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

Insight®

The cybercrime boom

Today, the cybercrime industry is more lucrative than ever. The most common tactic? Ransomware. In fact, **73% of organizations worldwide paid ransom to recover data in 2023.**[1]

And ransomware isn't just becoming more prevalent — it's becoming more sophisticated and targeted. This is particularly disturbing given that the **average ransom payment rose from $328,000 to $740,000 between Q1 and Q2 of 2023.**[2] What's more, the **average downtime per ransomware attack is 24 days.**[3]

With cybercrime booming, it's increasingly important for your organization's data to be portable, accessible and available — but this requires modern data protection strategies. Keep reading to discover what's trending in data protection today, common data protection challenges and how to position your organization for security success.

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, take 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 deleting and/or compromising them. Modernizing your data protection infrastructure and processes can help safeguard your organization against these types of attacks.

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 should be cognizant of and work to avoid.

1

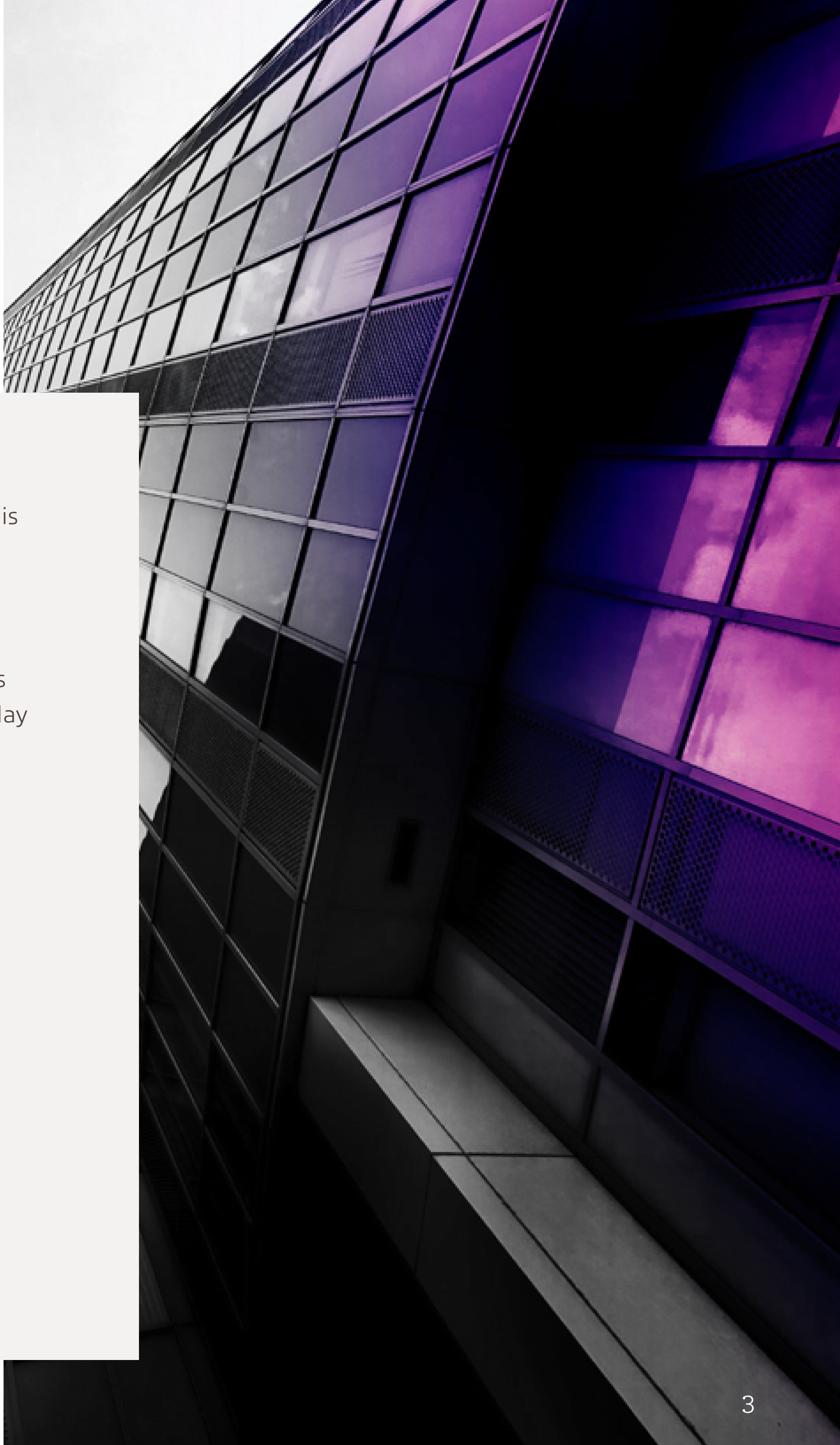
Lack of extensive testing

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 as well as AI, machine learning and edge compute 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
- Lack of visibility
- Hybrid cloud complexity

Data challenges:

- Protecting data
- Compliance, regulatory, data sovereignty and privacy requirements
- Data integrity

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.

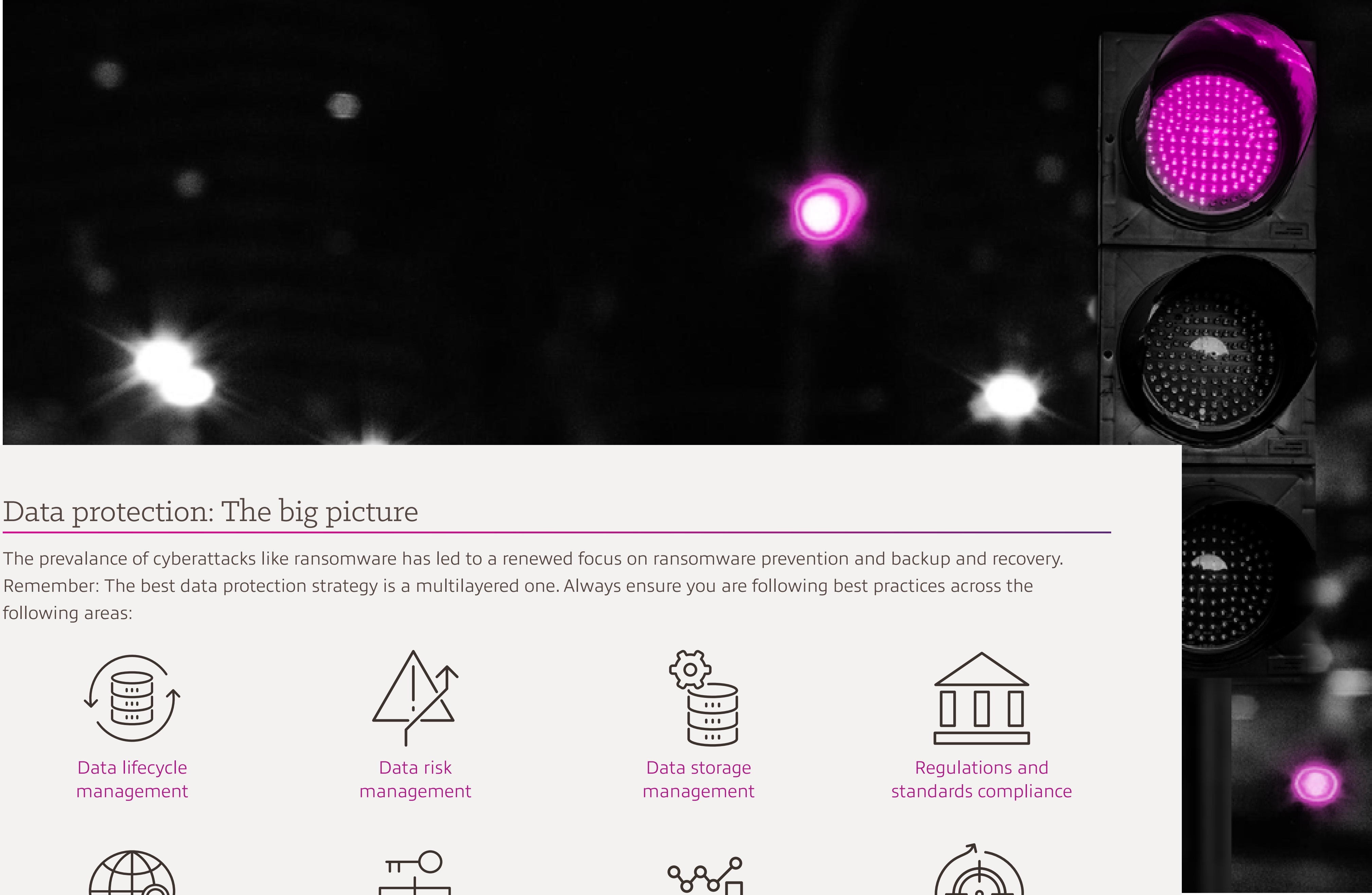
The only way to ensure readiness for an attack is to develop and execute a strategy that spans risk avoidance (security controls, firewalls, end-user education, etc.) and risk minimization (modern data protection infrastructure).

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 time frame. 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 prevalance 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 soveriengty
- Data access management control
- Testing, exercising and reporting
- Continuous improvement

Factors for success

There are several key traits found across modern organizations that have proven success minimizing the damage and impact of ransomware attacks.

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. Isolated backups

There are many ways to back up data. Tape is making a comeback for 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.

For total business continuity when it comes to multiplatform infrastructure, cybersecurity vaults provide maximum control for data and infrastructure. Vault technology can exist on-premises, in a colocation or even in a public cloud, providing comprehensive opportunities to protect not just data, but also services and infrastructure needed for critical business support.

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

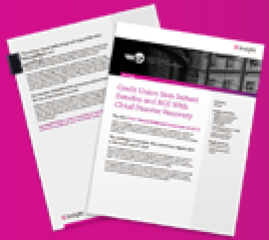
Historically, immutable storage was a perk. However, many modern data protection solutions are now built around the idea that immutable storage is essential. Immutability lets organizations take a snapshot of their data and set policies on its expiration, knowing that the data is unaffected and completely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

Client success with data protection

Secure data sharing for a healthier future

Today, Vivli is the largest data-sharing platform for clinical trials around the world. Discover how Insight helped Vivli build a single intuitive platform to combine and integrate clinical health data — without sacrificing privacy.

→ Read the client story

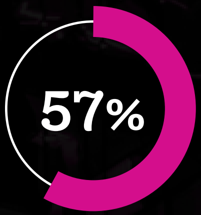


Cost-effective, scalable disaster recovery in Microsoft Azure cloud

Dow Chemical Employees’ Credit Union (DCECU) needed to move its on-premises data center to Microsoft® Azure®. Explore how Insight helped DCECU achieve increased data access and security through the cloud, faster disaster recovery and improved ROI.

→ Read the client story

Did you know?



of organizations that offer Multi-Factor Authentication (MFA) use either push notifications via phone/email or one-time passwords.[4]

05. Two- or multi-factor authentication

One relatively simple way organizations can mitigate the risk of an attack is by deploying two-factor authentication or MFA to validate users prior to granting access to data. In fact, even one of the most basic forms of two-factor authentication — verification via SMS text messages — can help stop automated attacks, bulk phishing attacks and targeted attacks. Hardware security keys are a recommended form 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.

06. Strong data discovery and classification processes

Understanding *what* data is being stored *where* is more critical than ever. To ensure highly effective data protection and storage, it is key to perform regular data discovery and classification. 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.

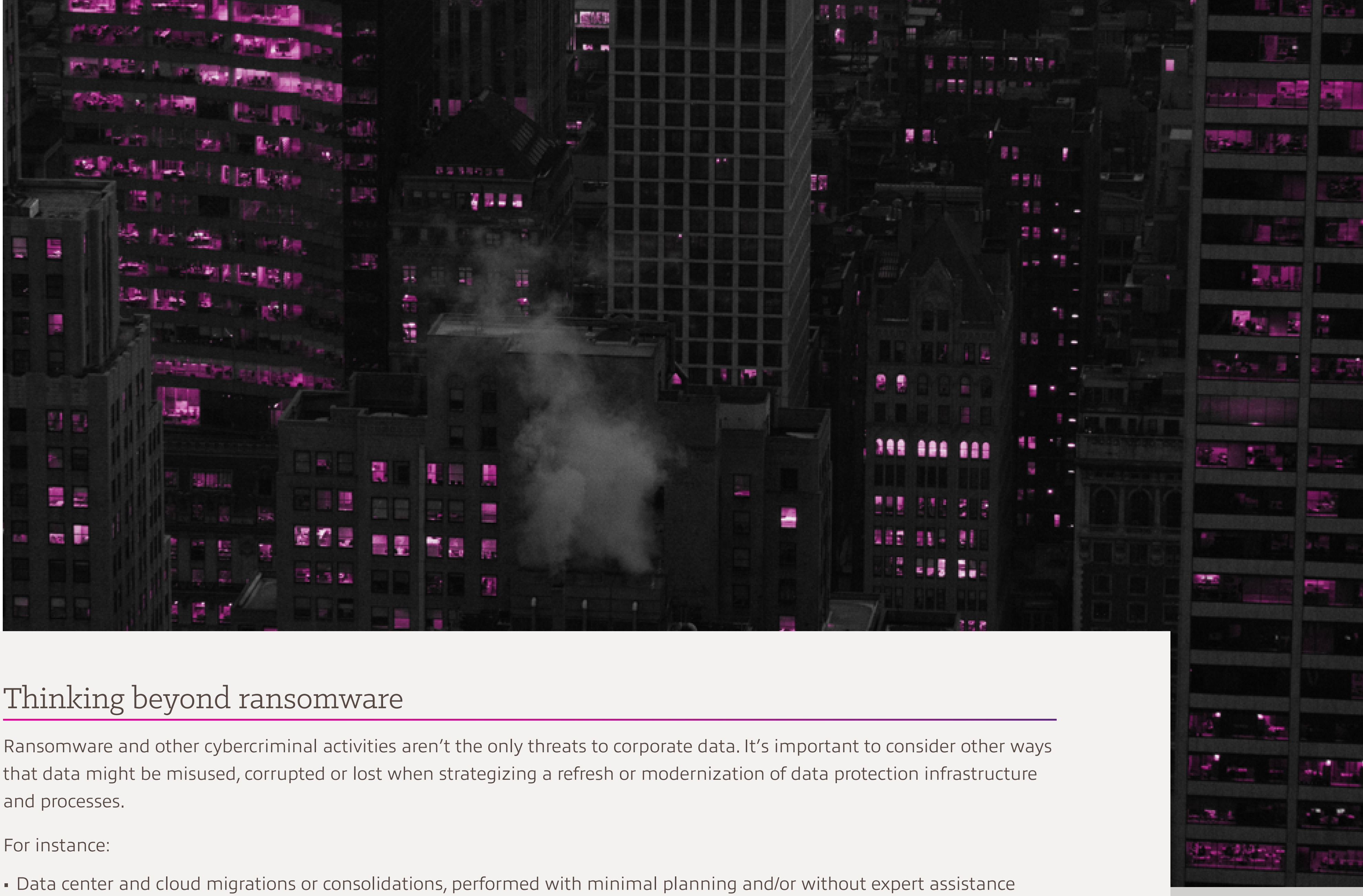
It's helpful to ask the following questions of your business:

- 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 to your organization's IT environment, business data and/or external environment should prompt changes to your 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

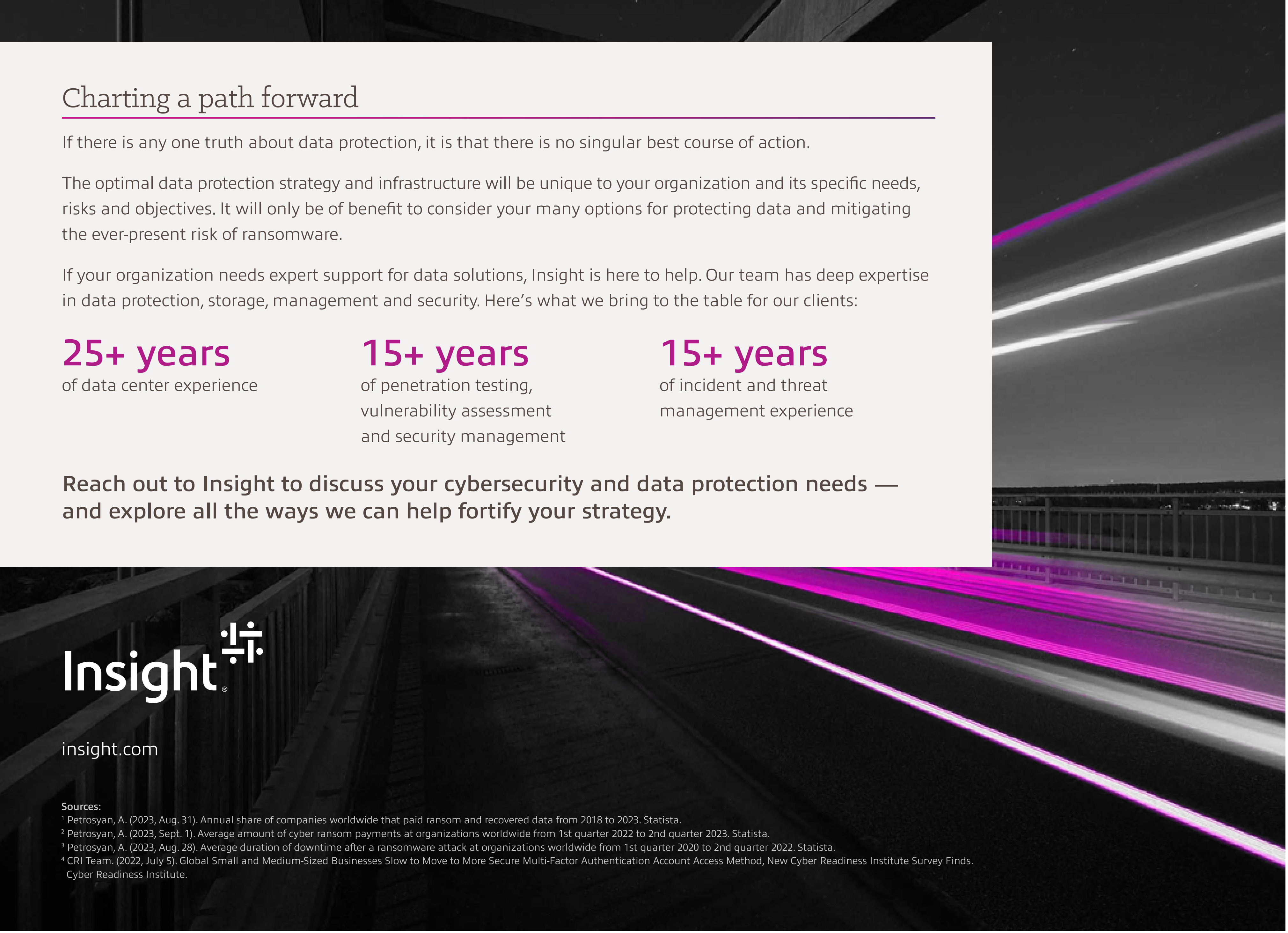


Thinking beyond ransomware

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
- 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 your organization needs expert support for data solutions, Insight is here to help. Our team has deep expertise in data protection, storage, management and security. Here's what we bring to the table for our clients:

25+ years
of data center experience

15+ years
of penetration testing, vulnerability assessment and security management

15+ 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.

Insight

insight.com

Sources:

[1] Petrosyan, A. (2023, Aug. 31). Annual share of companies worldwide that paid ransom and recovered data from 2018 to 2023. Statista.

[2] Petrosyan, A. (2023, Sept. 1). Average amount of cyber ransom payments at organizations worldwide from 1st quarter 2022 to 2nd quarter 2023. Statista.

[3] Petrosyan, A. (2023, Aug. 28). Average duration of downtime after a ransomware attack at organizations worldwide from 1st quarter 2020 to 2nd quarter 2022. Statista.

[4] CRI Team. (2022, July 5). Global Small and Medium-Sized Businesses Slow to Move to More Secure Multi-Factor Authentication Account Access Method, New Cyber Readiness Institute Survey Finds. Cyber Readiness Institute.