Commvault

eBOOK

Three Ransomware Readiness Essentials for Education

The Education Blueprint to Cyber Resilient Data Protection

Commvault

Introduction

Ransomware is an unwelcome reality in the digital universe, impacting businesses and operations across private and public sectors. For educational institutions, ransomware and malicious attacks have doubled in two years.[1] Bad actors are exploiting institutions, with 80% of lower-education providers reporting being hit by ransomware in 2023 and 79% of higher-education providers reporting being hit.[2] Educational institutions must develop new cyber-resilient strategies to keep students, faculty, practitioners, and their data safe.

In this ebook, we'll uncover the growing threat of ransomware, the importance of cyber resilient data protection strategies for educational organizations, and best practices to mitigate the risk of data loss in the face of new and emerging threats.

Schools are targeted because of their data-rich environments.[3]

THE RAPID EVOLUTION OF RANSOMWARE

The rapid evolution of ransomware has not spared the education field, as cybercriminals increasingly employ artificial intelligence (AI) to carry out their malicious activities. This alarming trend poses a significant threat to educational institutions, students, and staff members.

AI-powered ransomware in education uses machine learning to find vulnerabilities in computer systems and networks, allowing cybercriminals to exploit them more effectively. This can result in the encryption of critical educational data, disruption of online learning platforms, and theft of sensitive information.

Recovery Costs[4]
Lower education $1.59M, Higher education $1.06M

Data encryption rates in education continue to increase, with 81% of attacks encrypting data in lower education and 73% in higher education.[5] Additionally, a significant number of organizations reported stolen encrypted data. To combat this threat, educational institutions must prioritize cybersecurity.

To combat this evolving threat, educational institutions must prioritize cybersecurity measures. Implementing robust security protocols, regularly updating software and systems, and educating staff and students about potential risks are essential steps in mitigating the impact of AI-powered ransomware attacks. By adopting AI and machine learning technologies for defense purposes, educational institutions can enhance their ability to detect and respond to ransomware attacks effectively.

1, 2. Sophos. The State of Ransomware in Education 2023.
3. Forbes, Frederick Hess, The Top Target For Ransomware? It's Now K-12 Schools, September 2023.
4, 5. Sophos. The State of Ransomware in Education 2023

THE GROWING IMPACT ON EDUCATION

The impact of ransomware-triggered shutdowns of educational facilities jeopardizes operational data, personal information, and drastically impacts the ability to administer learning. And for educational institutions handling sensitive research data or on government grants, a successful breach could put providers in jeopardy of violating compliance and regulation standards.

Accelerating cyberattacks. The education sector experienced a staggering surge in malware volume, with attacks against K-12 institutions skyrocketing by an astonishing 323%, while higher education institutions faced a comparatively modest increase of 26%.[6]

High payouts. Educational institutions are prime targets for ransomware attacks due to their data-rich environments, making them vulnerable to cybercriminals seeking to exploit valuable information. Alarmingly, 47% of lower education institutions and 56% of higher education institutions have resorted to paying the ransom[7] to retrieve their encrypted data, highlighting the significant financial impact and urgency faced by these organizations in recovering their critical information.

Costly downtimes. Disruptions of any kind are expensive and can impact organizations with stretched IT resources beyond their limits. Ransomware attacks shake the foundation of an institution, and raise doubts about its ability to protect its students, faculty members, and it's data. and their private data. On average, recovery costs, which include downtime, has a median average of $750K for lower education and $375K for higher education.[8]

Failure to comply. As a regulated industry, many schools receive government grants and support. Higher ed institutions may also receive research grants, and handle highly sensitive data. This introduces the potential failure to meet regulatory compliance requirements, causing costly, lengthy, and distracting audits.

Reputation damage. In the aftermath of a ransomware attack, a school's reputation can be irretrievably harmed, with communities, students, and government agencies questioning the providers ability to protect their own assets. Not only can this damage enrollment and future government grants.

ENHANCING CYBER RESILIENCE: COMMVAULT® CLOUD POWERED BY METALLIC® AI

Commvault Cloud powered by Metallic® AI is revolutionizing data management and protection for educational institutions. It provides a cyber resilience platform built to meet the demands of the hybrid enterprise at the lowest TCO. Commvault Cloud intelligently secures data to rapidly uncover risk, minimize cyberthreats, continuously control data and its access, and drive more informed recovery outcomes, wherever data lives.

SECURITY

Commvault Cloud secures all your hybrid workloads—combining the power of the market's most innovative capabilities and unique architecture with cloud simplicity for all your data.

Cyber Resilience across all hybrid workloads:

All Data: Commvault Cloud offers the broadest data security of more workloads than any other provider.

Secured everywhere: Commvault Cloud separates data security management from data location.

One Cloud: See, protect, and recovery all hybrid your workloads from a single platform.

6, 7, 8. Sophos. The State of Ransomware in Education 2023

INTELLIGENCE

Go beyond the backup to proactively stop ransomware in its tracks. Powered by Metallic AI, Commvault Cloud provides layered defense—minimizing the impact of cyberattacks.

Advanced AI, enabling next generation capabilities:

Detection: Commvault Cloud connects early warning to backup environments and uses intelligent cyber deception recommendations to minimize the blast radius of an attack and speed the time to detect threats.

Response: Commvault Cloud uses AI to power automated recovery validation and restore processes to speed response times. Accelerate incident response and forensics with rich backup metadata and history to ensure verification and compliance.

Recovery: Leverage AI-driven automation for any-to-any location recovery processing, giving you the industry's fastest recovery times, at massive scale, with the best TCO.

RECOVERY

With recovery predictability your data is always secure and available, wherever it lives, with powerful AI-driven automation to verify clean recovery points, and unparalleled scaling to recover data faster than the competition, at a fraction of the cost.

Your business, recovered with certainty, at scale:

Your business: Commvault Cloud ensures your business is up-and-running, without breaking the bank.

Certainly: Commvault Cloud connects immutable, indelible, and clean backups in the cloud to recovery, so you ensure predictable, reliable, and ransomware-free recovery.

At Scale: Leverage AI-driven cloud scaling techniques (even for on-prem recovery), and recover more data, faster.

Next steps

Get more value from your data and gain true cyber resilience without making compromises to your business. Visit https://www.commvault.com and **contact us** for more information.