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

As the world continues to recalibrate and recentre 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 organisations experienced ransomware attacks in 2020.[1]

And ransomware isn't just becoming more prevalent — it's becoming more sophisticated and targeted. Of the organisations 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 organisations 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 organisations 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 organisations determine how best to protect data, manage risk, and care for sensitive data.

As part of the EU Cybersecurity strategy, the European Commission proposed the EU Network and Information Security Directive (the NIS Directive). Adopted in 2016, this is the first piece of EU-wide cybersecurity legislation, and every EU member state has started to adopt national legislation, which follows or 'transposes' the directive.

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 organisation 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 minimised.

Organisations 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 organisation for several months to learn about those environments, then delete and/or compromise them. Modernising your data protection infrastructure and processes can greatly help defend against these types of attacks.

No business is safe.

Organisations across industries have suffered crippling ransomware attacks.

European oil facilities

IT systems were disrupted at Oiltanking in Germany on 28 January 2022 after being hit with a cyberattack that also impacted its supply chain. SEA-Invest in Belgium and Evos in the Netherlands were also affected by similar attacks.

Oiltanking is one of the largest independent partners of tank terminals for oils and biofuels in Germany. It owns and operates a portfolio of terminals with a total storage capacity of 2.375 million cbm. The total throughput of all its terminals in 2020 was around 18.2 million tonnes.

- The company was forced to operate at a limited capacity whilst they investigated the incident.
- A total of 13 distribution terminals across Germany were impacted. Shell diverted its operations to alternative suppliers to minimise the impact on its own supplies.
- It's thought that all companies were affected because they use the same software for operations that may have been compromised by hackers.[4]

Public health & social care

On 14 May 2021, Ireland's Department of Health and Health Service Executive (HSE) was impacted by a human-operated 'Conti' ransomware attack.

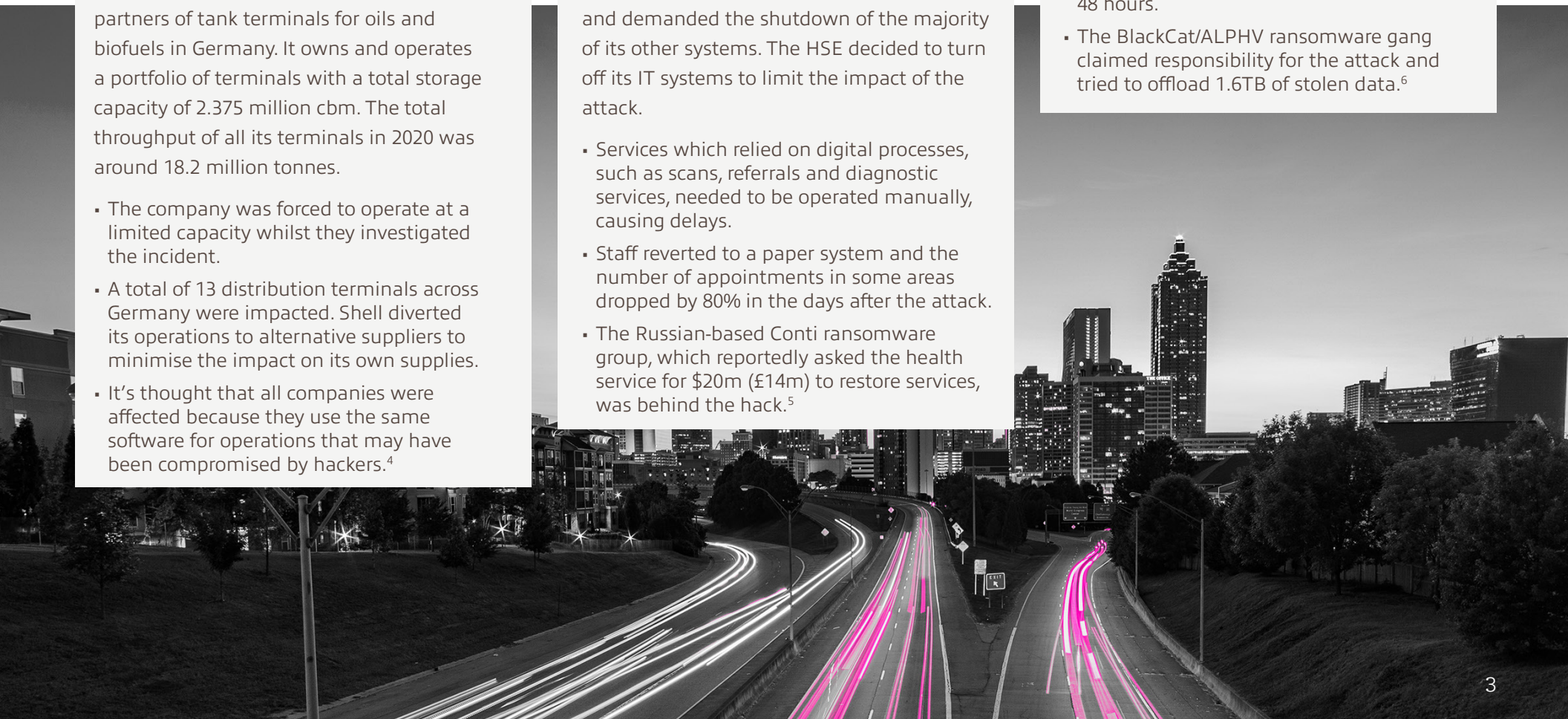
Malicious cyber activity was detected on the Department of Health's network which severely disabled a number of HSE systems and demanded the shutdown of the majority of its other systems. The HSE decided to turn off its IT systems to limit the impact of the attack.

- Services which relied on digital processes, such as scans, referrals and diagnostic services, needed to be operated manually, causing delays.
- Staff reverted to a paper system and the number of appointments in some areas dropped by 80% in the days after the attack.
- The Russian-based Conti ransomware group, which reportedly asked the health service for $20m (£14m) to restore services, was behind the hack.[5]

Swiss aviation services company

Aviation services company, Swissport, was the victim of a ransomware attack on 4 February 2022, with some flights forced into delays and other operations disrupted.

- A small umber of flights were delayed by 3 to 20 minutes.
- The incident was contained within 48 hours.
- The BlackCat/ALPHV ransomware gang claimed responsibility for the attack and tried to offload 1.6TB of stolen data.[6]



Missteps and missed opportunities

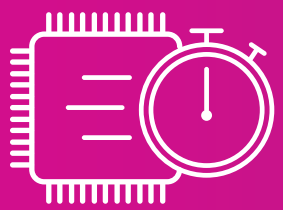
The issue of ransomware is multifaceted — and part of the problem is the integrity of data protection infrastructure.

Organisations 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 cognisant of and work to avoid.

1 Lack of extensive testing

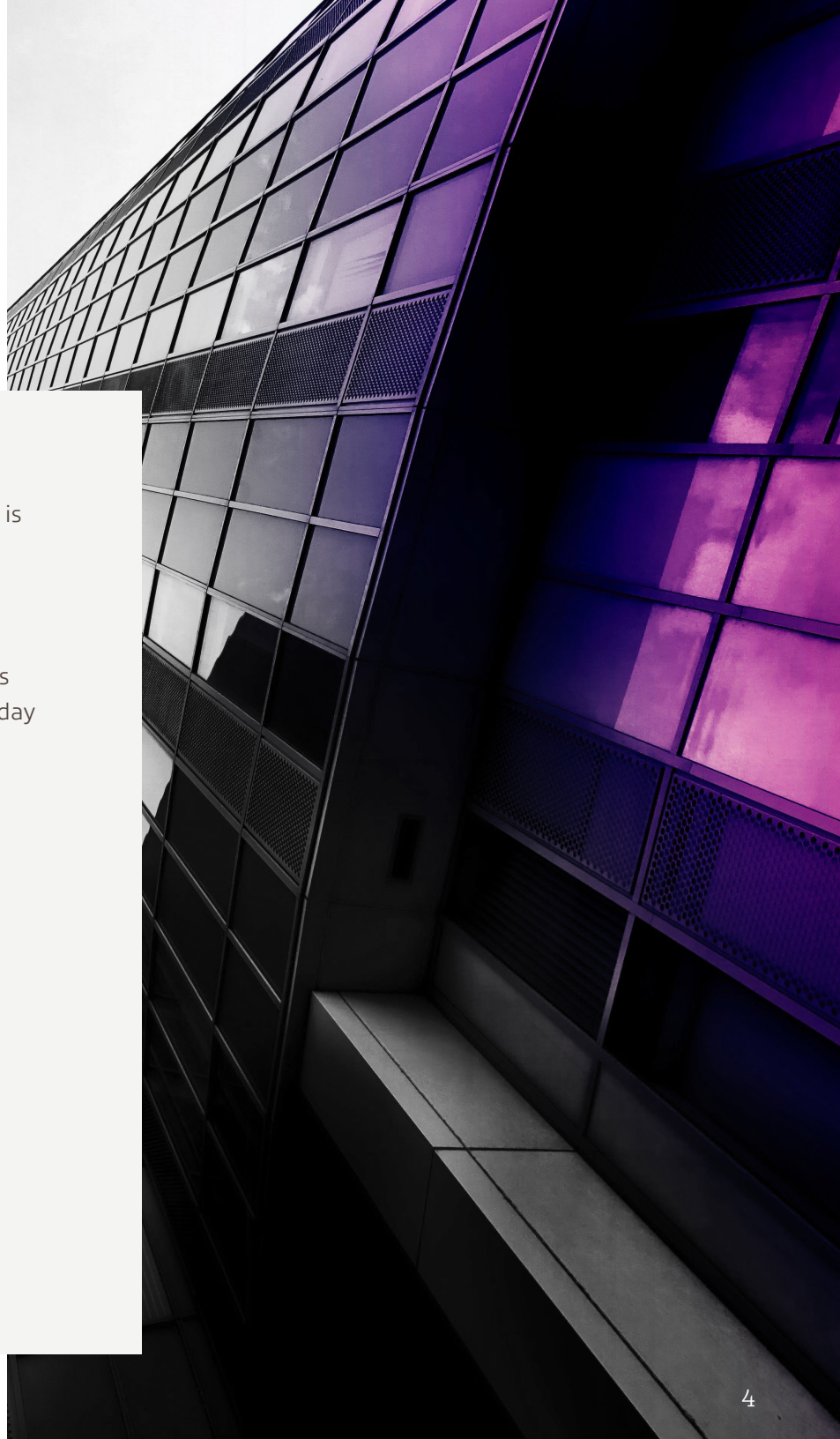
When a bad actor infiltrates a system and a ransomware event occurs, timing is everything — how long will it take for the organisation to get back online?

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 organisations 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

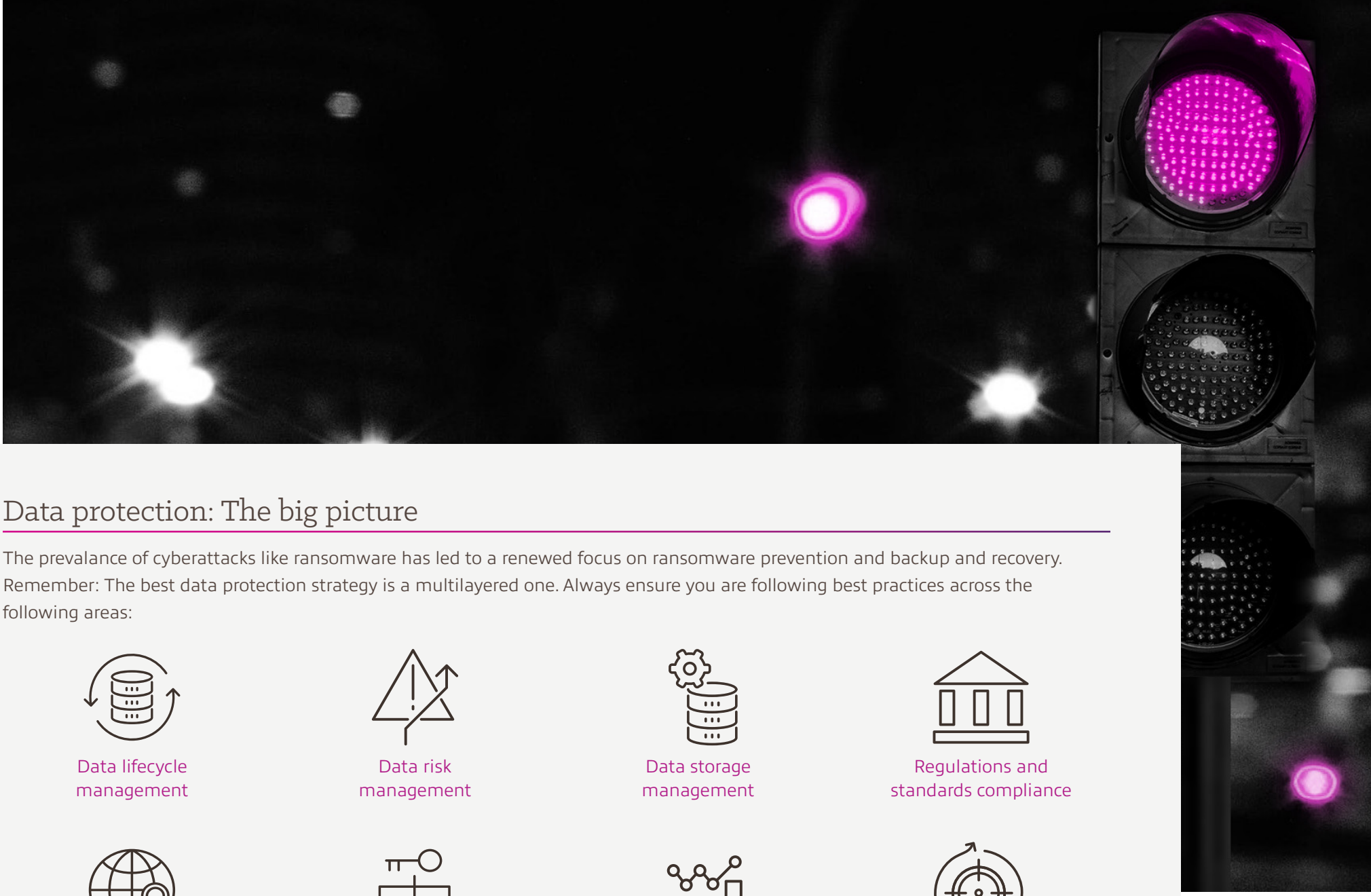
Many products claim to singlehandedly stop ransomware. This simply isn't possible. There is no point solution that addresses all aspects of ransomware prevention and response.

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 minimisation (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.

Organisations 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 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

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

01. A security team mindset shift

Security teams play a key role in defending an organisation against cyberattacks, but programmatic approaches have become critical. Organisations 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 realise more business outcomes.

02. Tape for air-gapped backups

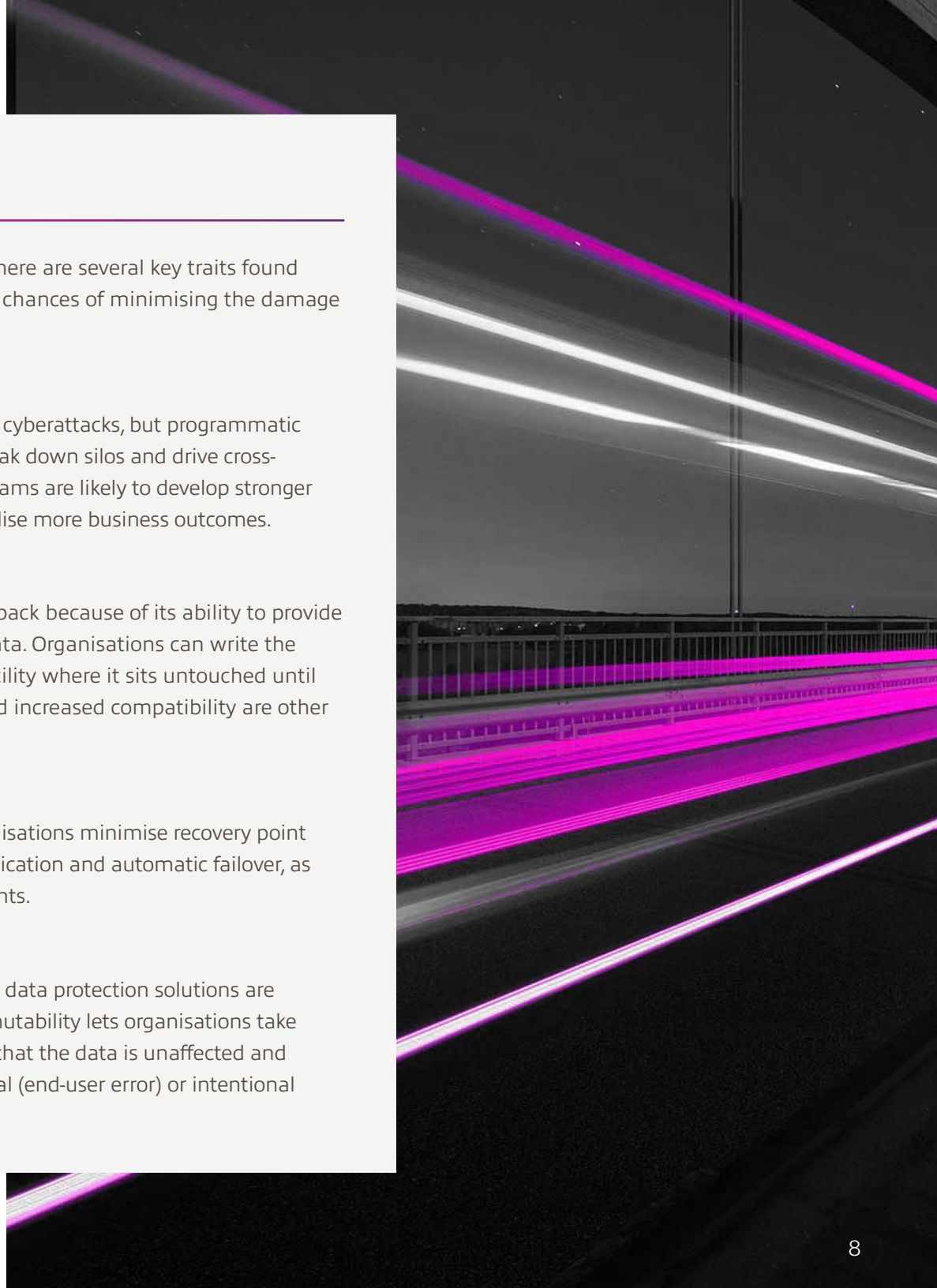
There are many ways to back up data. But tape is making a comeback because of its ability to provide an air gap — a completely offline, inaccessible copy of sensitive data. Organisations can write the copy, physically handle the tape, and ship it to a secure storage facility where it sits untouched until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

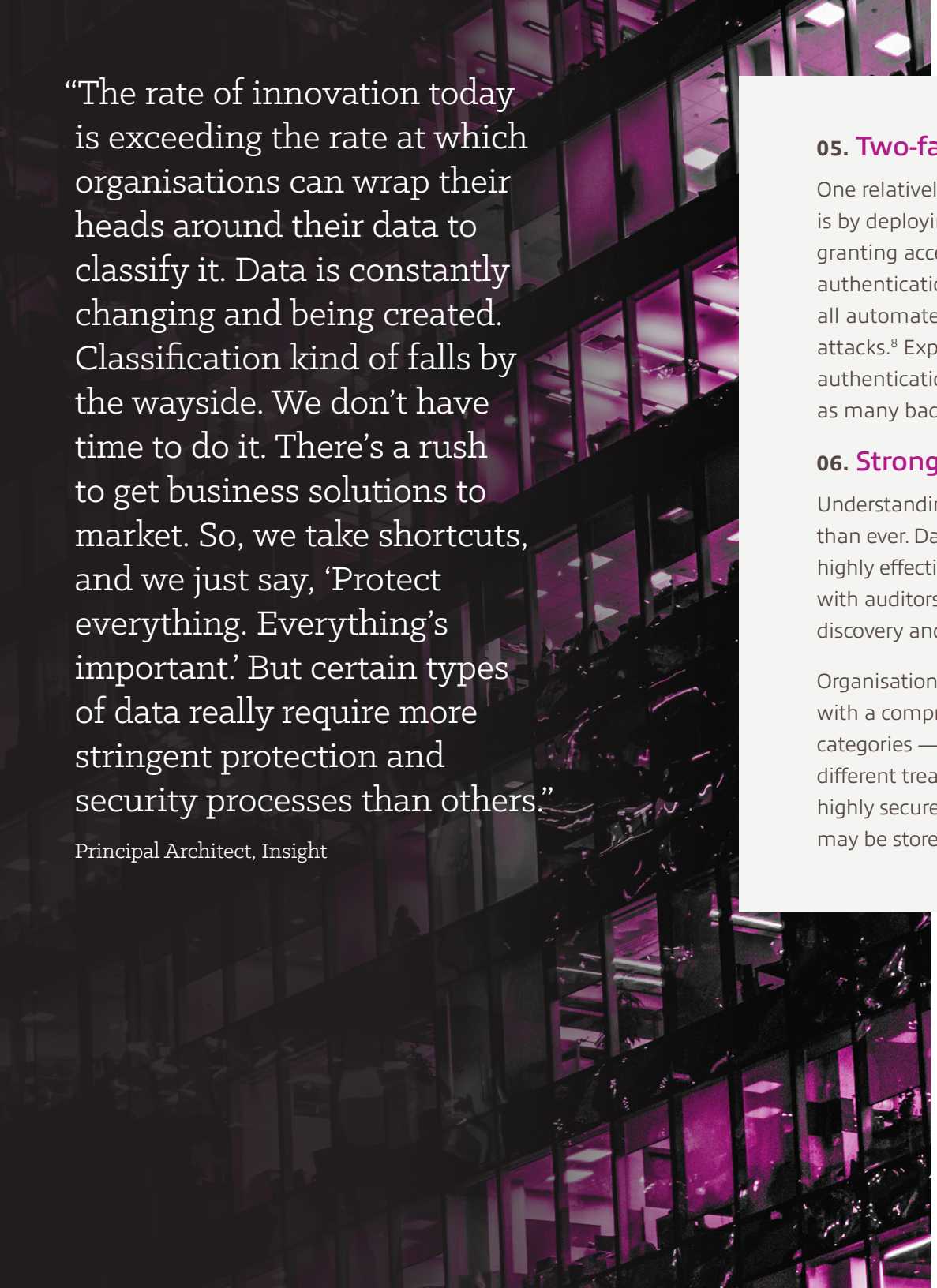
03. All-flash

Flash storage is another backup storage option that's helping organisations minimise 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 organisations 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.





"The rate of innovation today is exceeding the rate at which organisations 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 organisations 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 organisations may avoid discovery and classification because it's a considerable undertaking.

Organisations 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 organisations 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 centre has been encrypted, as is the case with a ransomware attack. Data should be replicated to a secondary data centre — 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 organisation'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:

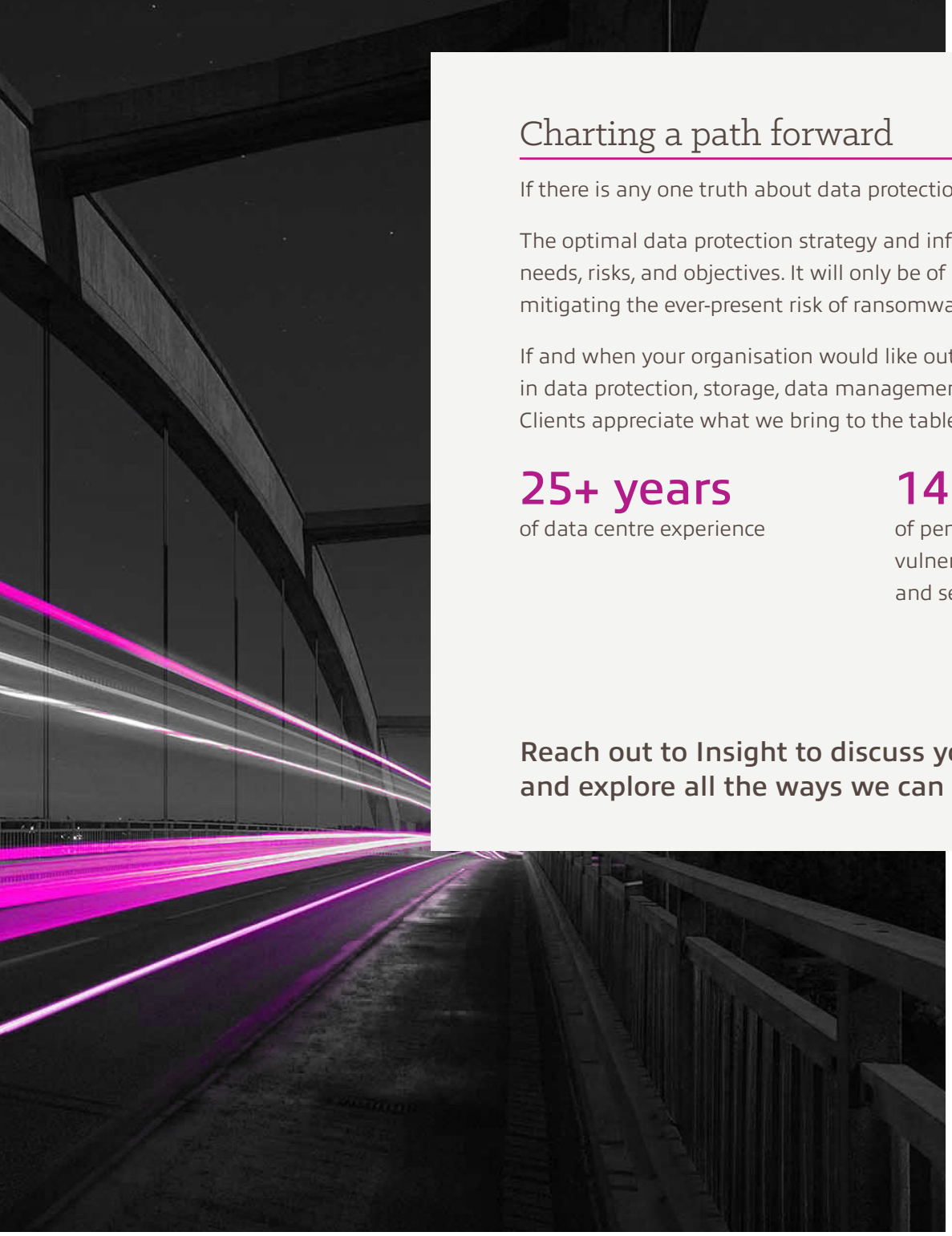
- Regular data discovery and classification
- End-user security awareness training
- Methodology testing
- Infrastructure modernisation
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) reviews and updates

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 strategising a refresh or modernisation of data protection infrastructure and processes.

For instance:

- Data centre and cloud migrations or consolidations, performed with minimal planning and/or without expert assistance
- Intentional or unintentional unauthorised 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 organisation 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.

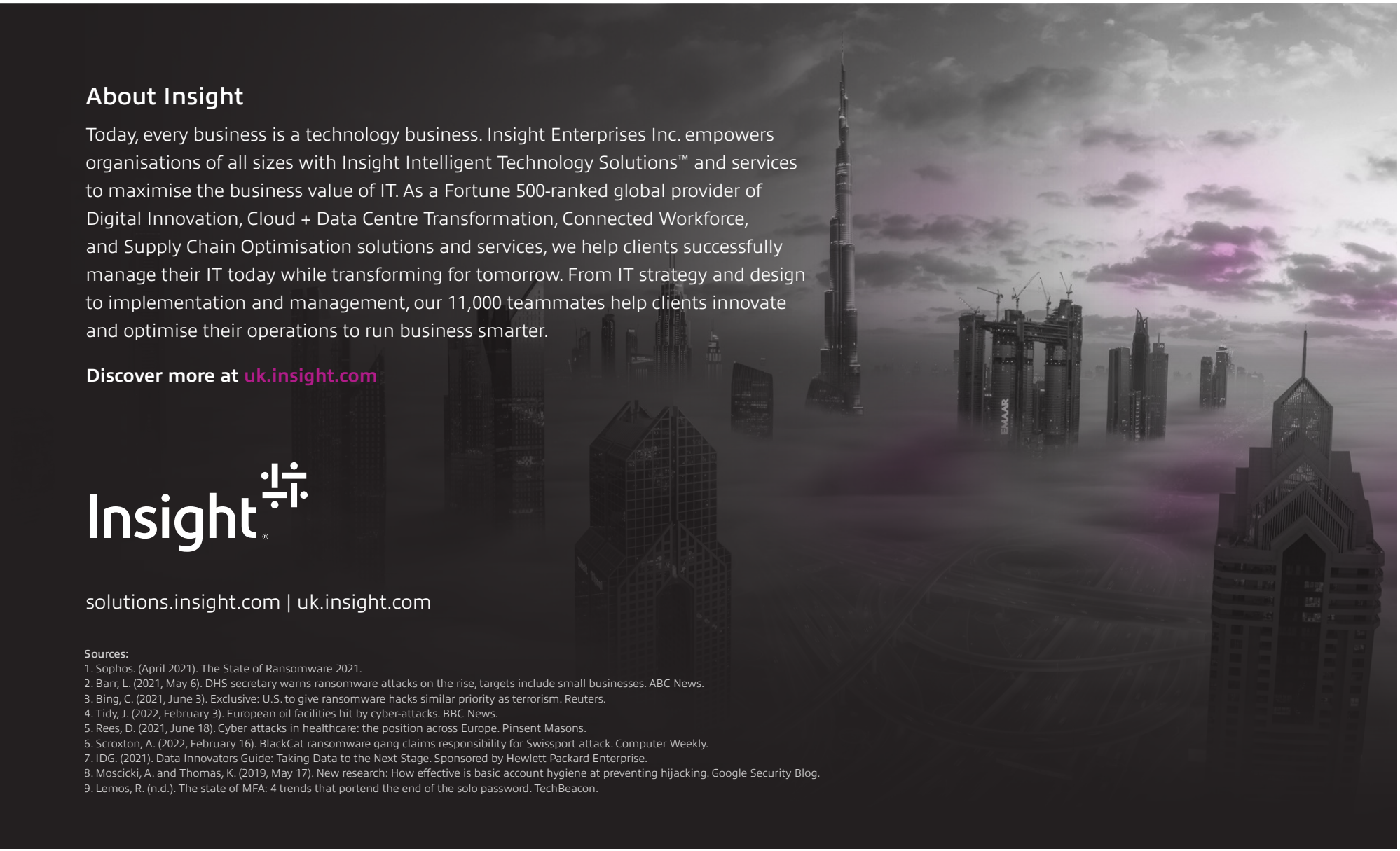
If and when your organisation would like outside support, Insight is here to help. Our team has deep expertise in data protection, storage, data management, and security across the entire NIST Cybersecurity Framework. Clients appreciate what we bring to the table:

25+ years
of data centre 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.



About Insight

Today, every business is a technology business. Insight Enterprises Inc. empowers organisations of all sizes with Insight Intelligent Technology Solutions™ and services to maximise the business value of IT. As a Fortune 500-ranked global provider of Digital Innovation, Cloud + Data Centre Transformation, Connected Workforce, and Supply Chain Optimisation solutions and services, we help clients successfully manage their IT today while transforming for tomorrow. From IT strategy and design to implementation and management, our 11,000 teammates help clients innovate and optimise their operations to run business smarter.

Discover more at uk.insight.com

Insight®

solutions.insight.com | uk.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. Tidy, J. (2022, February 3). European oil facilities hit by cyber-attacks. BBC News.
5. Rees, D. (2021, June 18). Cyber attacks in healthcare: the position across Europe. Pinsent Masons.
6. Scroxton, A. (2022, February 16). BlackCat ransomware gang claims responsibility for Swissport attack. Computer Weekly.
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.

MKT6302