Ransomware Readiness Best Practices

Insight

A brief history of ransomware

From the early days of the locker-based trojan attacks originating in 1989, ransomware has gone from a low-level concern to a top cybersecurity threat. With encryption joining the attack strategy in the early 2000s, ransomware took off, evolving even more rapidly between 2010 and 2020.

This growth spurt occurred in part because of the emergence of Bitcoin as a convenient method of ransom payment that protected the bad actors' anonymity, and in part because of the success of exfiltration-style attacks (also known as leakware or doxware), in which malicious actors threaten to go public with sensitive data unless ransom is paid.

Ransomware over five decades

1980s

The first known ransomware attack, a trojan horse, is launched.

1990s

Upticks in home PCs and email viruses bring cybersecurity to public awareness.

2000s

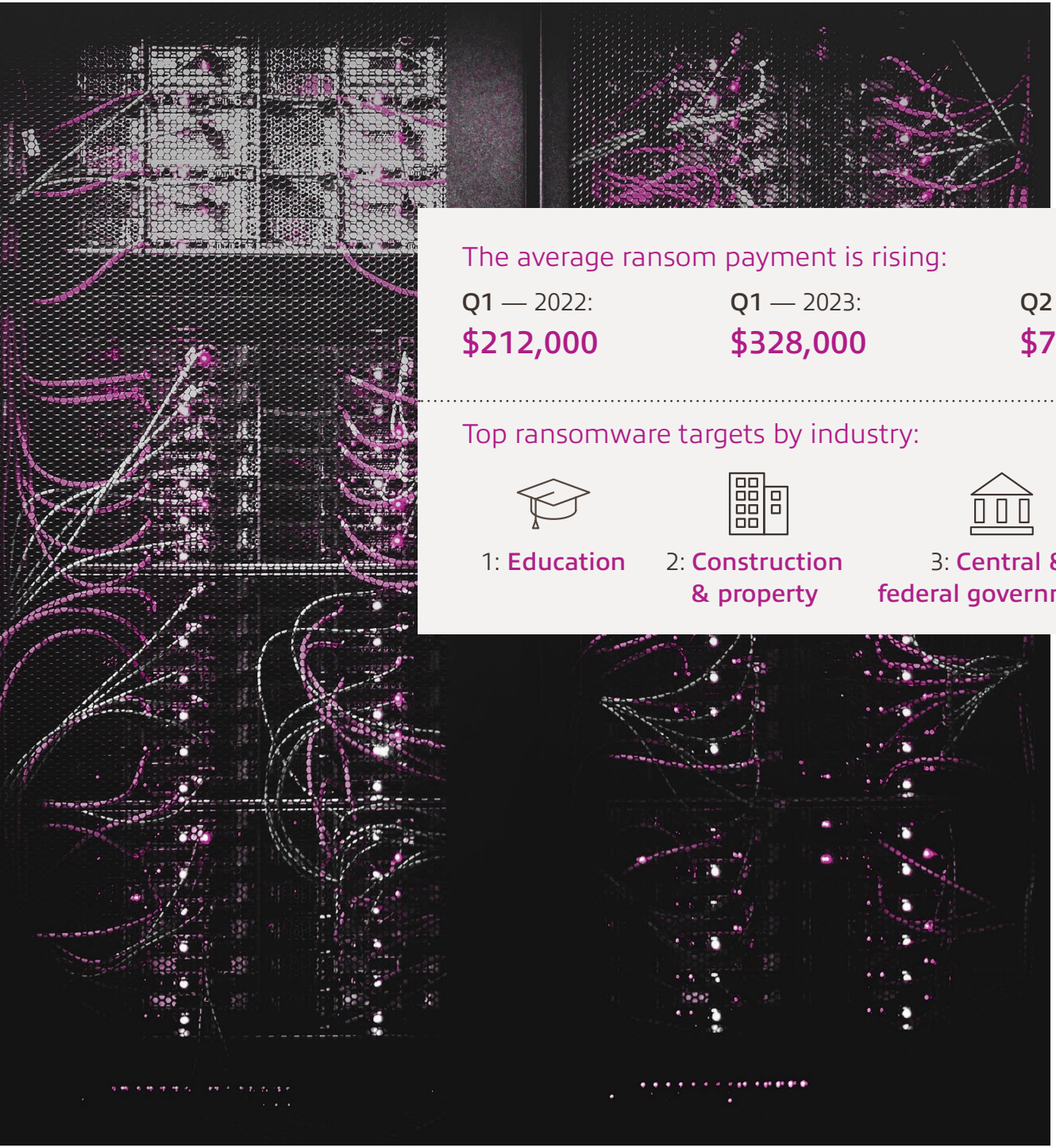
Bitcoin hits the market, making extortion simpler for malicious actors.

2010s

Exfiltration and extortion begin dominating ransomware strategy.

2020s

Cybersecurity jobs are among the fastest growing. Employment of information security analysts is projected to grow 32% between 2022 and 2032.[1]



Ransomware trends today

Today's ransomware attacks are stronger and more severe than ever before. As the number of impacted organizations grows, associated costs have skyrocketed.

The average ransom payment is rising:

Q1 — 2022:
$212,000

Q1 — 2023:
$328,000

Q2 — 2023:
$740,000[2]

Average downtime per attack **24** days[3]

Top ransomware targets by industry:

1: **Education**

2: **Construction & property**

3: **Central & federal government**[4]

73% of organizations worldwide paid ransom to recover data in 2023.[5]

Ransomware is an increasing threat that requires proactive strategy and a multilayered approach. Knowing the likelihood and financial ramifications of an attack is just the beginning.

Keep reading this guide to learn the primary components of effective ransomware readiness and response.

Know your vulnerabilities.

Ransomware preys on an organization's vulnerabilities to infiltrate the environment. There are two fundamental considerations to keep in mind when assessing your organization's vulnerabilities:

1. Risk exists in every layer of your IT environment.

Ransomware protection starts with taking a full-stack view of your entire infrastructure. It only takes one weak spot to let attackers in. Identifying and addressing existing security concerns at every level of your organization, from network security to backup architectures and beyond, should be top priority.

2. Human error is behind most successful ransomware attacks.

The prevalence of human error is so profound that most ransomware attacks depend on it. Even though ransomware has evolved, most attacks still rely on an end user to accidentally provide credentials or click to activate a malicious program.

While it may never be possible to solve the problem of human error entirely, it is possible to minimize your risks and fill the gaps with properly built architectures and properly implemented security protocols across your organization.

How to: Mitigate security incidents with confidence and efficiency.

Cybersecurity attacks can lead to the loss or disruption of critical assets or business functions. A robust security strategy is more important than ever to stay ahead of bad actors. Read our expert guide to incident response to learn 11 best practices for handling modern threats.

Secure your data.

Considerations for securing your data start with understanding what it is you're trying to protect. The prevalence of exfiltration attacks can be tied to the increasing value of data and the growing amounts of sensitive data generated, stored and used by high-risk organizations.

Data immutability is another point to consider — that is, creating data that can't be changed once written. The term comes up often in conversations about ransomware. In theory, it's a practical solution. In practice, it can be difficult to achieve. Especially when your attackers are leveraging access to internal controls to compromise your backup environments — but more on that in the next section.

Because of the difficulty of true data immutability, it's critical to ensure your data protection platform is secure. While this consideration is still important for on-premises data, organizations need to take extra care to protect data stored in the cloud.

There's a common assumption that data is automatically safer in the cloud. This couldn't be further from the truth. Cloud service agreements often specifically recommend you employ a third-party source for data protection. Remember: You're responsible for your data.

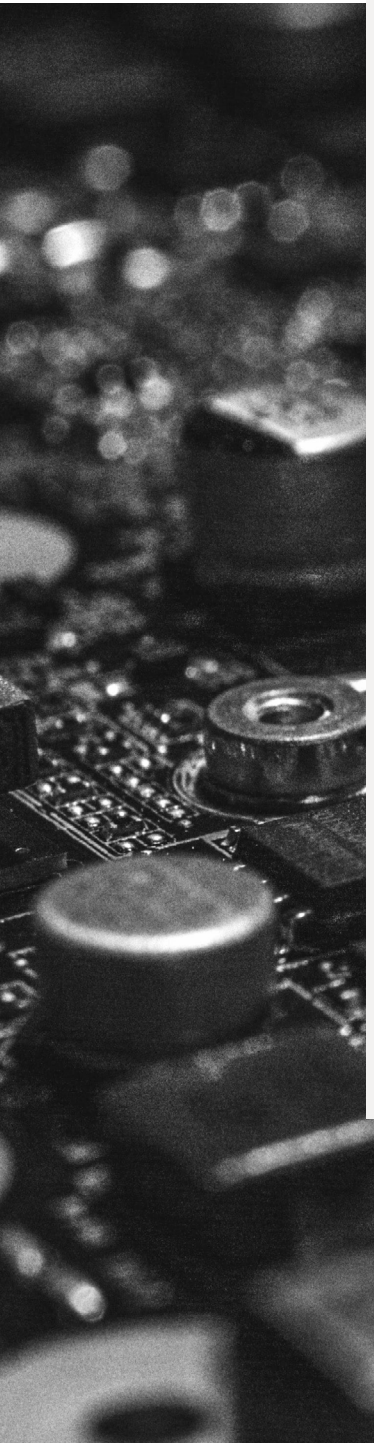
Take a data-focused approach and ask:

"What kind of data am I dealing with?"

"Where does this data live?"

"How are we protecting it?"

When you can answer all of those questions, you'll have a much stronger foundation for moving forward.



Back up your backups.

For a long time, data backups have been considered the primary plan in case of an attack. Now? Backups are where the attackers are choosing to start. It works something like this: Your backup software and architecture are great; you think you're protected. Then, someone in your organization slips up. As a result, an attacker has admin credentials. With those credentials, they can spend time in your environment, learning your backup process, and then attacking the backups before unleashing their ransomware. Now your failsafe is gone, and you're much likelier to pay the ransom to unencrypt your remaining data.

> "I've had customers who did all the right steps as far as having backup appliances, having data replicated between two data centers, etc. But it wasn't really the backup software or the appliances themselves that posed a problem. It was either a default password, or somebody was able to compromise the admin credentials. **They got in there and basically wiped the backup appliances and then set loose the ransomware.**"
>
> — **Data Protection Solutions Architect**, Insight

Backups alone aren't enough, and backups in the cloud don't mean your data is secure. Backups were safer back when networks and physical perimeters were easier to secure. But with the evolution of work from home and Internet of Things (IoT), perimeters are harder to define and secure, making it even more important to audit your backup environments and have appropriate data isolation/air gap strategies in place.

Tips for data protection:

- Keep multiple copies of your data.
- Span multiple media types.
- Store data in multiple locations, preferably including off-site.

Have a plan — then test, modify and practice it.

There are many things you can do to reduce your risk of ransomware attacks, but there's no way to completely prevent them. The best course of action is to prepare as if you're certain you'll experience a data breach because — statistically speaking — it's likely.

> "The assumption should be that it's not if, it's when. So, are we prepared, and what are we going to do?"
>
> — **Lead Architect**, Insight

Planning

Developing a disaster recovery plan is a critical, and often overlooked, piece of the ransomware puzzle. From network security considerations to legal implications, evaluate all the potential impacts of a ransomware event and determine a plan of action. You can collaborate with security service professionals to create a customized, actionable incident response plan. Too many organizations have limited remediation plans that exist only in someone's brain somewhere. It's also important that the plan is well documented and extends to your entire organization.

Testing

Just as important as developing a plan is testing it. Test your plan in your current environment for any flaws, adjusting as necessary, and practicing it on a timely basis, continuing to revise as needed. This not only ensures that internal teams are ready to respond quickly and effectively in case of an event, but that your plan is up to date and optimally positioned for best results.

Education

With human error at the top of the ransomware chain reaction, education can't be overlooked. All individuals within an organization should receive basic training on ransomware, particularly how to spot and report phishing attempts.

Ransomware is ready. Are you?

Every organization's approach to ransomware will be unique. An effective strategy will take into account several factors, including the quantity and nature of your data as well as the complexity of your IT infrastructures.

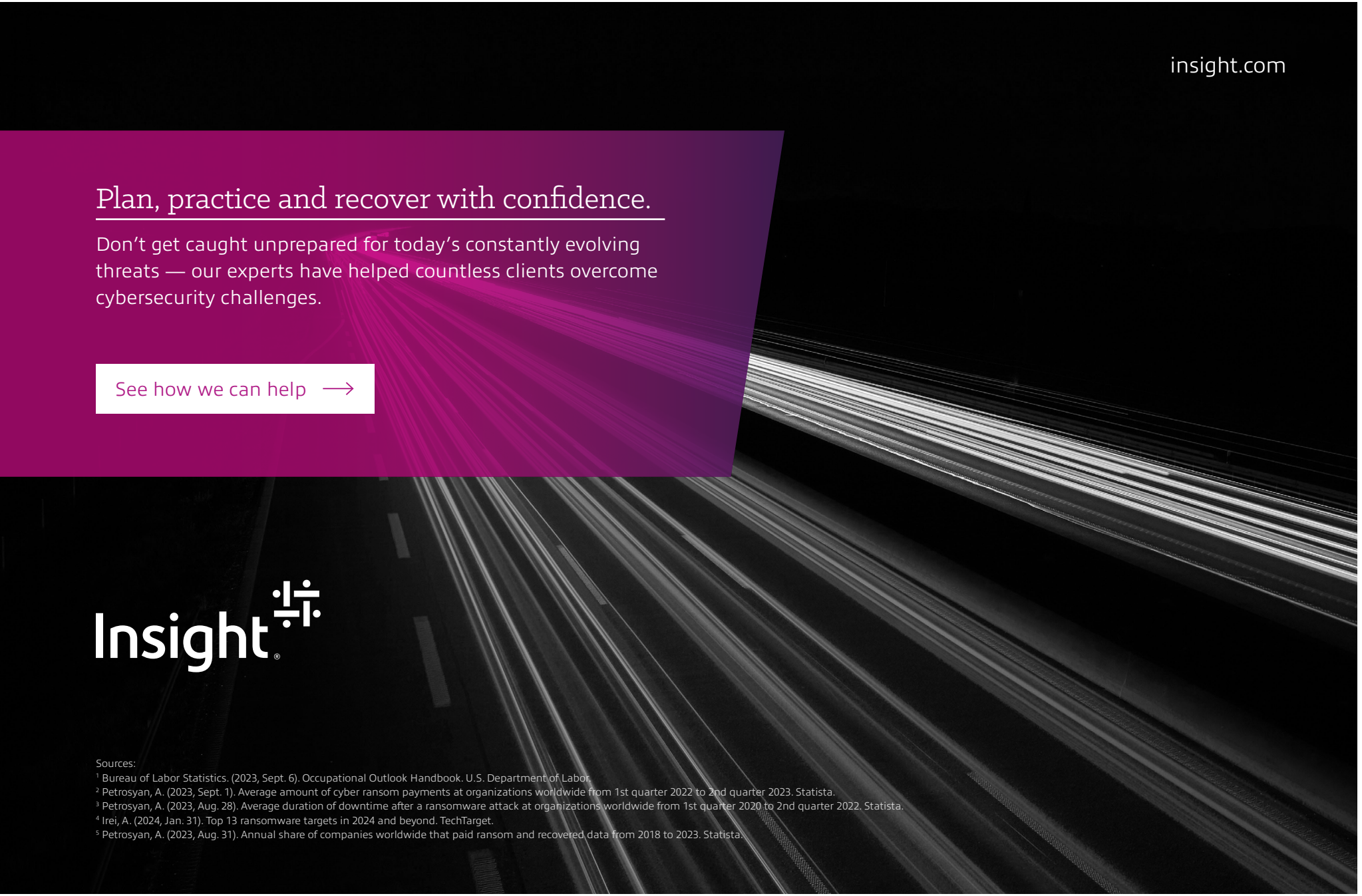
Insight can help you evaluate your current security stance in light of the evolving threat of ransomware, working with you to develop a holistic approach to cybersecurity that protects every layer of your IT environment and matches your organization's specific needs.

If you're ready to talk about ways to improve your organization's ransomware readiness, contact us.

Related resources:

Webinar: Maximize Your Cloud Security — Discover managed security solutions and services available from Insight and Microsoft to help you secure your data in the cloud.

Solution brief: Ransomware Readiness Scorecard — Learn how you can increase confidence in your security posture with a Ransomware Readiness Scorecard assessment from Insight.



Sources:
[1] Bureau of Labor Statistics. (2023, Sept. 6). Occupational Outlook Handbook. U.S. Department of Labor.
[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] Irei, A. (2024, Jan. 31). Top 13 ransomware targets in 2024 and beyond. TechTarget.
[5] Petrosyan, A. (2023, Aug. 31). Annual share of companies worldwide that paid ransom and recovered data from 2018 to 2023. Statista.