InterVision

CLOSING THE GAPS IN YOUR RANSOMWARE STRATEGY

66%

OF ORGANIZATIONS SURVEYED SAID THEY'D SUFFERED AT LEAST ONE RANSOMWARE ATTACK IN THE PAST 12 MONTHS.

CrowdStrike Global Security Attitude Survey 2021

Cybercrime is one of the leading causes of data center downtime, and when a business is hit with a ransomware attack, the losses can be staggering. **Detecting and preventing ransomware attacks is vital, but most security experts agree:** even with the best protection schemes, businesses will continue to fall victim. In this whitepaper, we'll examine the current ransomware threat landscape and how you can mitigate those risks with a comprehensive ransomware strategy that covers both prevention and recovery.

THE RANSOMWARE THREAT IS GROWING

In 2021, the number of ransomware attacks in the U.S. more than doubled from 2020, and 66% of survey respondents said they'd suffered at least one ransomware attack in the past 12 months.[1] While it's challenging to identify the culprits behind most ransomware attacks – even the groups change their names to evade capture – ransomware attacks are getting more sophisticated. State actors and hacktivists alike use ransomware, along with its companion attack strategy – Distributed Denial of Service (DDoS), to cripple economies, target entire industries, and shut down companies they don't like. The novice with an ax to grind can even purchase a basic Ransomware as a Service (RaaS) kit on the dark web for less than $100.

The COVID-19 pandemic has also fueled the fire as businesses allowed more employees to work from home in 2020 and 2021. Of those organizations that experienced a cyberattack, 69% said the incident was a direct result of teams working remotely.[1] "The challenge was that many businesses were not prepared for the speed at which they needed to implement their work-from-anywhere strategy," said John Gray, CTO at InterVision Systems. "One of the primary reasons we developed our ransomware protection as a service™ (RPaaS)™ solution was to help these businesses bring their defenses up to the level where they need to be to support the business's growth plan."

InterVision ransomware experts are also quick to point out that, while the breach may have happened through their remote workforce, in many cases these attacks have been successful even if everyone were working out of the same office. Businesses, across the board, simply are not ready for the ransomware threat and the impact it can have on their business.

RANSOMWARE PUTS BUSINESSES IN TRIPLE JEOPARDY

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. One recent survey found that, of the 32% of organizations that decided to pay the ransom, a mere 8% got all of their data back.[2] In another survey, 46% said that, when their systems were restored, some or all of their data was corrupted.[3]

Perhaps even more alarming is what these cybercriminals do with the data while it's under their control. In what's referred to as a double-extortion attack, data thieves may lurk in the organization's system for months, stealing data and credentials before they execute a ransomware attack. Once they encrypt the data, the threat of selling this data on the dark web raises the stakes for the victim. In 2021, 96% of business leaders who said they paid the initial ransom also had to pay extortion fees.[1] In some cases, data thieves sold the data even when their demands were met. Industry sources reported an 82% increase in ransomware data leaks in 2021.[1]

To top it all off, a quarter of businesses hit with a ransomware attack, were forced to close either permanently or for a period of time as they tried to recover.[3] But, even for businesses that survive a ransomware attack, the story may not be over. A strong majority (80%) of those who reported paying the ransom were attacked again with additional demands.[3] This statistic underscores the need for a comprehensive ransomware response strategy that doesn't reward cyberthieves for their malicious actions.

HOW RELIANT ON TECHNOLOGY ARE YOU?

FINANCIAL SERVICES

80% of respondents to a 2022 business insider survey said mobile was their primary banking method.

MANUFACTURING

The global supply chain relies on electronic transactions between manufacturers, distributors, customers, and logistics companies.

HEALTHCARE

Covid accelerated the use of telehealth services. In Q1 2022, telehealth visits jumped 50%. Post-pandemic, many providers have continued to offer telehealth as a way to relieve some of the burden on the system.

HIGHER EDUCATION

Colleges and universities have been increasing their online class offerings for years. The global pandemic brought online learning to K-12 education.

STATE & LOCAL GOVT.

State and local governments have always been pressed for resources. Offering online interactions is helping many municipalities and state governments improve constituent services.

Businesses around the world are implementing work-from-anywhere policies to increase productivity, improve employee morale, and provide greater access to talent.

IS CYBER INSURANCE THE ANSWER?

Cyber insurance is increasingly seen as a cost of doing business, and it must be an element of a comprehensive ransomware response strategy. However, the rising frequency and severity of ransomware attacks has instigated what cybersecurity reinsurer Howden, calls a "hard reset." According to their report, cybersecurity insurance rates rose 31% in 2021.[6] As the ransomware threat and the impact of an attack on business grows, insurance companies will need to cover their costs and the price tag for cyber insurance will continue to rise.

Insurers are also expanding their due diligence before approving policy applications. Depending on the coverage obtained, once the settlement is finalized, businesses may be responsible for a large part of the costs. In a recent study a cyber insurance company found that insurance did not cover all costs for 42% of businesses.[3]

"THE CYBER INSURANCE MARKET IS UNDERGOING ONE OF ITS MOST TRANSFORMATIVE CHANGES SINCE THE FIRST POLICY WAS UNDERWRITTEN SOME 20 YEARS AGO."

- Howden, Cyber Insurance: A Hard Reset

THE HIGH COST OF POOR PLANNING

Businesses across the board are increasingly reliant on technology to the extent that they couldn't do business "on paper" even if they wanted to. As organizations seek to become more global, agile, cost effective, and customer-centric, digitization of business will increase. If current trends hold, so will remote work arrangements. In February 2022, global consulting firm Korn Ferry, reported that office capacity across several large cities was still at just 31%.[4]

Given this increasing reliance on data and systems as well the alarming rise in ransomware frequency and demands, it would be natural to assume most business leaders have crafted a solid ransomware strategy. Unfortunately, that's not always the case. A survey on security attitudes found that more than half (57%) of businesses hit by ransomware did not have a coordinated response strategy.[1]

57% OF BUSINESSES HIT BY RANSOMWARE IN 2021 DID NOT HAVE A COORDINATED RESPONSE STRATEGY.

- 2021 CrowdStrike Global Security Attitude Survey

There are a number of reasons why businesses fail to plan. Business executives need to focus on their business—that big order, the latest acquisition, their next board meeting, etc. Of course, the threat of ransomware needs to be addressed, but it's easy to rationalize rescheduling a ransomware strategy discussion to tomorrow while more urgent matters are attended to. As the statistics show, tomorrow may be too late.

Some business executives expect IT leadership to be responsible for mitigating the threat of a cyberattack, including ransomware. However, technology executives are also expected to spearhead the organization's digital transformation efforts, and the infrastructure they manage is incredibly complex and always evolving. For the growth-oriented business, little time is left for strategy and planning that doesn't directly correlate to the business's growth or revenue goals.

The total cost of ransomware, including remediation costs and revenue loss, has risen to an average of $4.62 million.[5] The average ransom payment alone increased by 63% in 2021 to $1.79 million.[1]

32% OF BUSINESSES HIT WITH A RANSOMWARE ATTACK LOST LEADERSHIP ROLES EITHER THROUGH DISMISSAL OR RESIGNATION, AND 29% WERE FORCED TO LAY OFF STAFF.

- Ransomware: The True Cost to Business, 2021

In addition to high costs for the business, poor planning can have devastating personal costs as well. Cybereason found that 32% of businesses hit with a ransomware attack lost leadership roles either through dismissal or resignation, and 29% were forced to lay off staff.[3]

"OF THE 75% OF BUSINESS 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."

- Ransomware: The True Cost to Business, 2021

FINDING THE GAPS IN YOUR RANSOMWARE STRATEGY

As is often said, an ounce of prevention is worth a pound of cure. That's certainly true when it comes to cybercrime. As the data shows, ransomware attacks are a matter of when, not if. Obviously preventing an attack from ever impacting your data and systems is the best outcome, but a singular focus on prevention can lead to gaps in your ransomware strategy that leave your organization vulnerable.

The first mistake many companies make is to focus too heavily on selecting tools and technologies and not enough on staffing and expertise. It would be great if there were a ransomware silver bullet: buy this cybersecurity device or application and you can go back to focusing on your business. Despite the claims made by technology vendors, it's not that easy to protect your business against cybercrime and probably never will be.

That's not to say there aren't some incredibly powerful tools that can be used in the fight against ransomware. There are multiple tools required to cover every aspect of ransomware protection, and using these tools effectively takes considerable training and experience. If you don't configure your ransomware detection systems properly, you can leave holes in your IT security perimeter. On the other hand, if you don't know what you're looking for, your staff can be so busy chasing every anomaly, they miss the ones that really matter. (The distraction technique is a favorite among data thieves.) In addition, setting the controls too tightly can hinder business because everything looks like a threat, including that login from your CEO trying to access data while traveling.

To protect your organization, you need to combine the best technologies with experienced security specialists 24x7x365. That's not just one or two people, but a team of skilled professionals available around the clock. If you're having trouble finding, recruiting, and retaining that kind of talent, you're not alone. Of the 75% of business 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.[3] No surprise when experts estimate that the global cybersecurity workforce is still 65% below what it needs to be.

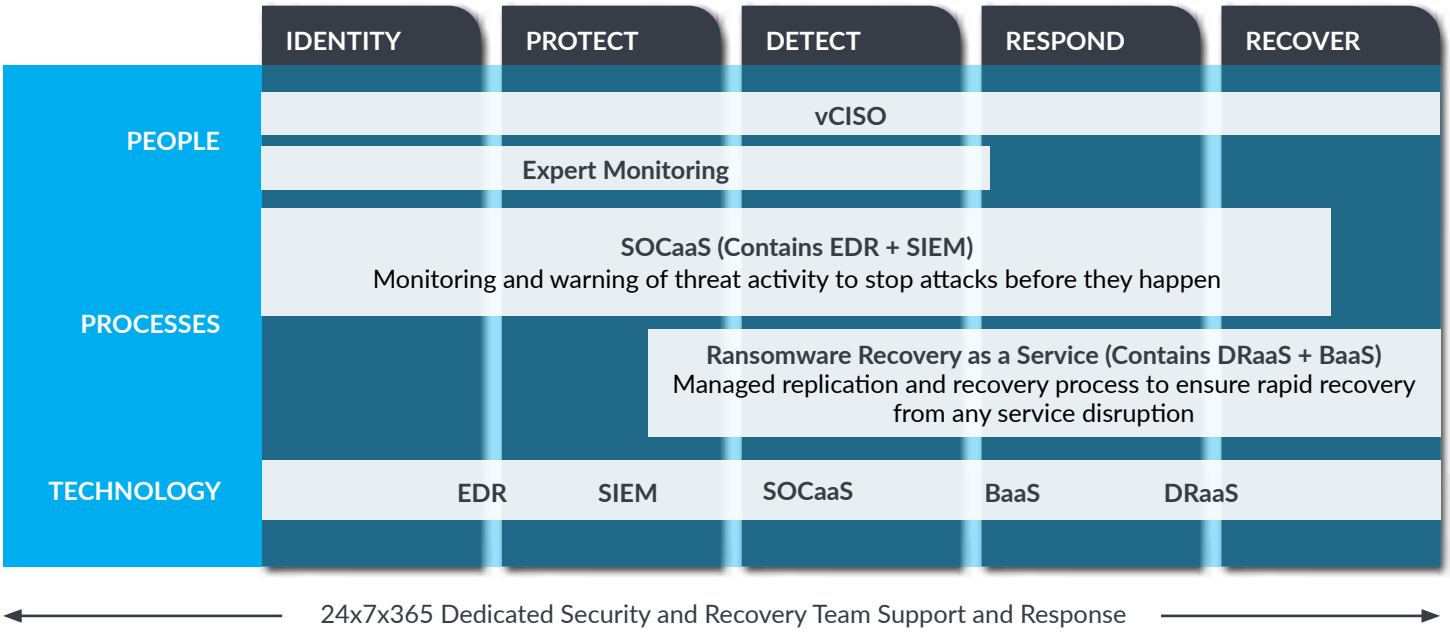
Even if you manage to assemble a team with the right people, that type of brainpower can put a pretty big dent in your budget. The scramble for IT security talent continues to push salaries higher. In 2021, the average salary for a cybersecurity role was almost $120K in North America.[7]

The second major mistake organizations make is to not focus enough on the entire spectrum of ransomware protection all the way through to recovery. As cyber-insurance provider Howden, states in their report, "The importance of being prepared for a cyberattack cannot be overstated."[6] No ransomware protection scheme is 100% reliable, so what you do when a cyberattack happens is just as important as what you do before your business is attacked.

Ideally, response planning would fall under the category of Disaster Recovery & Business Continuity Planning, but that discipline comes with its own set of issues. According to the online magazine, Security, only 54% of organizations have a disaster recovery plan. Of those, only 50% take the time to test their plan. Of those that did test, NONE said their systems performed as expected with no issues.

The reasons given for poor disaster recovery planning are often the same as those for poor IT security planning: the high cost of finding and retaining staff, increasingly complex and always evolving technology, and lack of time and resources. As a best practice, Disaster Recovery & Business Continuity Planning should include ransomware recovery, but given the challenges faced by both disciplines, many business leaders rightfully lack confidence in their ability to recover from ransomware.

INTERVISION RPAAS DELIVERS COMPREHENSIVE PROTECTION



RANSOMWARE PROTECTION AS A SERVICE

"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 as a Service and Disaster Recovery as a Service (DRaaS).

As we've discussed, both of these elements are vital components of ransomware protection and recovery, but few solution providers have connected the dots between the two. InterVision has combined its 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 clients' ransomware protection and recovery strategies.

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. Just as importantly, InterVision weaves together the key elements of people, processes, and technology into a comprehensive solution.

"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, vCISO, InterVision

PEOPLE

The primary role of the chief information security officer (CISO) is to reduce business technology risks. However, while the role of CISO is becoming more common, individuals with this level of expertise can be the hardest to find, the most expensive to hire, and the most difficult to retain. When IT leadership lacks critical expertise, organizations struggle with their overall security strategy and get lost in day-to-day operational tasks.

With InterVision's RPaaS service, you'll be paired with one of our virtual CISOs (vCISO) who will work with you to develop a holistic security strategy. These senior security advisors are "big picture" cybersecurity strategists who bring years of experience overseeing security across a vast array of disparate environments. Following the NIST CSF model, your vCISO and team of InterVision security experts will work with you to identify critical assets and design the appropriate protection, detection, response, and recovery tools and processes.

"When it comes to security and disaster recovery planning, every business needs to approach it differently," said Allen Jenkins, vCISO at InterVision. "However, 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."

PROCESSES

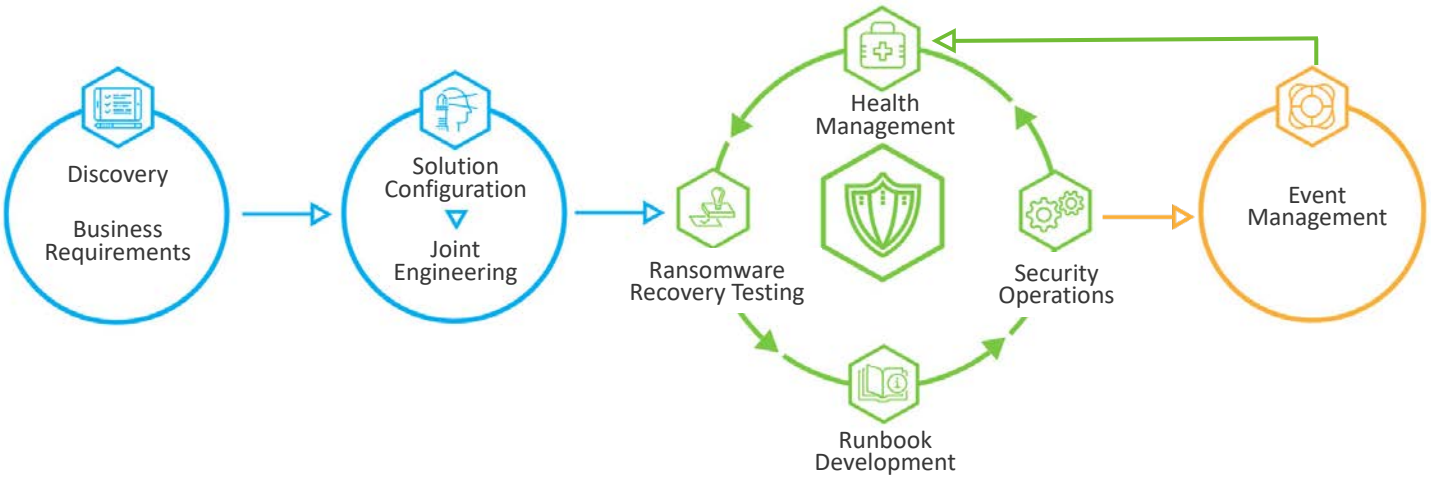
Well-architected processes, including security monitoring and ransomware response, are a key component of a robust ransomware strategy. One of the key goals with the InterVision RPaaS offering is to create a plan for each customer that meets the security and recovery objectives for each of their critical workloads that **does NOT entail paying a ransom**.

After your solution is deployed, your systems will be monitored 24X7 from our Security Operation Center to quickly identify and contain any anomalous activity. In the event of a ransomware attack, the vCISO will lead the triage team to provide cyber-incident coordination efforts to ensure appropriate, effective, and rapid recovery to normal business operations.

TECHNOLOGY

The foundation of your RPaaS solution is created by the technologies we deploy on your behalf. Our security and disaster recovery experts work with these tools 24X7 so they know them inside and out. In addition, we're always looking for the best tools for the current threat landscape so our clients are geared up for whatever the future brings.

THE INTERVISION RPAAS PROCESS



A comprehensive approach backed by industry-leading SLAs

DON'T BECOME A STATISTIC

The tech news can be misleading because the latest stories make it seem like it's only the high-profile companies that are being hit with ransomware. In reality, the data we shared in this paper includes ransomware attacks against companies of all sizes and in all industries. In fact, smaller companies may be more at risk of ransomware because cybercriminals know they often lack the budget and resources to mount a proper defense.

Don't let your organization 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

[1] 2021 CrowdStrike Global Security Attitude Survey.
[2] Sophos State of Ransomware report 2021.
[3] Cybereason, Ransomware: The True Cost to Business, 2021.
[4] Why is Office Occupancy only 31%? Korn Ferry, February 2022.
[5] IBM Cost of a Data Breach Report 2021.
[6] Howden, Cyber Insurance: A Hard Reset, 2021
[7] (ISC)2 Cybersecurity Workforce Study, 2021.

