VERITAS

6 WAYS RANSOMWARE CAN HURT THE FINANCIAL SERVICES SECTOR—

AND WHAT YOU CAN DO TO COMBAT THE THREAT

Start now

ARE YOU RANSOMWARE READY?

The first half of 2020 saw a **238%** increase in cyber attacks targeting financial institutions.[i]

The average cost of a data breach in the financial sector in 2021 was **$5.72 million**.[ii]

The U.S. was the most attacked nation on the planet in 2021, taking **421.5 million** hits. With a year-on-year increase of 89%, it's a staggering rise in cases.[iii]

In a rapidly evolving marketplace, it's essential that the financial sector adopts a next-generation mindset. Consumers expect seamless, personalized digital experiences, while simultaneously feeling highly conscious of data protection and privacy. This means the financial sector must balance the need to innovate with the need to minimize risk to reputation and customer trust. **So, it's time to ask yourself the question:**

IS YOUR ORGANIZATION REALLY PREPARED FOR A RANSOMWARE ATTACK

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

IT'S LIKELY YOU WILL BE SOON.

[i] https://www.vmware.com/resources/security/modern-bank-heists-2020.html [ii] https://techxplore.com/news/2021-10-mn-ransomware-payments-surge.html [iii] https://www.ibm.com/security/data-breach

THE RISE OF RANSOMWARE

The banking industry saw a **1,318%** year-on-year increase in ransomware attacks in the first half of 2021.

That's largely due to the upsurge of Ransomware as a Service (RaaS). 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. The case for prioritizing cybersecurity hygiene and implementing best practices immediately is clear. That's 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.

THE REAL COST OF RANSOMWARE

Financial institutions in particular are regular targets for ransomware attacks. And with an attack taking place every 11 seconds, it's not a matter of 'if' but 'when'.

If the worst does happen, the impact can take many different forms:

Click on the numbers to find out more.

1 2 3 4 5 6

LOSS OF COMPANY DATA:

Data is the lifeblood of your sector. Temporary loss is bad. Permanent is a disaster.

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

THE IMPACT:

The Reserve Bank of New Zealand suffered a serious data breach by way of a third-party file-sharing app. Access was gained by exploiting a previously unknown vulnerability in the FTA application, with DOBs, credit details and personal email addresses uncovered. In total, the breach cost around **NZ$3.5m**.[iv]

[iv] https://securitybrief.co.nz/story/the-biggest-cyber-attacks-of-2021-in-new-zealand [v] https://www.computerweekly.com/news/252498029/Average-ransomware-cost-triples-says-report [vi] https://www.infosecurity-magazine.com/news/ransomware-demands-surge-2021/ [vii] https://www.bankinfosecurity.com/cna-discloses-breach-related-to-march-ransomware-attack-a-17022#:~:text=The%20insurance%20company%20CNA%20Financial,and%20breach%20notifications%20that%20went [viii] https://three-two-four.com/insights/ransomware-the-growing-threat/ [ix] https://totalsecuritysummit.co.uk/briefing/financial-retail-healthcare-and-manufacturing-suffer-revenue-losses-following-ransomware-attacks/ [x] https://www.computerweekly.com/news/252506646/Cost-of-ransomware-attack-in-financial-sector-exceeds-2m [xi] https://gulfbusiness.com/financial-services-companies-may-be-vulnerable-to-ransomware-for-another-two-years/ [xii] https://chessict.co.uk/media/3738/sophos-state-of-ransomware-financial-services-2021-wp.pdf [xiii] https://techcrunch.com/2021/08/18/ransomware-recovery-can-be-costly-and-not-just-because-of-the-ransom/ [xiv] https://biztechmagazine.com/article/2021/09/ransomware-what-financial-firms-need-know

COMBAT THE THREAT WITH VERITAS

The pace of technological change in financial services might be exciting news for customers, but it creates potential vulnerabilities cybercriminals will look to exploit, such as:

- **Compliance**, which is always front of mind in finance.
- **Competition** from the cloud-born banks and FinTech start-ups, as well from the 'big tech' firms on a mission to roll financial services into their offerings.
- **Cloud technology** and the analysis of data in real-time.

These factors are attractive to the criminal element.
The importance of a strong ransomware strategy is obvious.

Veritas will help you modernize your data management architecture so that you can deliver digital experiences that set your organization apart and grow market share—without risking data security or your reputation.

How? With a unified, multi-layered cybersecurity strategy built on three pillars:

Click on the buttons to find out more.

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.

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 your IT environment, 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 can work with their malicious code. And advanced scanning functionality ensures restored data is clean and uncompromised.

Detect gaps in your resiliency plan before they become a problem, with a holistic view across your whole data estate.

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, such as secondary data centers and data centers in the cloud on-demand—fits the bill.

True resiliency requires a rock-solid partnership founded on flexibility, a hybrid model, and rapid recovery.

Click on the numbers to find out more.

1 2 3

AUTOMATION IS AT THE HEART OF AN EFFECTIVE RECOVERY STRATEGY

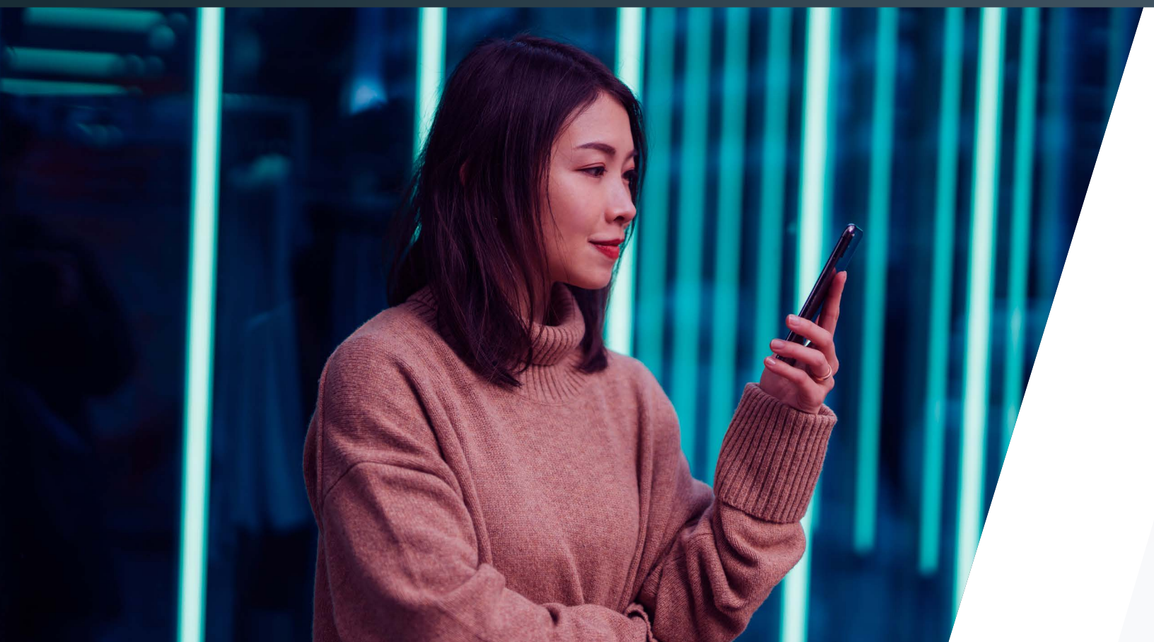
The coordination of disparate teams such as network, storage, and security MUST be done in advance. So that when a ransomware attack does hit, the recovery plan is simple and clear. All aspects of recovery can be abstracted into a Virtual Business Service (VBS). This VBS provides one-click automatic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

WHAT'S YOUR NEXT STEP?

The threat of ransomware is frightening. We're seeing more bad actors and more attacks.

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 on the rise. Financial services organizations like yours are feeling exposed, with critical data widely distributed across physical, virtual, and cloud environments.

Fortunately, 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 organisation safe, schedule a meeting.

veritas-events.com/Financial-Services-Customer-Briefing/

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™