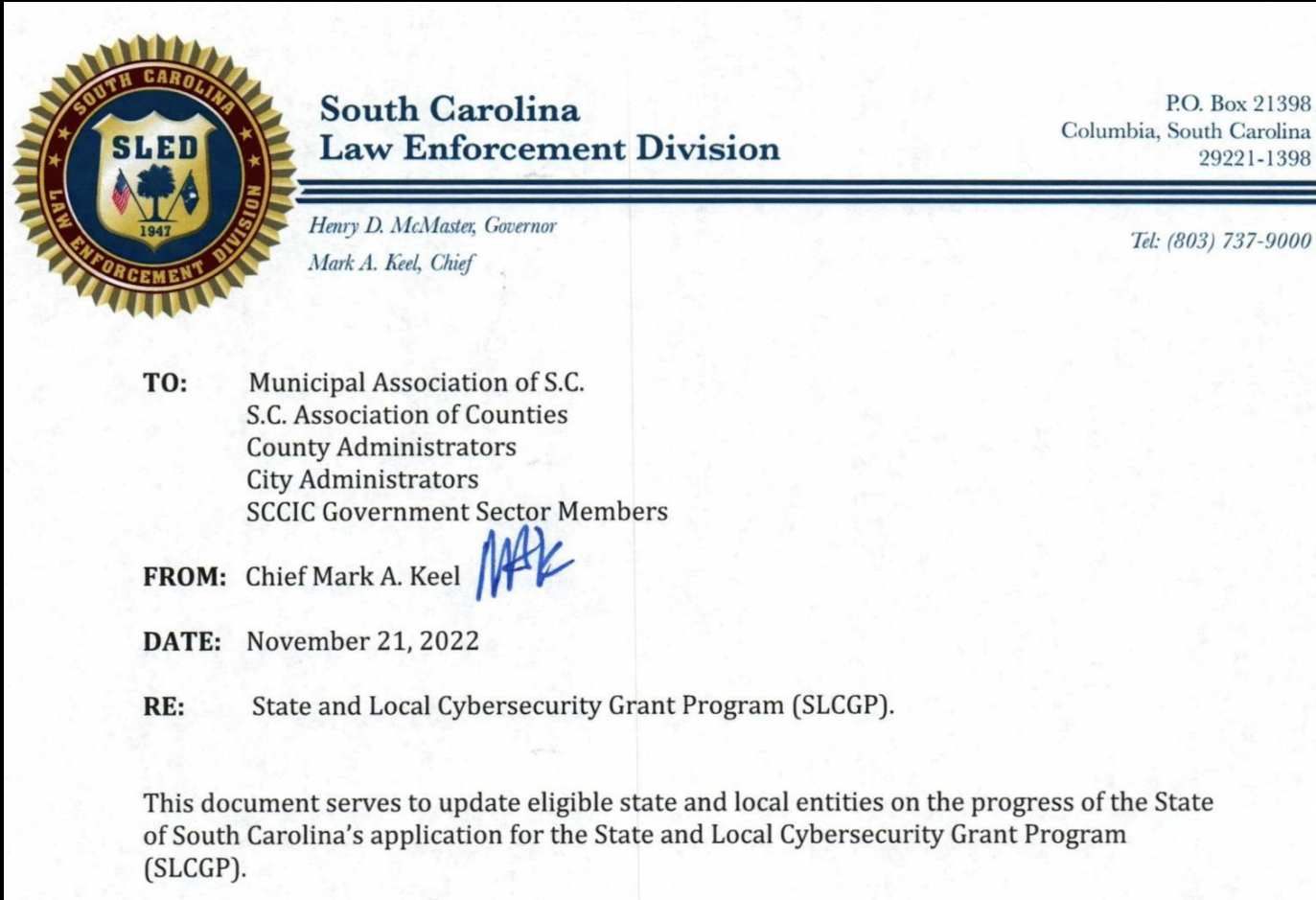


The Way Forward

- Funding / Partnerships
- Ransomware Prevention and Cyber Liability Insurance
- Solving the People Challenge



South Carolina: State and Local Cybersecurity Grant Program



Next Steps:

- *Cybersecurity Planning Committee to write and submit the statewide Cybersecurity Plan - SLED deadline 2/28/2023*
- *Upon DHS plan approval SLED will send an application proposal package to all entities that have provided their contact information to SLED (rconnell@sled.sc.gov).*
- *Committee will review application packages, recommend and distribute grant funds.*

More Information: <https://www.sled.sc.gov/homeland#grants>



Whole of State Cybersecurity

NATIONAL
ASSOCIATION
of COUNTIES **NACo**

IN WHOLE-OF-STATE CYBERSECURITY, COUNTIES ARE NOT ONLY ONE PIECE OF THE PIE

DECEMBER 12, 2022, 1:00 P.M. TO 2:00 P.M.



Whole-of-State Cybersecurity Gains Ground in Government

Governments are embracing a larger role in collective cybersecurity, creating cross-jurisdictional partnerships to make states, cities and counties more secure.

October/November 2021 • Adam Stone



2022 National Summit On State Cybersecurity

Jun. 28, 2022

North Carolina provided a case study of its whole-of-state approach and explained the efficacy of confronting the cyber threat in coordination with state and local agencies, the critical infrastructure sector, private companies, academic partners, hospitals, and other key stakeholders.



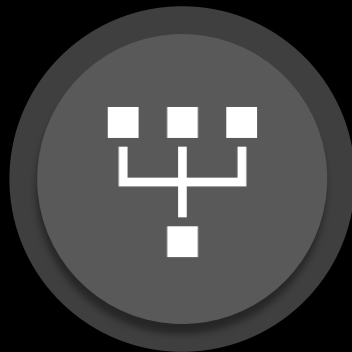
Ransomware & Learning From Others



State of Colorado: Ransomware Impact Reduction



System
Backups
Assured CDOT
Recovery



Network
Segmentation
Prevented
Spreading



Incident
Response Plan
and
Partners



Tools and
Improvements
Already
Underway



State of Colorado: Security Controls Implemented



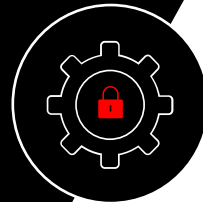
Reducing Privileged Access



Two-Factor Authentication Deployed



Security Tools Standardization



Security Policies Tightened Across the State



CrowdStrike Endpoint Detection and Response (EDR) Fully Deployed Across all Agencies



Ransomware Prevention and Learning from Prior Incidents



CULTURE OF CYBERSECURITY

Community awareness and practice are key to healthy cybersecurity; Engage your execs & board in a risk-based cyber program



ROLL IT OUT, TURN IT ON

Secure all of your tech infrastructure; Enable prevention capabilities, properly integrate



BE VIGILANT & READY TO ACT

Beyond technology, match defenders and adversaries 24x7x365, leveraging 1-10-60 rule



PROTECT YOUR IDENTITY

Use multi-factor for all accounts, protect service and admin accounts, adopt zero trust approach



CONTROL REMOTE ACCESS

Refrain from exposing SMB and RDP ports to the internet, restrict remote access tools



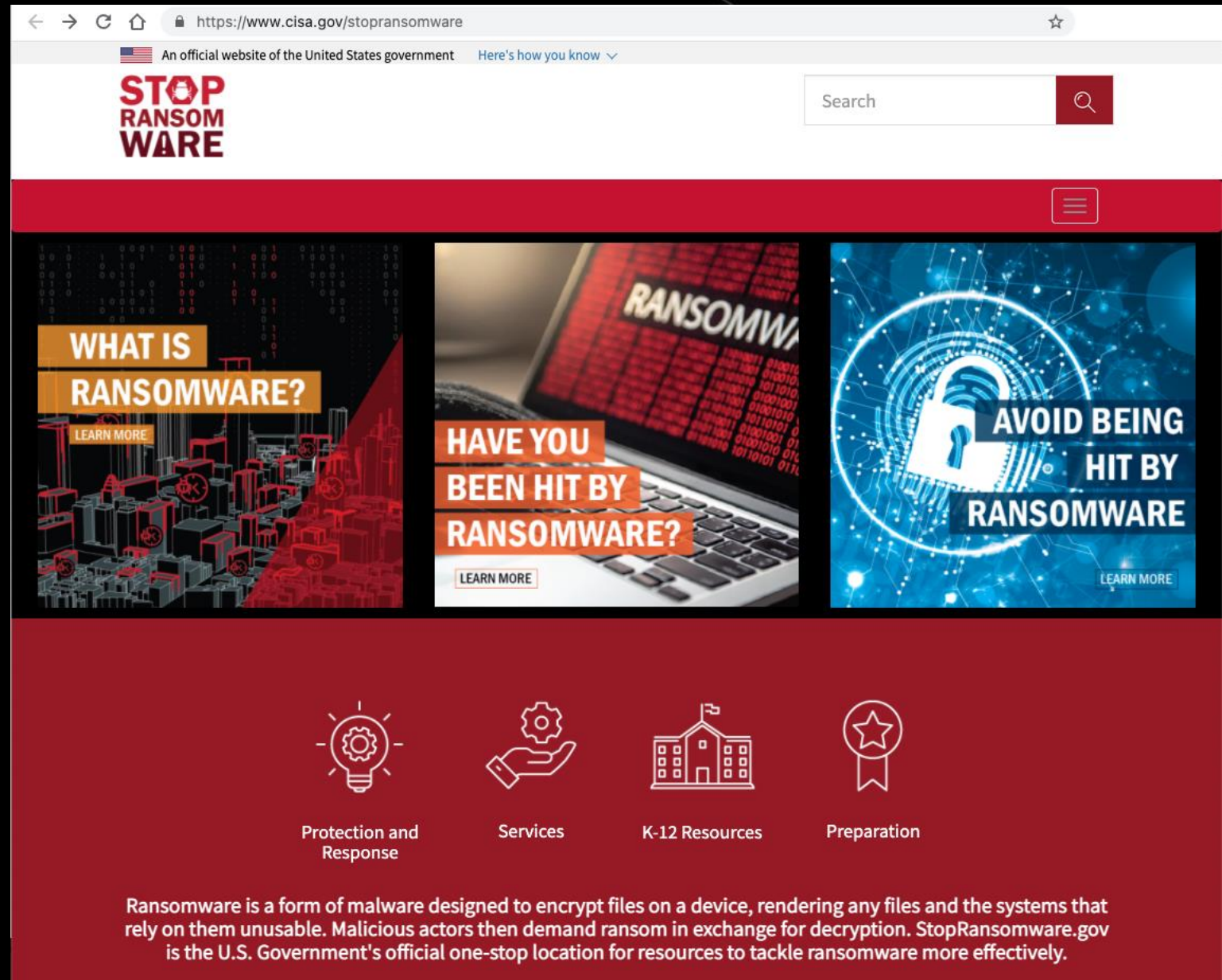
PRACTICE GOOD HYGIENE

Control software, eliminating unneeded software, keep up-to-date with latest patches



CISA Ransomware Recommendations

cisa.gov/stopransomware



The screenshot shows the CISA Stop Ransomware website. The browser address bar displays <https://www.cisa.gov/stopransomware>. The page features a white header with the CISA logo, the text "An official website of the United States government", and a search bar. Below the header is a red navigation bar with a menu icon. The main content area is divided into three columns, each with a large graphic and a "LEARN MORE" button. The first column is titled "WHAT IS RANSOMWARE?" and features a graphic of a city skyline with red ransomware icons. The second column is titled "HAVE YOU BEEN HIT BY RANSOMWARE?" and features a graphic of a laptop screen displaying the word "RANSOMWARE". The third column is titled "AVOID BEING HIT BY RANSOMWARE" and features a graphic of a blue padlock with a keyhole. Below these columns is a red footer with four icons and their corresponding labels: a lightbulb for "Protection and Response", a hand holding a gear for "Services", a building for "K-12 Resources", and a star for "Preparation". At the bottom of the page, a paragraph explains that ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. It states that malicious actors then demand ransom in exchange for decryption and that StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

← → ↻ 🏠 🔒 <https://www.cisa.gov/stopransomware> ☆

🇺🇸 An official website of the United States government [Here's how you know](#) ▾

**STOP
RANSOM
WARE**

Search 🔍

☰

**WHAT IS
RANSOMWARE?**
[LEARN MORE](#)

**HAVE YOU
BEEN HIT BY
RANSOMWARE?**
[LEARN MORE](#)

**AVOID BEING
HIT BY
RANSOMWARE**
[LEARN MORE](#)

💡
Protection and
Response

🔧
Services

🏢
K-12 Resources

🌟
Preparation

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.



Attaining Cyber Liability Insurance

Top cybersecurity controls are the key to risk mitigation, resilience, and insurability



Multifactor authentication (MFA) for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected



Vendor/digital supply chain risk management



Overcoming the People Challenge

Consider
Strategic
Partnerships
for necessary
expertise



Upgrade your security technology
AI / ML / Human Expertise
Cloud-based



Consider non-
traditional
Internships to find
the right fit



Thank you!

