VERITAS | Hitachi Vantara

SOLUTION BRIEF

Optimize Your Cyber Resiliency.

Improve your security posture with Veritas and Hitachi Vantara.

Ransomware Risk and Rising Costs

As cyber threats continue to rise, individuals in state and local government as well as education are facing an expanding landscape of cybersecurity challenges. It's crucial to recognize that these threats affect not only businesses but every organization within the public sector. According to Deloitte's predictions, over the next decade, the financial toll of ransomware attacks is estimated to exceed $265 billion.[1]

Veritas and Hitachi Vantara, together, combine their proven, best in class technologies to create cyber resilient data protection solutions for public sector organizations who need protection both on premise and in the cloud.

Highlighting the severity of the issue, research conducted by Barracuda Networks in 2020 revealed that 44 percent of global ransomware attacks were directed at municipalities. This alarming statistic underscores the significant concerns surrounding cybersecurity in the public sector. State and local governments, as well as educational institutions, now find themselves grappling with the daunting task of defending against cyber threats as well as strategizing on resilience and site continuity.

The magnitude of this problem became so apparent that in 2021, the Biden administration took action by recognizing ransomware as a shared global threat. This recognition led to the issuance of Executive Order 14028, which aimed to enhance the nation's cybersecurity efforts, emphasizing the need for collaboration between government entities and the private sector.

265B

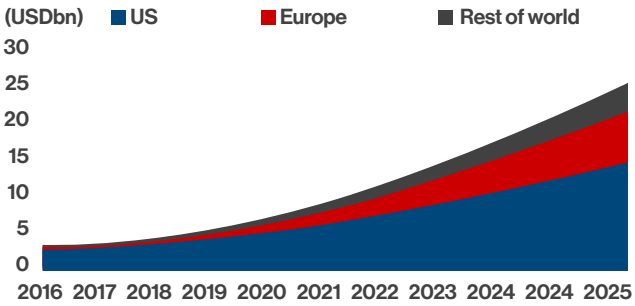
The cost of ransomware attacks over the next 10 years.[1]

Given that no organization is immune to these cyber threats, the risk has escalated to such an extent that ransomware has emerged as a new challenge for the public sector. Consequently, managing these risks and the associated costs has become a paramount consideration for leaders in the public sector, including those in state and local government and education.

FitchRatings

Global Cyber Insurance Premiums

2016-2025



Source: Fitch Ratings, Howden, MunichRe, EIOPA

Figure 1. A recent report by Fitch Ratings illustrates the staggering increase in cyber insurance premiums year-over-year

Reality Check

In Verizon's 2022 Data Breach Investigations Report, ransomware incidents increased nearly 13 percent between 2021 and 2023[2] – that's bigger than the past five years combined. And the Sophos State of Ransomware in State and Local Government 2022 report found that 58 percent of state and local government organizations were hit by ransomware in 2021[3], up from 34 percent in 2020 – an increase of more than 70 percent over the course of a year. Part of this increase comes from more digital services being offered to citizens, which are expected in this digital age. But with more online engagement comes more risk.

Attacks on local government entities are attractive because they are significant targets, affecting critical utilities, emergency services, educational facilities, and much more. Yet, local governments are far less successful in stopping attacks compared with other sectors[3]. The risks are high. State and local government agencies, as well as educational institutions, must take a proactive approach to get a reality check about the looming threat of ransomware. The consequences of falling victim to ransomware attacks can be devastating, both in terms of financial losses and the disruption of critical services.

Why State and Local Governments are Targeted

- Sheer number of different local governments in US (90,075)
- Holders of sensitive (valuable) information
- Inadequate cybersecurity
- Financial constraints
- Use of Internet of Things (IoT) technology

How State and Local Governments are Attacked

- Public sector especially vulnerable to phishing emails
  - 80 percent of attacks attempted to steal logins and passwords

Mitigating Risk

With the increasing value of personally identifiable information (PII) in today's digital infrastructure, it is incumbent upon every organization to find ways to reduce their exposure in the event of a successful cyberattack. And while state and local governments and education organizations acknowledge challenges when it comes to budget, resources, and training relating to risk management, these actions don't require large budgets, more technology, or hiring more staff. However, they do require a better understanding of how ransomware attacks occur and the best implementation policies that can drastically reduce the ability for cyber criminals to access valuable data.

After a data breach occurs, most organizations test and restore their systems. But it may not be enough. However, tearing down and rebuilding a working data system isn't always practical, as it's expensive, time consuming, and potentially risky.

Assessing data systems for gaps and vulnerabilities is a strategic way to evaluate system security and future cyber readiness. Organizations don't have to tear down to rebuild because there are key tools at their disposal that can go a long way in mitigating their risk. Veritas and Hitachi Vantara support the public sector by strengthening their resiliency posture and providing strategic risk management to thwart attacks to align with Executive Order 14028.

MAINTAIN CONTROL | **ELIMINATE UNCERTAINTY** | **REDUCE RISK & COMPLEXITY**

Illuminate with Data Visibility

Complete Infrastructure and Data Visibility:
– Edge to Core to Cloud

Across All Major Data Protection Solutions

Protect All Data from All Sources

Reduce Attack Surface

20+ years Experience with Security Engineered into Products

Gartner Leadership with Veritas 17 Times

Implement Immutable and Indelible Storage and Air Gap

Immutability Your Way:
– BYO, Appliance, Cloud, and SaaS

Indelibility Using Zero Trust Principles

Built-In Air Gap Solutions

Industry's Only Tamper-Proof Immutability Timer

Adopt Anomalous Activity Detection and Malware Scanning

Near Real-Time AI-Based Anomaly Detection

Automated and On-Demand Malware Scanning

Recovery of Clean Data

Optimize for Flexible, Rapid, Hybrid Recovery at Scale

Flexible, Hybrid, Rapid Recovery:
– Any Size/Scale Failure
– Anywhere from Anywhere

Recovery from Object Level to Entire Data Center

Recovery Success Rate: 100%

Orchestrated Rehearsal and Recovery

Non-Disruptive, Cost-Effective Recovery Rehearsals

Tier "0" to Tier "N" Application Recovery with Varying RPO

How to Get the Most Out of Your Cyber Resiliency Tools

State and local government entities and education organizations can maximize the benefits of cyber-resilient tools by integrating them seamlessly into their cybersecurity strategy. To achieve this, it's essential to start with a thorough assessment of the organization's unique risks and vulnerabilities. Once identified, cyber-resilient tools should be strategically deployed to address these specific challenges.

Access Management

Attacks can be significantly reduced when a comprehensive access management process is in place that controls and manages who can do what in a system. This ensures that agencies can track and log all actions taken by users with Administrator credentials and editing rights, such as enterprise administrators, service accounts, domain administrators, global administrators, hybrid identity administrators, and privileged role administrators. Additionally, transparency and authentication measures for third parties or managed service providers (MSPs) accessing the network remotely significantly improves security.

Security

Security is top of mind for everyone and anyone responsible for managing and protecting data. Attacks and accidents can and do happen, which is why agencies need to take a holistic approach to security. Endpoint security and protection is one area that agencies should focus heavily on when seeking to understand how authentication occurs for employees and vendors, what security tools are used to protect emails and endpoints, and how network security is achieved when applications sit on-premises and in the cloud.

Software and Hardware Management

While not always top-of-mind for organizations, when there isn't a sound software and hardware management process in place, significant risks are present. Organizations need to be cognizant of what happens with their end-of-life/support for hardware and software. Are updates required? Does decommissioning need to occur? Does certain software need to be segregated from the rest of the network? This is important for end-of-life platforms as well as the servers and workstations running on them.

SOLUTION BRIEF

Cyber Resiliency powered by Veritas & Hitachi Vantara

Resiliency

Resiliency can be costly and complicated as it is the foundation for business continuity, and can serve as a guide to improve an organization's overall data and cloud management strategy. Important questions that state, local, and education organizations should ask themselves are:

- How often is critical information being backed up?
- Where are the backups stored?
- Is the backed up information quickly accessible?
- What data is being backed up?
- Does the organization have a business continuity plan?
- Does the organization have recovery time objectives (RTO) in place?
- How often does the organization perform disaster recovery drills?
- Is the organization able to test the integrity of backups prior to restoration to be confident that they are free from malware?

Benefits

Veritas and Hitachi Vantara offer solutions to protect valuable data; ensure anytime, anywhere access; and to recover quickly in event of a disaster. At the same time, these solutions provide the insight to transform data into valuable information and shape it into an integral, cost-effective source of business intelligence.

About Hitachi Vantara

Hitachi Vantara, a wholly-owned subsidiary of Hitachi Ltd., delivers the intelligent data platforms, infrastructure systems, and digital expertise that supports more than 80% of the Fortune 100. To learn how Hitachi Vantara turns businesses from data-rich to data-driven through agile digital processes, products, and experiences, visit hitachivantara.com.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers – including 95 percent of the Fortune 100 – rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas is uniquely equipped to help state and local organizations of all sizes conquer the complexity of managing and protecting their business critical data. Our approach closes the gaps in your ransomware resiliency with a proven strategy aligned to the National Institute of Standards and Technology (NIST) framework. We also help you meet PII laws, meaningful use standards, and more – as well as give you a head start on meeting any future requirements. Additionally, our integrated product portfolio, unified data management experience, and proven track record of recovering nearly 100 percent of data after cyberattacks solidifies.

Veritas as an industry leader – from edge to core to cloud. Veritas is an industry member of the U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program and actively working with DHS to mitigate global cyber threats. Through this program, Veritas supports DHS's focus on enabling actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors. We are committed to preventing ransomware attacks across our 80,000 customers around the world. To that end, Veritas delivers the most comprehensive technology ecosystem you can find. It's trusted by many of the world's largest companies, including 95 percent of the Fortune 100. The Veritas unified Cloud Data Management Platform lets you take control of all your enterprise data and applications across any cloud, any environment at scale.

Our integrated approach to data management and protection is proven to deliver unmatched versatility, performance, and cost-savings. Now is the time to discover what we can do for your state, local or education organizations.

[1] Deloitte report: Defending against ransomware in an age of emerging technology
[2] Verizon 2022 Data Breach Investigations Report
[3] Sophos report: The State of Ransomware in State and Local Government 2022

Contact Us →

For more information and to learn how Veritas and Hitachi Vantara can help you transform your data, visit www.hitachivantara.com/veritas.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
GLOBAL: 1-858-547-4526
HitachiVantara.com/contact

HV-345Marketing-SP-HitachiVeritasCyberResiliency-07112023-A