



AN EDUCATOR'S GUIDE TO
Ransomware Protection
as a Service™



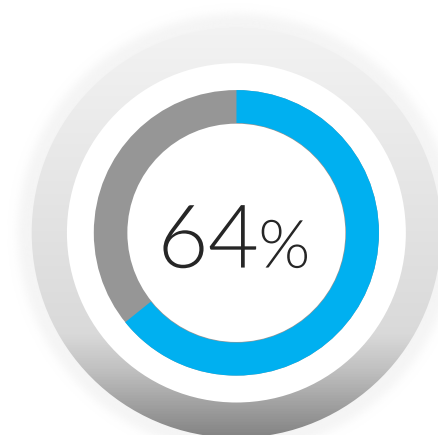
©2022 InterVision Systems, LLC. All rights reserved.

Ransomware is on the rise in higher education

Year over year, higher education sees more ransomware attacks than most other sectors in the U.S.. Experts agree that cybercriminals don't *think* institutes of higher education know how to protect their most sensitive data. They also *think* administrators are more willing to pay the ransom to make the problem "just go away."

By mitigating the risks of cybercrime, including ransomware, higher-ed administrators and IT professionals can decrease the cost of cybercrime and show cybercriminals that they couldn't be more wrong. To help you find the information and insights you need, we've divided this eBook into three sections:

1. The current state of the ransomware threat and its impact on higher education.
2. Why most ransomware strategies miss the mark and leave institutions vulnerable.
3. How Ransomware Protection as a Service™ (RPaaS™) can help you close the gaps.



64%
of institutes of higher
education were hit by
ransomware in 2021.

- CrowdStrike Global Security Attitude
Survey 2021



INTRO:

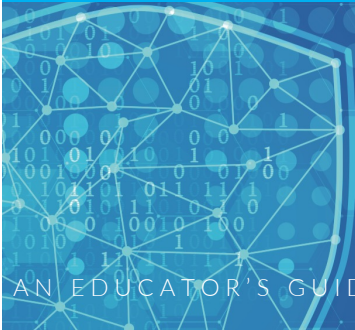
The Ransomware Threat Landscape



AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

WHAT YOU DON'T KNOW, WILL HURT YOU.

...the ransomware threat is growing.



AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

Ransomware attacks are getting more sophisticated, frequent, and costly. This has led to some alarming statistics for leaders focused on risk mitigation:



66%

of businesses suffered at least one ransomware attack.

COVID-19 strains educational systems

When COVID hit in early 2020, universities were some of the first to resort to online learning and remote work. While this approach helped protect students, staff, and educators, it put tremendous strain on educational systems and IT personnel.

When asked for his perspective on the data, John Gray, InterVision CTO, shared,

“Many educational institutions didn’t have a work-from-anywhere plan in place, so when COVID hit, they had to scramble to catch up. One of the reasons we developed our ransomware-as-a-service solution was to allow these institutions to focus on delivering remote access to learning and administrative systems, while we focused on protecting their data and systems from the threat of ransomware.”



74% saw an increase in cybersecurity workloads in 2020.

65% said IT response slowed.



PART ONE:

Ransomware's Impact on Higher Education



AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

The high cost of ransomware in higher education

The financial cost of ransomware is high in education, but even more damaging can be its potential to disrupt the lives of students and the viability of the institution.



The average cost for rectifying a ransomware attack in higher education. **The highest** of any sector in 2020.



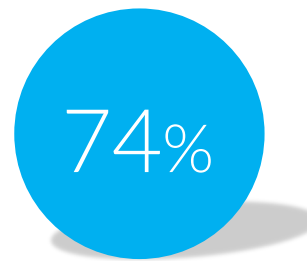
2 out of 5 institutions reported taking more than a month to recover. The slowest of any sector.

Other Notables:

- ✓ A leading university in England was forced to shut down nearly all of its IT systems and **delay the start of the next term.**
- ✓ Ransomware disabled a North Carolina college's systems, including phones, email, and learning management platforms, forcing the school to **cancel classes and all scheduled events.**
- ✓ After 157 years of serving students and the community, a ransomware attack in Dec of 2021 forced Lincoln College in Illinois to **close its doors – permanently.**

Ransomware threatens data security & compliance

Ransomware attacks often target personal data, putting institutions of higher learning at risk of violating FERPA as well as regulations governing how consumer financial information is handled. HIPAA violations are also a risk if the institution handles health data for students, faculty, or staff – as many do. Unfortunately, the threat is getting worse.



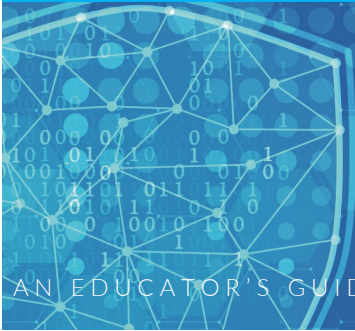
of education institutions hit by a significant ransomware attack in 2021 said their data was encrypted.
(Up from 58% in 2020)



of those whose data was encrypted, paid the ransom to get their data back.
(Up from 35% in 2020)

WHAT YOU DON'T KNOW, WILL HURT YOU.

...a quick ransomware self-check



AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

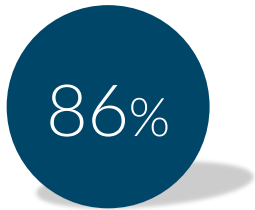
Here's a quick self-check that will help you spot the gaps in your ransomware protection and recovery strategy. No need to tally up the responses.

Simply circling yes, no, or not sure will tell you what you need to know.

| | | | |
|--|-----|----|--------|
| We have a Chief Information Security Officer (CISO) who oversees and is accountable for both cybersecurity and disaster recovery strategy. | YES | NO | UNSURE |
| We have a documented ransomware protection and recovery strategy that we review at least once a year. | YES | NO | UNSURE |
| All of our business and IT leaders understand our approach to ransomware and why adherence to the plan is vital to business continuity. | YES | NO | UNSURE |
| We've decided ahead of time on how to handle ransom demands, and we're confident we can stick to the plan. | YES | NO | UNSURE |
| We have ransomware insurance, and our executive team understands exactly what it does and does not cover. | YES | NO | UNSURE |
| Our entire staff knows exactly what to do if they suspect a ransomware attempt has been made or an attack has been successful. | YES | NO | UNSURE |
| We have dedicated IT security specialists and tools with a focus on ransomware detection, protection, and mitigation. | YES | NO | UNSURE |
| Our IT staff is confident our current systems can detect any threats lying dormant in our systems or gathering data in advance of an attack. | YES | NO | UNSURE |
| Our disaster recovery plan includes ransomware contingencies. | YES | NO | UNSURE |
| We revisit our disaster recovery strategy, especially for new and critical workloads, at least once a year and test it regularly. | YES | NO | UNSURE |

How do you compare?

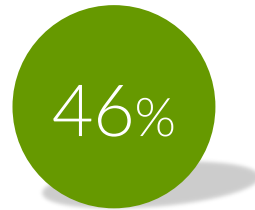
If you think you failed the pop quiz on the last page, you're not alone. While many higher-ed leaders said they think they're ready for a ransomware attack, many admit to major gaps in their planning.



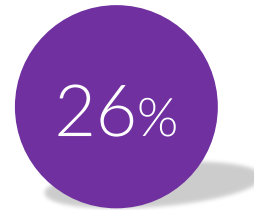
said their institution had the tools and knowledge to investigate suspicious activity.



said they had weaknesses in their cybersecurity strategy.



said ransomware was getting harder to stop as attacks increased in sophistication.



said it was difficult to prevent users from compromising security.



PART TWO:

Crafting a Comprehensive Ransomware Strategy



AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

RANSOMWARE STRATEGY

Does your ransomware strategy miss the mark?



NOT IF, BUT WHEN.

Ransomware attacks are not a matter of if, but when. Understanding that, many organizations have invested heavily in tools to strengthen their IT security position. That's good, but no detection and prevention scheme is 100% failsafe. Mitigating your risks requires a ransomware strategy that includes both protection and response.

RANSOMWARE STRATEGY

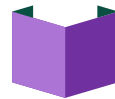
Why Higher Education falls short

If your strategy includes hoping you won't get hit with ransomware, you're not alone. Several factors combined to make executing a comprehensive ransomware strategy more challenging than ever:



PEOPLE

Of the 75% of higher-ed leaders who said they had a specific plan or policy in place to effectively manage a ransomware attack, less than 60% felt they had the staff needed to execute that plan.



PROCESSES

Ideally, ransomware strategy would be included in disaster recovery and business continuity planning, but only about half of organizations have a disaster recovery plan, and few take the time to test their plan.



TECHNOLOGY

It would be great if there were a ransomware silver bullet, but there isn't. IT departments often deploy half a dozen or more technology "solutions" and still fail to fill all the gaps in their protection and recovery plan.

Should paying the ransom be part of your

response strategy?

As you craft your ransomware strategy, one of the questions you'll need to talk about is your organization's stance on paying ransom demands. Cybercriminals would like you to believe that, if you fulfill their demands, you'll be able to go back to business as usual. That isn't always the case. Recent research underscores the need for a comprehensive ransomware response strategy that doesn't reward cyberthieves for their malicious actions.

8%

of organizations that paid the ransom got all of their data back.

96%

said they paid additional extortion fees to prevent the release of their data on the dark web.

46%

said that some or all of their data was corrupted.

80%

were hit with additional demands after they paid the initial ransom.

Is cyber insurance the answer?

In a 2021 study of cybersecurity in higher-ed, only 37% percent of respondents cited ransomware insurance as part of their resiliency strategy. While that percentage is sure to grow as cyber insurance becomes more of a “must have,” administrators need to keep in mind that insurance is only part of the picture.

Of higher-ed institutions hit by ransomware reported that cyber insurance paid



! Cybersecurity insurance is rapidly becoming a “must-have” for many businesses, but it is not a replacement for a comprehensive ransomware protection and response strategy.



PART THREE:

InterVision's Ransomware Protection as a Service™ (RPaaS™)



AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

RPAAS DEFINED

What is ransomware protection as a service (RPaaS)?

“As a service” solutions are gaining traction as a way to ensure coverage of critical aspects of IT operations while freeing up internal staff to focus on business-building initiatives. Two of the most common solutions are Security Operations Center as a Service (SOCaaS) and Disaster Recovery as a Service (DRaaS). Both of these elements are vital components of ransomware protection and recovery, but few solution providers have connected the dots between the two.

AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™



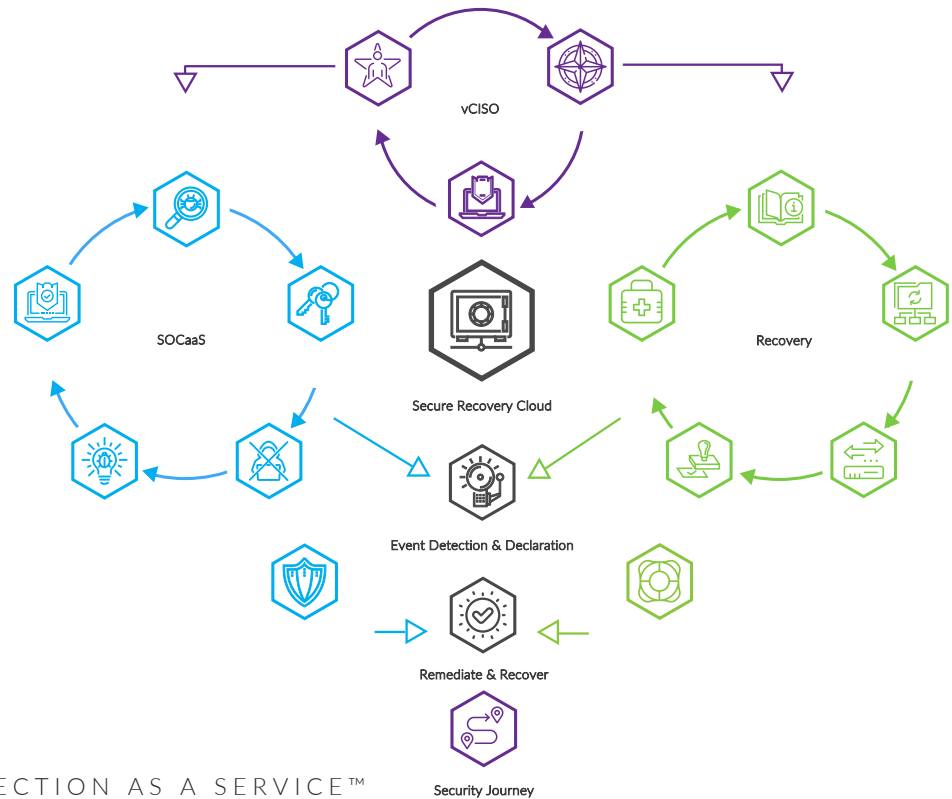
RPAAS DEFINED

InterVision's RPaaS solution

InterVision combines its industry-leading DRaaS and security services into one comprehensive **Ransomware Protection as a Service (RPaaS)** solution that addresses an organization's broader IT security and disaster recovery requirements while closing the gaps in its ransomware detection & protection, respond and recover and advise & adapt strategies.

AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

InterVision Ransomware Protection as a Service (RPaaS)

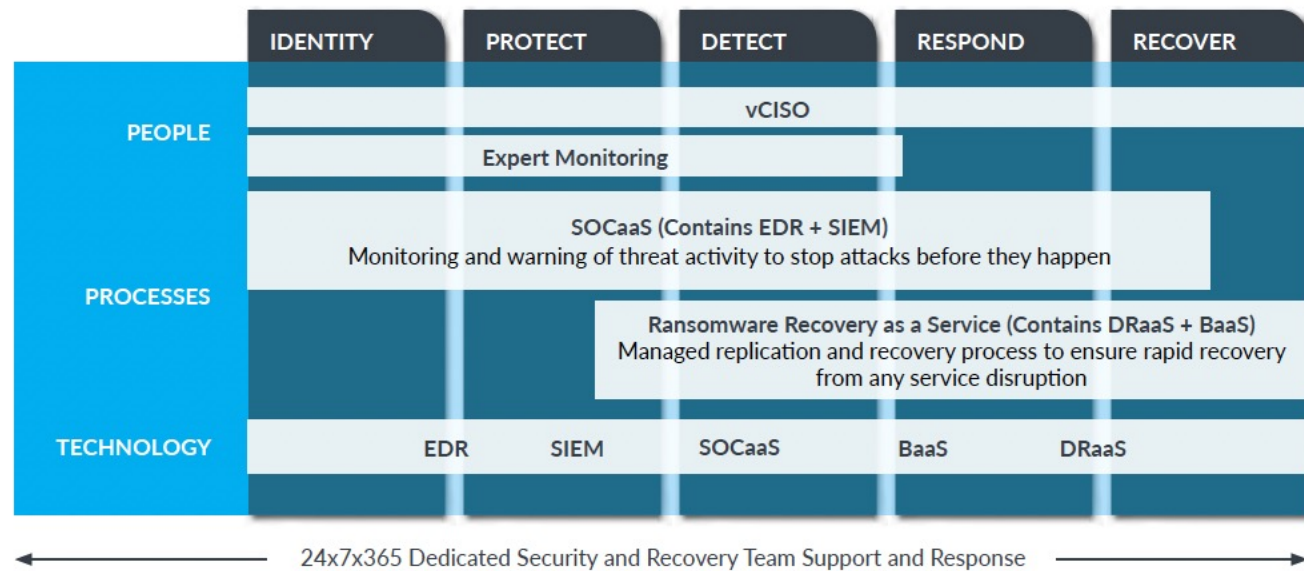


RPAAS DEFINED



Comprehensive protection

To ensure end-to-end protection, the InterVision RPaaS solution follows the five steps of the NIST Cybersecurity Framework (CSF) for Critical Infrastructure: Identify, Protect, Detect, Respond, and Recover.



At InterVision, people make the difference

While lots of managed services companies could cobble together a plan for ransomware protection and recovery, what really ties the InterVision RPaaS solution together is the vCISO assigned to your account. These senior security advisors are “big picture” cybersecurity strategists who bring years of experience overseeing security across a vast array of disparate environments.

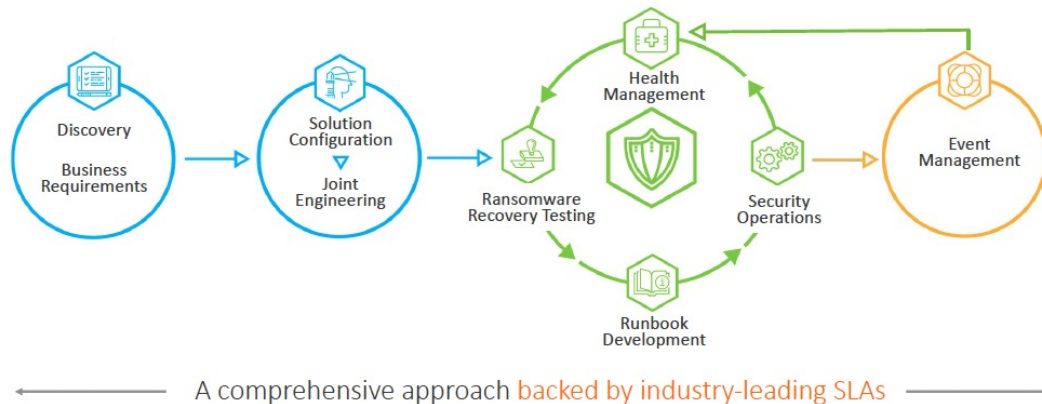


“When it comes to security and disaster recovery planning, every business needs to approach it differently. When I help clients map out their strategy, one of the key objectives I’m looking to achieve is to create a plan that meets their security and recovery objectives for their critical workloads but does not entail paying a ransom in the event of a ransomware attack.”

Allen Jenkins, InterVision Client vCISO


RANSOMWARE PROTECTION AS A SERVICE (RPaaS)

We're with you every step of the way.



From day one, your InterVision RPaaS team will work with you to create a ransomware protection and recovery strategy that uses the right tools for the job. Then they'll help you document, implement, and train your team on how to execute that plan, providing extra hands and expertise in areas where your current staffing may fall short. We'll also be with you every step of the way should a ransomware event require you to put your recovery plan into action.





Don't
become a
statistic

The tech news makes it seem like it's only the high-profile companies that are being hit with ransomware. In reality, every organization is at risk. In fact, attacks on higher education institutions continue to rise at dramatic rates due to the vulnerability and sensitivity of the data plus overall impact to students, educators and staff.

Don't let your institution be one of this year's data points. The first step is to reach out to our RPaaS team for a complimentary consultation to discuss your business requirements and answer any questions you may have.

[CONTACT US](#)



www.intervision.com/rpaas/

Sources

AN EDUCATOR'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

24



2021 CrowdStrike Global Security Attitude Survey



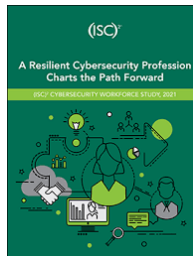
Howden, Cyber Insurance: A Hard Reset, 2021



Cybereason, Ransomware: The True Cost to Business, 2021



Sophos State of Ransomware Report 2021



(ISC)2 Cybersecurity Workforce Study, 2021



Why is Office Occupancy only 31%? Korn Ferry, February 2022. 5 IBM Cost of a Data Breach Report 2021