VERITAS

6 WAYS RANSOMWARE CAN HURT YOUR PUBLIC SECTOR ORGANIZATION—

AND HOW TO COMBAT THE THREAT

Start now

ARE YOU RANSOMWARE READY?

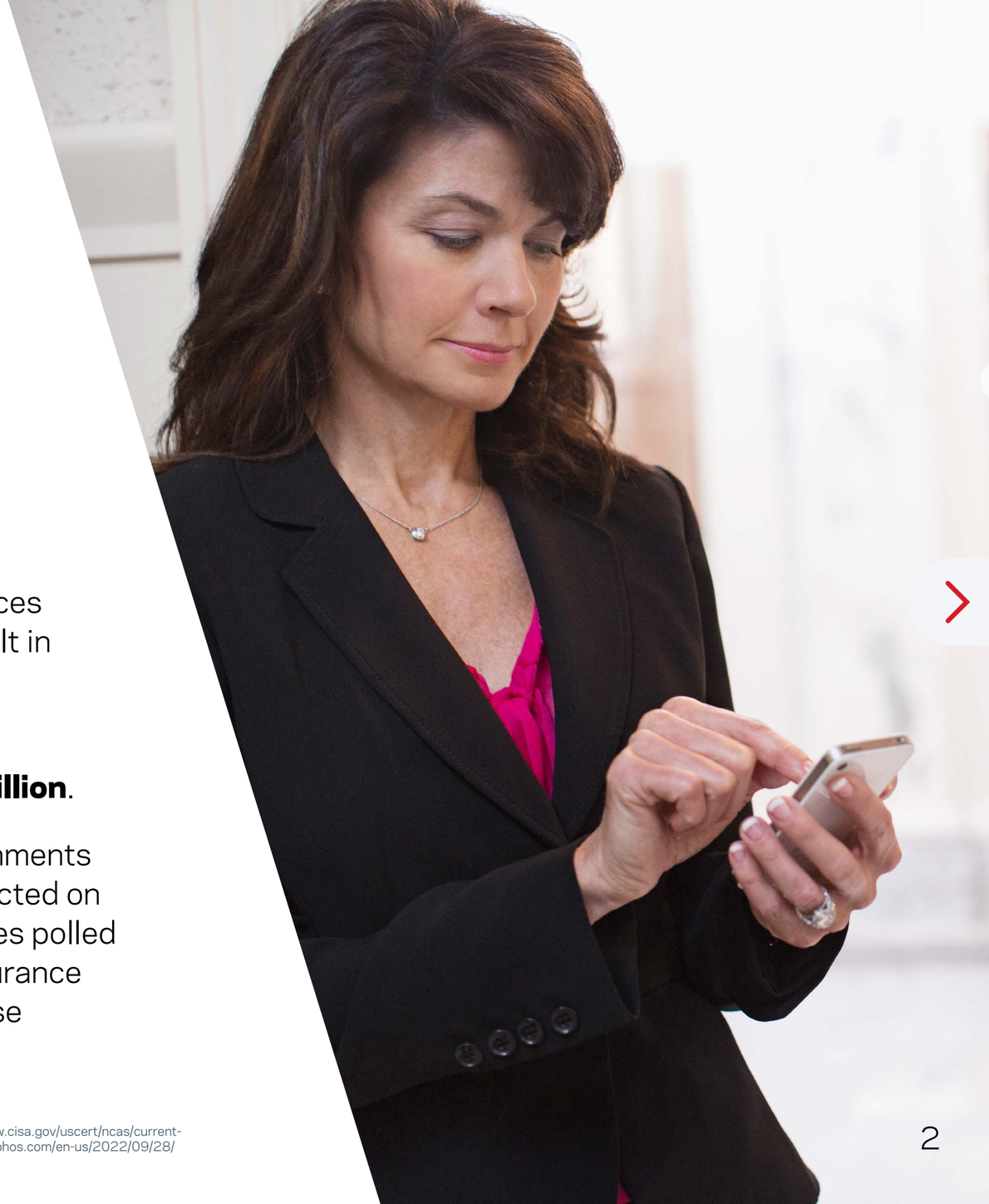
$590 million in ransomware-related payments were reported to US authorities in the first half of 2021 alone.[i]

More than **2,300** state and local governments and academia in the U.S. were compromised by ransomware in 2021.[ii]

In March 2022, the Federal Bureau of Investigation (FBI) issued an alert, warning that local government agencies are attractive targets for cybercriminals to hit with ransomware, because they oversee critical services on which the public depends.[iii] The FBI advised that these attacks can result in disrupted operational services, risks to public safety and financial losses.

Cumulatively, **246** ransomware attacks struck U.S. federal government organizations between 2019 and 2021 at an estimated cost of **$52.88 billion**.

A little more than half of the data is typically restored by state/local governments after paying ransomware, and **82%** of state/local governments were impacted on their ability to operate. It is important to note **43%** of state/local employees polled said fewer insurance providers are offering cyber insurance. So, fewer insurance options and increased cyber attacks could be the recipe for disaster if these organizations are not properly prepared.[iv]



[i] https://home.treasury.gov/news/press-releases/jy0471 [ii] https://www.msspalert.com/cybersecurity-research/us-local-governments-schools-healthcare-stats/ [iii] https://www.cisa.gov/uscert/ncas/current-activity/2022/03/31/fbi-releases-pin-ransomware-straining-local-governments-and-public [iv] The State of Ransomware in State and Local Government 2022: https://news.sophos.com/en-us/2022/09/28/the-state-of-ransomware-in-state-and-local-government-2022/

Overall, ransomware attacks were aimed at **14** out of **16** U.S. critical infrastructure sectors in 2021.[v]

U.S. public sector entities continued to suffer significant attacks on a frequent basis.

June 2022 alone saw exponential increases in reported ransomware attacks across public service organizations to include transit authorities, municipal governments, K-12, and higher education.[vi]

So, it's time to ask yourself the question:

ARE YOU REALLY PREPARED FOR A RANSOMWARE ATTACK?

BECAUSE IF YOU HAVEN'T BEEN A VICTIM YET...

THE ODDS SUGGEST YOU WILL BE —VERY SOON.

[v] https://www.securityweek.com/ransomware-targeted-14-16-us-critical-infrastructure-sectors-2021
[vi] https://www.techtarget.com/searchsecurity/news/252522479/Public-sector-still-facing-ransomware-attacks-amid-decline

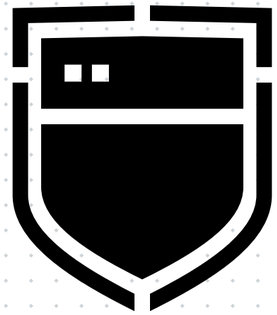
THE RISE OF RANSOMWARE

The rise of Ransomware-as-a-Service (RaaS) has changed the game. Savvy, sophisticated, and funded by wealthy backers, modern cybercriminals are tightly networked and share code and best practices. Many are highly profitable businesses and operate as such.

Ransomware attacks can happen to ANYONE but public sector entities represent a particularly lucrative target for cybercriminals. Hackers know that these organizations have much to lose if their systems go offline or if their data is compromised. Victims are in a position where they are almost forced to pay ransom fees. If they refuse, they face the criticism and suffering of their constituents, whose data and even livelihoods may be at risk of compromise.

Without doubt, growing attack surfaces, outdated technologies and inadequate defenses mean that public sector agencies are increasingly being perceived as easy targets for cybercriminals.[vii]

Organizations need to prioritize cybersecurity hygiene and implement best practices immediately. This is where Veritas comes in.



THE RISE OF RAAS

Ransomware as a Service (RaaS) is a subscription-based turnkey model that enables affiliates to use pre-existing tools to automate attacks and wreak havoc.

Affiliates earn a percentage of each successful ransom payment. Just like a SaaS solution, RaaS users don't need to be skilled or even experienced, which allows even the most novice hackers to execute highly sophisticated cyberattacks.

[vii] https://www2.deloitte.com/content/dam/insights/us/articles/6421_Ransoming-government/DI_Ransoming-government.pdf

THE REAL COST OF RANSOMWARE

Rather than assume you MIGHT get hit by cybercriminals one day, work on the basis they've infiltrated your systems ALREADY.

Historically, this is how they operate, laying low, hiding, observing your vulnerabilities, waiting for the right time to strike. This process can take many months. When they do finally launch an offensive, the impact can take many different forms.

Even the weakest ransomware can result in costly downtime, diminished trust, reputation damage, and setbacks from destroyed or compromised data and systems. In the public sector, this can translate into severe damage to critical infrastructure and networks that impact the lives of thousands or even millions of people.

The price of compromised public data

The increasing digitalization of critical infrastructure and public records has rendered many public sector organizations more exposed than ever before. And the cost of poor cybersecurity is steep.

Click on the numbers to find out more.

1 2 3 4 5 6

LOSS OF CITIZEN OR PATIENT DATA:

Data is the lifeblood of every public sector and healthcare entity. Temporary loss of citizen or patient data is bad. Permanent loss is a disaster.

The loss of Personal Identifiable Information (PII) is commonplace. Medical records, passport details, national insurance numbers, social security information and other personal details can be 'taken hostage', with the threat of public release.

THE IMPACT:

In May 2021, a PayOrGrief ransomware attack infected local U.S. county government systems, making servers inaccessible and disrupting online services, including the ability to book COVID-19 vaccination appointments.

The attackers claimed to have stolen 2.5GB of data containing internal documents and personal information.[viii]

[viii] https://duo.com/decipher/local-government-ransomware-attacks-disrupt-public-services#d-nav-drawer [ix] https://www.computerweekly.com/news/252498029/Average-ransomware-cost-triples-says-report [x] https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/ [xi] https://medium.com/@SeedSpark/whats-the-real-cost-of-a-ransomware-attack-in-2021-ce4df5c30dfd [xii] https://www.zdnet.com/article/fbi-ransomware-attacks-are-piling-up-the-pressure-on-public-services/ [xiii] https://www.techtarget.com/searchsecurity/news/252508453/Gartner-analysts-debate-ransomware-payments

COMBAT THE THREAT WITH VERITAS

The rapid rise of ransomware suggests now is the time to create a truly resilient government. How? With a unified, multi-layered cybersecurity strategy built on three pillars:

PROTECT
BY SAFEGUARDING

DETECT
THREATS

RECOVER
AT SPEED

PROTECT BY SAFEGUARDING

Cybercriminals have exploited the ‘trust perimeter’ for years. But the explosion of ransomware attacks has generated an immediate need for even more robust cybersecurity across the public sector.

The first step in any ransomware resiliency plan is to ensure your most critical, most important assets—your data and your IT infrastructure—are protected.

Every part of your IT environment, be it physical, virtual, cloud, or containers must be backed up to immutable storage.

Proactive protection takes many forms:

- **A reduction** in attack surface through system hardening and segmentation.
- **Adoption** of zero trust via role-based access controls (RBAC) and multi-factor authentication (MFA).
- **Encrypted** data both in-transit and at rest.
- **No single points** of failure through replicated data, so indelible and immutable copies are available in the worst-case scenario.

Adopting a **‘trust nothing, verify everything’** position puts users in a position of strength.

DETECT THREATS

Ransomware is smart. It hides in the dark corners of IT environments, where security and oversight are slight or even non-existent.

Protect your disparate systems with total visibility; the ability to view each and every system, and cross reference them to ensure no part of the environment is unprotected. Rest easy knowing your environment is clean, safe and secure.

AI-driven anomaly detection for both data and users—featuring automated, on-demand malware scanning—provides a chance to act before cybercriminals get to work with their malicious code. And advanced scanning functionality ensures restored data is clean and uncompromised.

Detect anomalies and malware with Veritas.

RECOVER AT SPEED

Cyberattacks come in many forms; they're rarely a one-size-fits-all affair. In today's ever-evolving threat landscape, it's vital to set up an optimized strategy extending beyond restore points and single backup copies.

A flexible solution with a range of recovery options—like secondary data centers and data centers in the cloud on demand—fits the bill.

True resiliency requires flexible, hybrid and rapid recovery.

Click on the numbers to find out more.

1 2 3

AUTOMATION IS AT THE HEART OF AN EFFECTIVE RECOVERY STRATEGY

The coordination of disparate teams such as network, storage and security MUST be done in advance so when a ransomware attack does hit, the recovery plan is simple and clear. All aspects of recovery can be abstracted into a Virtual Business Service (VBS). This provides one-click automatic recovery as well as a means to visualize and re-shape the recovery plan as required. Crucially, it allows for sandbox testing.

Now **not only** will you have a plan, but the proof it will work when it comes to the crunch.

WHAT'S YOUR NEXT STEP?

The threat of ransomware is frightening and attacks will continue against public sector organizations. We're seeing more bad actors and more attacks. To reiterate, your systems are most likely the home of an unwelcome host already.

But that doesn't mean you're helpless. Far from it.

Adopt the following best practices today. Create a multi-layered, flexible, unified defense strategy designed to give your organization the resilience it needs to thrive.

Click on the numbers to find out more.

1 2 3 4 5

PROMPTLY UPDATE AND UPGRADE

Attackers seek out security vulnerabilities in end-of-life software. Minimize your attack surface by patching and upgrading all infrastructure, operating systems and software applications regularly.

GET READY FOR CYBER RESILIENCY

Ransomware attacks are becoming more sophisticated by the day. Public sector entities are feeling exposed, with highly sensitive citizen data widely distributed across physical, virtual, and cloud environments. Veritas provides a unified platform approach designed to extend beyond data protection, delivering multi-layered, proactive solutions that ensure cyber resiliency.

Find out more about how we can keep your public sector organization safe—by visiting:

veritas.com/solution/government

Alternatively, speak to an agent and call **1 (866) 837-4827** today.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc

veritas.com

VERITAS™