



An IT Leader's Guide to Data Protection for the New Threatscape

Strategies for establishing a last line of defense to improve business resilience and resist the impacts of ransomware



The cybercrime boom

As the world continues to recalibrate and recenter after many months of life-altering events, the cybercrime industry has become more lucrative than ever.

The most common tactic? Ransomware. The average weekly ransomware activity has increased more than tenfold since just last year. More than one-third of organizations experienced ransomware attacks in 2020.¹

And ransomware isn't just becoming more prevalent — it's becoming more sophisticated and targeted. Of the organizations that were hit by ransomware last year, the majority (54%) said the cybercriminals succeeded in encrypting their data. However, on average, only 65% of the encrypted data was restored after the ransom was paid.¹

This lose-lose scenario is particularly disturbing given that the average ransom paid by mid-sized organizations was \$170,404. What's more, the average bill for rectifying a ransomware attack — considering factors such as downtime and staffing, ransom paid, and device, network, and opportunity costs — was \$1.85 million.¹

\$350 million

was paid out for ransomware attacks in 2020.²



Small businesses comprise approximately **one-half to three-quarters of ransomware victims**.²

The U.S. Department of Justice has **elevated investigations of ransomware attacks to a similar priority as terrorism**.³





In search of security

To mitigate risk, there are now dozens of security frameworks — some voluntary, some required by government regulation — that organizations can align to. Compliance standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) exist to help organizations determine how best to protect data, manage risk, and care for sensitive data.

One of the most reputable voluntary frameworks is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, created in 2013 in response to an executive order by former U.S. President Obama. NIST uses business drivers to guide cybersecurity activities and considers cybersecurity risks together with an organization's risk management program. Organizations like Insight proudly align with NIST as the framework continues to evolve with ongoing research, analysis, and collaboration across a diverse group of stakeholders.

Businesses may wind up adopting multiple security frameworks, by choice or by necessity, to weave together a security program that can stand up to today's cybercriminal activity. But ultimately, there are no guarantees. Whether or not your organization will experience a cyberattack may no longer be a matter of "if," but "when."

Thus, it has become essential to have robust data protection infrastructure in place. A strong data protection environment offers a fallback plan and more peace of mind — even if bad actors take hold of, encrypt, delete, or compromise your data.

In the event you become a victim of a cyberattack, effective data protection ensures:

- You have reliable access to your data.
- You have minimal downtime.
- You don't have to pay a ransom if one is demanded.
- Losses (financial, productivity, reputation, etc.) are minimized.

Organizations with legacy data protection infrastructure should note: Bad actors are increasingly zeroing in on data protection environments as a cyberattack strategy, finding an entry point and lingering within the organization for several months to learn about those environments, then delete and/or compromise them. Modernizing your data protection infrastructure and processes can greatly help defend against these types of attacks.

No business is safe.

Organizations across industries have suffered crippling ransomware attacks.

Privately owned pipeline operator

The company publicly announced on May 7, 2021, that it was a victim of a ransomware attack and it needed to temporarily shut down operations and freeze IT systems. The company provides roughly 45% of the East Coast's fuel and is one of the largest pipeline operators in the U.S.

- More than 100GB of corporate data was stolen in just two hours.
- A legacy virtual private network profile was identified as the most likely threat vector.
- The company paid a ransom of nearly \$5 million in return for a decryption key that was so slow the company still had to restore from backups.⁴

University medical center

Complaints of access issues from staff prompted the IT desk at the medical center to perform an investigation. What they found was a file with instructions to contact the perpetrators of a cyberattack. For almost a month, the medical center's electronic health records, payroll, and other systems were unavailable.

- Though a ransom was never paid, the attack cost an estimated \$63 million.
- Surgeries were delayed, and patients were referred elsewhere.
- It took IT staff three weeks working 24/7 to scrub network systems and restore 5,000 infected computers and endpoints.⁵

Large commercial insurer

In March 2021, one of the largest commercial insurers in the U.S. paid a cybercriminal group two weeks after corporate data was stolen and executives were locked out of their network. For days, the company delayed payment and attempted to recover files, but they were unsuccessful.

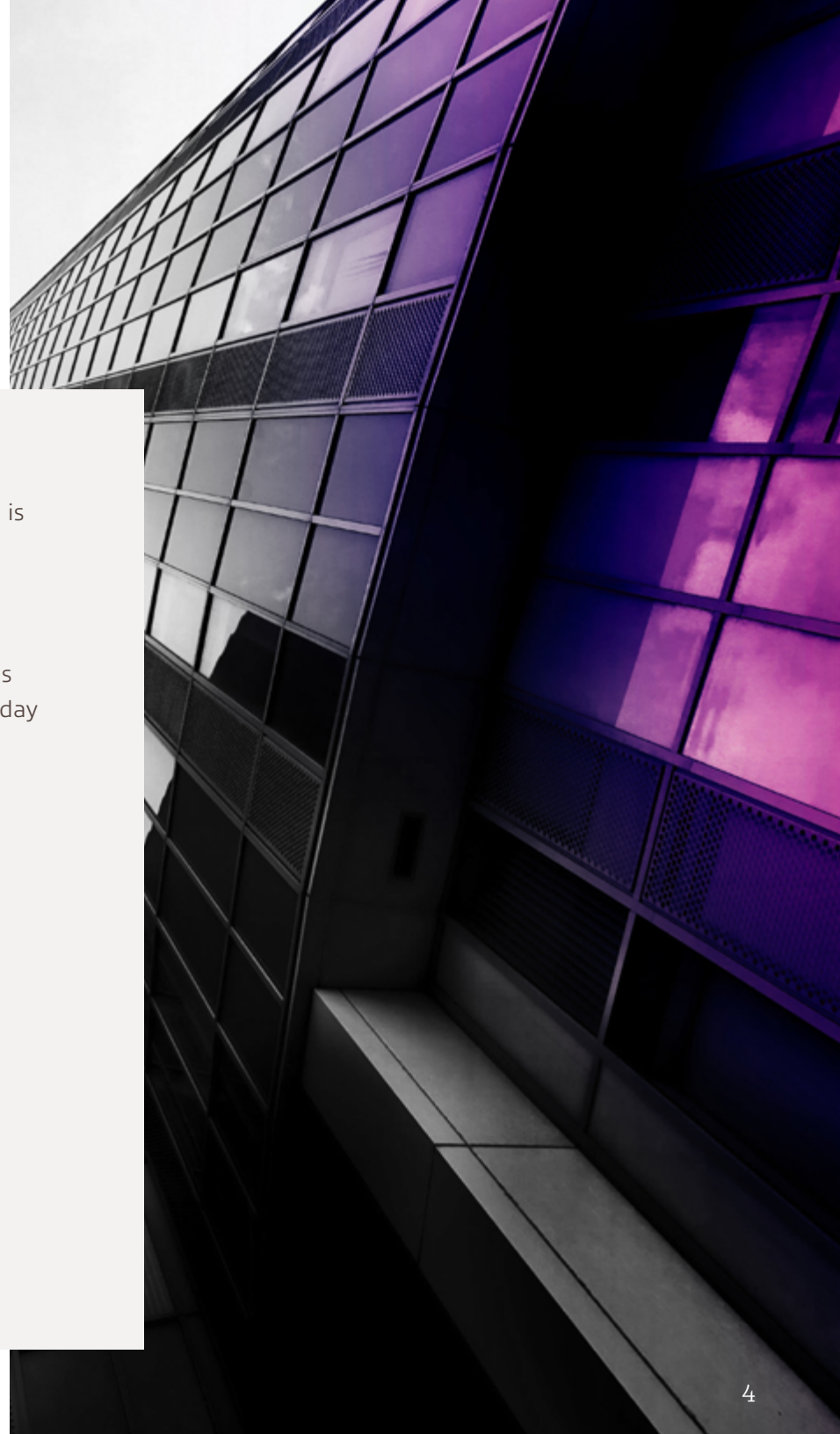
- A ransom payment of \$40 million was issued to the hackers.
- The malware used in the attack was created by a Russian cybercrime syndicate.
- Sensitive data (names, health benefits info, SSNs, etc.) of roughly 75,000 individuals was compromised.⁶



Missteps and missed opportunities

The issue of ransomware is multifaceted — and part of the problem is the integrity of data protection infrastructure.

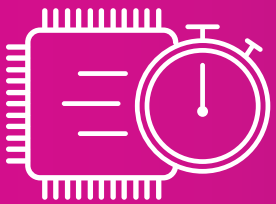
Organizations need to reassess how data is stored, protected, and backed up across environments. There are a handful of common pitfalls that IT leaders can be cognizant of and work to avoid.



1 Lack of extensive testing

When a bad actor infiltrates a system and a ransomware event occurs, timing is everything — how long will it take for the organization to get back online?

Without a commitment to testing, there's no telling how long it will take for a business to bounce back because that scenario hasn't been validated. Test restores are commonly performed on smaller parts of an environment, such as restoring a file, application, or part of a network. What we don't see a lot of today is testing entire ransomware response plans.



Back in a flash

If you ask any IT expert in the security and data protection space, they'll tell you that flash storage is a worthwhile consideration. Flash provides very low SLA times, helping you get systems back online quickly.



2

Failing to understand data estates

IT environments today are a sprawling landscape of platforms and systems. Legacy infrastructure intermixes with new architectures and ways of operating. New technologies and Artificial Intelligence (AI), machine learning, and edge computing workloads are producing massive quantities of data. Data is everywhere, silos are rampant, and complexity is nearly unavoidable.

The unfortunate outcomes of this situation, among others, are minimal visibility and poor security — and organizations that don't know what data they have, where it resides, and how to protect and manage it effectively.

Top challenges of data management:

- Data growth (67%)
- Lack of visibility (60%)
- Hybrid cloud complexity (60%)

Data challenges:

- Protecting data (53%)
- Compliance, regulatory, data sovereignty, and privacy requirements (47%)
- Data integrity (46%)⁷

3

A siloed focus on tools

Many products claim to singlehandedly stop ransomware. This simply isn't possible. There is no point solution that addresses all aspects of ransomware prevention and response.

The only way to ensure readiness for an attack is to develop and execute a strategy that spans risk avoidance (security controls, firewalls, end-user education, etc.) and risk minimization (modern data protection infrastructure).

4

Single-restore mindset

It's relatively easy to test and enable single-file or single-application restores, but this isn't enough today. Ransomware attacks don't target single machines — they impact entire IT environments and the businesses to which they belong.

Organizations need to be ready and able to restore entire environments within a reasonable timeframe. Failing to think about secure recovery at scale puts the business at risk for significant additional damage when an attack occurs.

Data protection: The big picture

The prevalence of cyberattacks like ransomware has led to a renewed focus on ransomware prevention and backup and recovery. Remember: The best data protection strategy is a multilayered one. Always ensure you are following best practices across the following areas:



Data lifecycle management



Data risk management



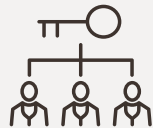
Data storage management



Regulations and standards compliance



Data sovereignty



Data access management control



Testing, exercising, and reporting



Continuous improvement

Factors for success

Ransomware attacks generally don't have happy endings — but there are several key traits found across modern organizations that are successfully improving their chances of minimizing the damage and impact of an attack.

01. A security team mindset shift

Security teams play a key role in defending an organization against cyberattacks, but programmatic approaches have become critical. Organizations that are able to break down silos and drive cross-functional efforts between security and infrastructure/operations teams are likely to develop stronger data protection strategies, improve overall security posture, and realize more business outcomes.

02. Tape for air-gapped backups

There are many ways to back up data. But tape is making a comeback because of its ability to provide an air gap — a completely offline, inaccessible copy of sensitive data. Organizations can write the copy, physically handle the tape, and ship it to a secure storage facility where it sits untouched until it's needed again. Tape's capacity, performance, longevity, cost, and increased compatibility are other qualities that make it appealing.

03. All-flash

Flash storage is another backup storage option that's helping organizations minimize recovery point and recovery time objectives. It can provide fast or synchronous replication and automatic failover, as well as be easily integrated with cloud and hybrid cloud environments.

04. Immutable storage

Historically, immutable storage was a perk. However, many modern data protection solutions are now built around the idea that immutable storage is essential. Immutability lets organizations take a snapshot of their data and set policies on its expiration, knowing that the data is unaffected and completely restorable until that time, regardless of any unintentional (end-user error) or intentional (cyberattack) breach of the environment.

A law firm gets attacked — and bounces back.


A top-ranked U.S. law firm and financial services provider was devastated when it learned of a phishing-based ransomware attack that infected its infrastructure. Digital assets were frozen, operations stalled, and 700 devices were rendered useless.

The firm took immediate action and contacted Insight for help. Our Incident Response team — 16 consultants, architects, and security experts — worked around the clock to restore data, remediate critical systems, restore desktop and server functionality, and enable multi-factor authentication and other security protocols.

Within 32 hours, the firm had some business functionality restored, with full environment functionality restored over the course of a week. Backup data was fully restored, so the firm did not have to purchase the cyberattacker's decryption tool or pay the ransom of \$1.8 million.

Want to read more success stories? Check out these case studies:

- [Credit Union Sees Instant Benefits and ROI With Cloud Disaster Recovery](#)
- [Minnesota Wild Scores With Infrastructure Refresh and New Disaster Recovery Solution](#)
- [Intellectual Property Law Firm Gains Robust On-Prem Data Protection](#)
- [Networking Technology Company Protects Data Easily and Cost-Effectively With Rubrik Solution](#)



“The rate of innovation today is exceeding the rate at which organizations can wrap their heads around their data to classify it. Data is constantly changing and being created. Classification kind of falls by the wayside. We don’t have time to do it. There’s a rush to get business solutions to market. So, we take shortcuts, and we just say, ‘Protect everything. Everything’s important.’ But certain types of data really require more stringent protection and security processes than others.”

Principal Architect, Insight

05. Two-factor authentication

One relatively simple way organizations can mitigate the risk of an attack is by deploying two- or multi-factor authentication to validate users prior to granting access to data. In fact, even one of the weakest forms of two-factor authentication — verification via SMS text messages — can stop 100% of all automated attacks, 96% of bulk phishing attacks, and 76% of targeted attacks.⁸ Experts suggest using hardware security keys as part of two-factor authentication for privileged users (senior executives, finance and HR staff, etc.), as many bad actors will target these individuals with great amounts of effort.⁹

06. Strong data discovery and classification processes

Understanding what data is being stored and where has become more critical than ever. Data discovery and classification, performed regularly, is the key to highly effective data protection and storage. Such efforts can also simplify working with auditors and improve data analytics. Yet, many organizations may avoid discovery and classification because it’s a considerable undertaking.

Organizations that are successful with data discovery and classification often start with a comprehensive data discovery exercise, followed by defining high-level data categories — sensitive, critical, regulated, etc. Different types of data should receive different treatment — for example, a company’s IP may be stored offline in a highly secure tape facility, whereas Word documents of HR operational processes may be stored in the cloud.

07. At-scale test restores

Proactive and secure organizations have made business continuity and disaster recovery top priorities. Today, this means performing at-scale test restores, in which the entire environment is being restored, as opposed to single files, apps, or machines.

In order to achieve fast and complete restores, testing scenarios should proceed with the premise that the primary data center has been encrypted, as is the case with a ransomware attack. Data should be replicated to a secondary data center — the last line of defense to get an environment back online.

It's helpful to ask the following questions of your business:

- Do we have the ability to completely restore our environment?
- What is our process for widescale restores?
- How long does it take to fully restore our environment?
- How long can the business survive while we're down restoring the environment?

08. Ongoing efforts around data protection

Changes within an IT environment, to business data, and across the external environment should prompt changes to an organization's data protection strategy.

Developing a strong data protection platform is not a one-and-done activity, but rather an ongoing commitment to key practices. Examples include:

- Regular data discovery and classification
- End-user security awareness training
- Methodology testing
- Infrastructure modernization
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) reviews and updates





Thinking beyond ransomware

Ransomware and other cybercriminal activities aren't the only threats to corporate data. It's important to consider other ways that data might be misused, corrupted, or lost when strategizing a refresh or modernization of data protection infrastructure and processes.

For instance:

- Data center and cloud migrations or consolidations, performed with minimal planning and/or without expert assistance
- Intentional or unintentional unauthorized user access (Modern networking should also be a top priority.)
- Poorly managed configurations



Charting a path forward

If there is any one truth about data protection, it is that there is no singular best course of action.

The optimal data protection strategy and infrastructure will be unique to your organization and its specific needs, risks, and objectives. It will only be of benefit to consider your many options for protecting data and mitigating the ever-present risk of ransomware.

If and when your organization would like outside support, Insight is here to help. Our team has deep expertise in data protection, storage, data management, and security across the entire NIST Cybersecurity Framework. Clients appreciate what we bring to the table:

25+ years

of data center experience

14 years

of penetration testing,
vulnerability assessment,
and security management

16 years

of incident and threat
management experience

Reach out to Insight to discuss your cybersecurity and data protection needs — and explore all the ways we can help fortify your strategy. [Contact our team.](#)

For more information about Insight's approach, explore the following resources:

Solution brief: [Ransomware Prevention and Recovery](#)

Solution brief: [Data Protection Assessment](#)

eBook: [4 Best Practices for Ransomware Readiness](#)

Infographic: [The Reality of Data Security and the New Normal](#)

Infographic: [Effective Disaster Recovery for IT Teams](#)

Video: [Prevent and Recover: Mitigating the Threat of Ransomware](#)

Video: [Preventing Data Loss With Remote Workforces: A CISO and a Security Expert Weigh In](#)

About Insight

At Insight, we help clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services help organizations strategically leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.



solutions.insight.com | insight.com

Sources:

¹ Sophos. (April 2021). The State of Ransomware 2021.

² Barr, L. (2021, May 6). DHS secretary warns ransomware attacks on the rise, targets include small businesses. ABC News.

³ Bing, C. (2021, June 3). Exclusive: U.S. to give ransomware hacks similar priority as terrorism. Reuters.

⁴ Osborne, C. (2021, May 13). Colonial Pipeline attack: Everything you need to know. ZDNet.

⁵ McKeon, J. (2021, June 24). UVM Health Continues to Feel Effects of Ransomware Attack. Health IT Security.

⁶ Mehrotra, K. and Turton, W. (2021, May 20). CNA Financial Paid \$40 Million in Ransom After March Cyberattack. Bloomberg.

⁷ IDG. (2021). Data Innovators Guide: Taking Data to the Next Stage. Sponsored by Hewlett Packard Enterprise.

⁸ Moscicki, A. and Thomas, K. (2019, May 17). New research: How effective is basic account hygiene at preventing hijacking. Google Security Blog.

⁹ Lemos, R. (n.d.). The state of MFA: 4 trends that portend the end of the solo password. TechBeacon.