stc

what a cyberattack really costs

a ransom is just the gust at the edge of a cyber sandstorm.

Bahrain is in the eye of the sandstorm, ranked among the most targeted countries for malware attacks in 2024.[1]

and the threat has evolved beyond traditional ransomware.

AI-powered attacks are accelerating:

deepfake technology enables sophisticated impersonation attacks

synthetic identities bypass traditional verification systems

fraud attempts using AI techniques surged 2,137% over the past three years

gone are the days when ransomware was simply about paying attackers to unlock your files.

the sophistication of threats means the cost landscape has grown more complex and more expensive.

the next pages expose what really happens after you pay, and what you can do to prepare.

cost 1: downtime

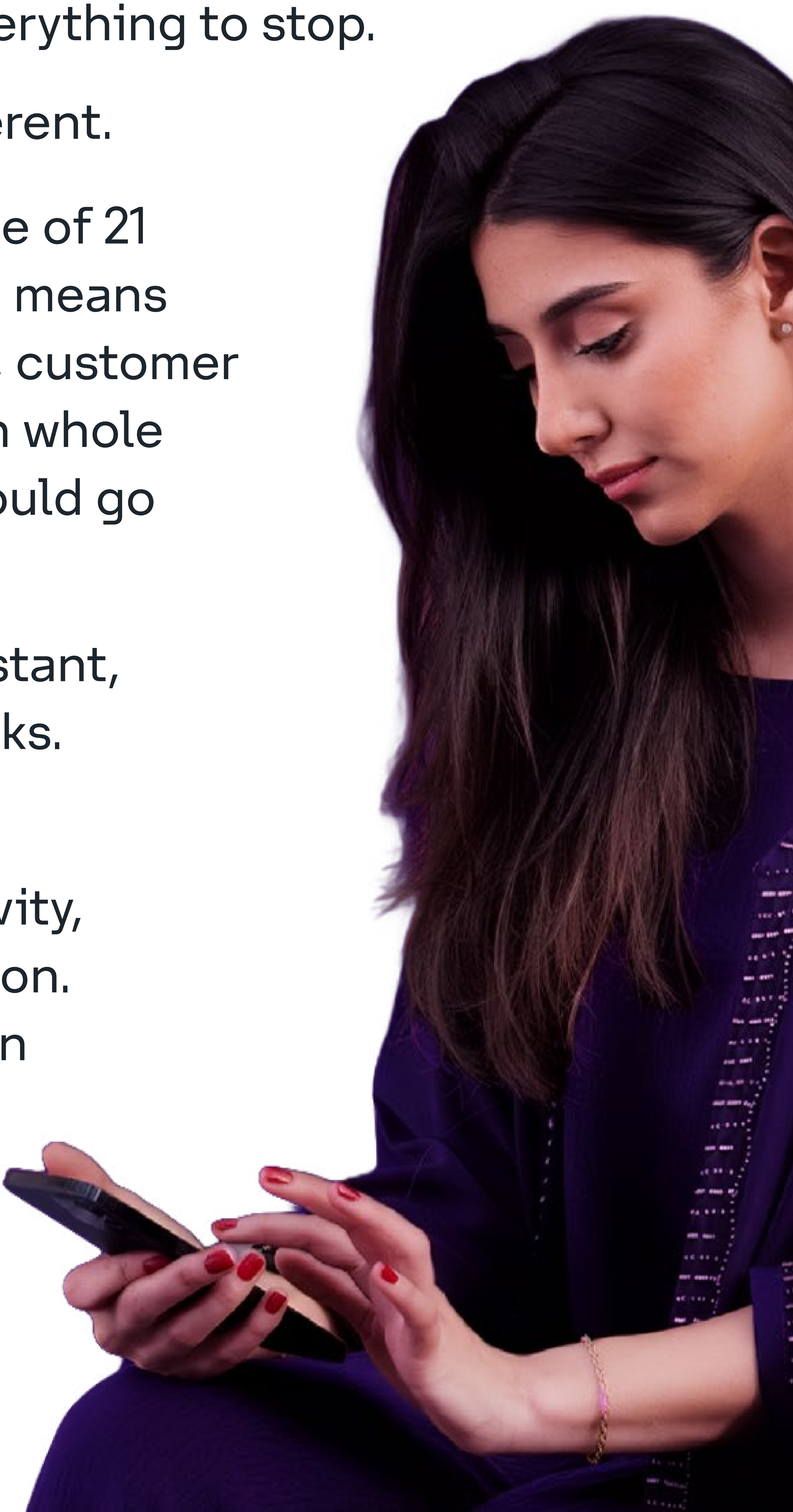
a sandstorm forces everything to stop.

ransomware is no different.

victims face an average of 21 days of downtime. this means your factories are idle, customer services halt, and even whole government portals could go offline.

recovery is far from instant, sometimes taking weeks.

every hour means lost revenue, lost productivity, and mounting disruption. in fact, downtime often eclipses the ransom amount.



estimated cost

for a typical mid-to-large enterprise, each hour of downtime can easily cost beyond USD $1 million in lost business[2]

cost 2: eroded trust

the notification that changes everything.

your customer learns about the breach through news reports, regulatory filings, or direct notifications.

the ramifications are brutal:

- 47% of customers stop buying from a hacked company[3]
- social media amplifies negative sentiment across industry networks
- recovery requires 3-5 years of sustained investment in brand rehabilitation, transparency initiatives, and enhanced security communications

estimated cost

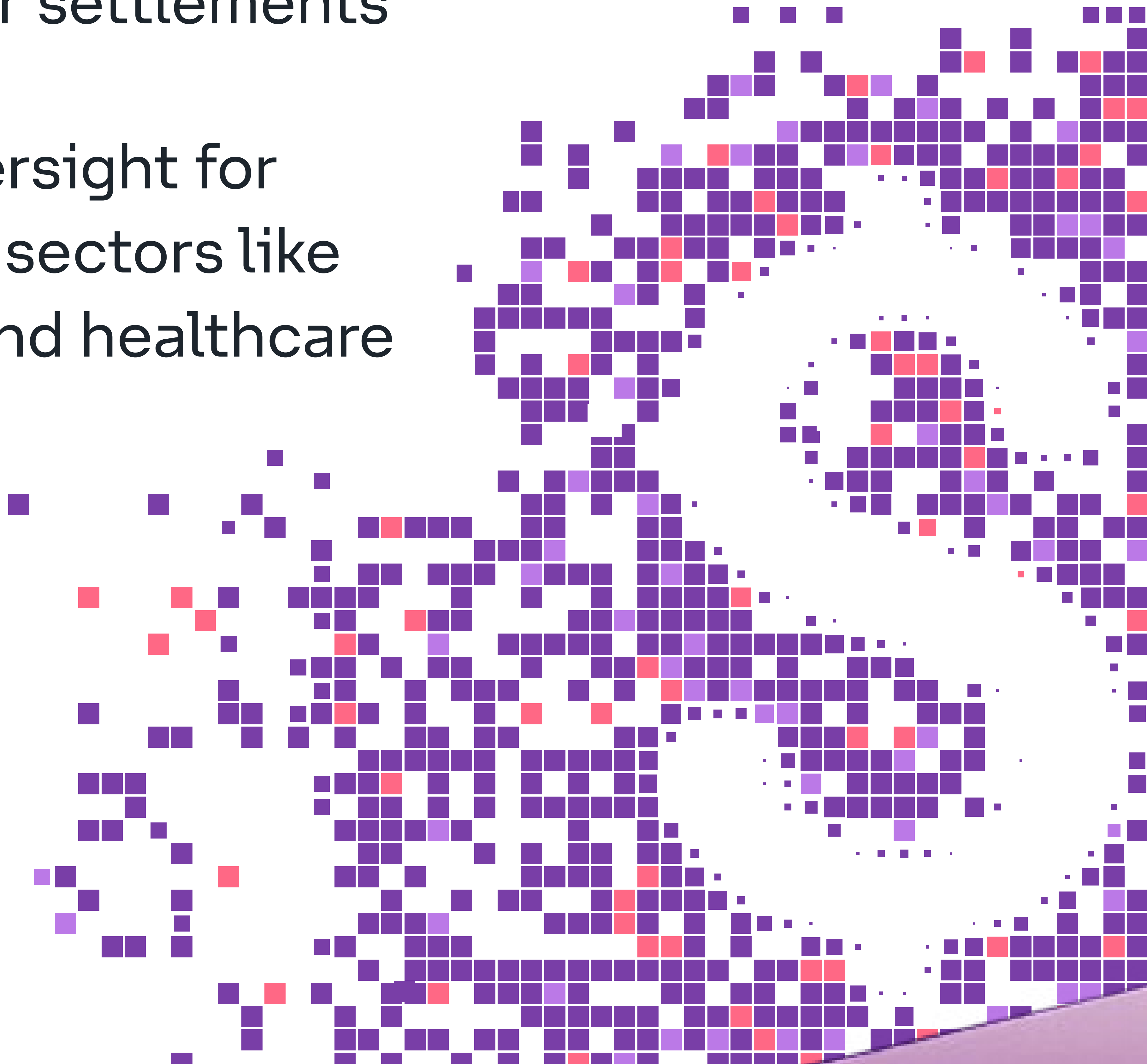
up to 20% of revenue lost
in customer exodus[4]

cost 3: regulatory reckoning

Bahrain's personal data protection law (PDPL) allows fines up to BD 20,000 ($53,000) per violation.[5]

that's before factoring in:

- compliance investigations by regulators
- potential class-action lawsuits or settlements
- added oversight for regulated sectors like banking and healthcare



estimated cost

USD $53,000 in fines[5]

cost 4: double extortion

today's ransomware also hides more than one storm: as well as encrypting systems, attackers steal and threaten to leak data.

key characteristics:

data theft – attackers copy sensitive files before encryption

ransomware-as-a-service (RaaS) – marketplaces rent ransomware tools to anyone, lowering the barrier to entry

targeted attacks – critical sectors (finance, energy, government) are priority targets where disruption hurts most

even if you recover from backups, you're still facing blackmail, leaks, lawsuits, and reputational fallout.

estimated cost

the global average cost of a data breach is USD $4.4 million[6]

cost 5: insurance fallout

after a ransomware incident, cyber insurance transforms from protection to problem:

- ransomware claims get rejected
- premium increases in subsequent renewals
- 56% will face increased scrutiny when renewal comes

estimated cost

premium increases of 50-300%, if renewal is even possible[7]

cost 6: cleanup

when the ransom is paid or systems are restored, the true cleanup begins.

operational

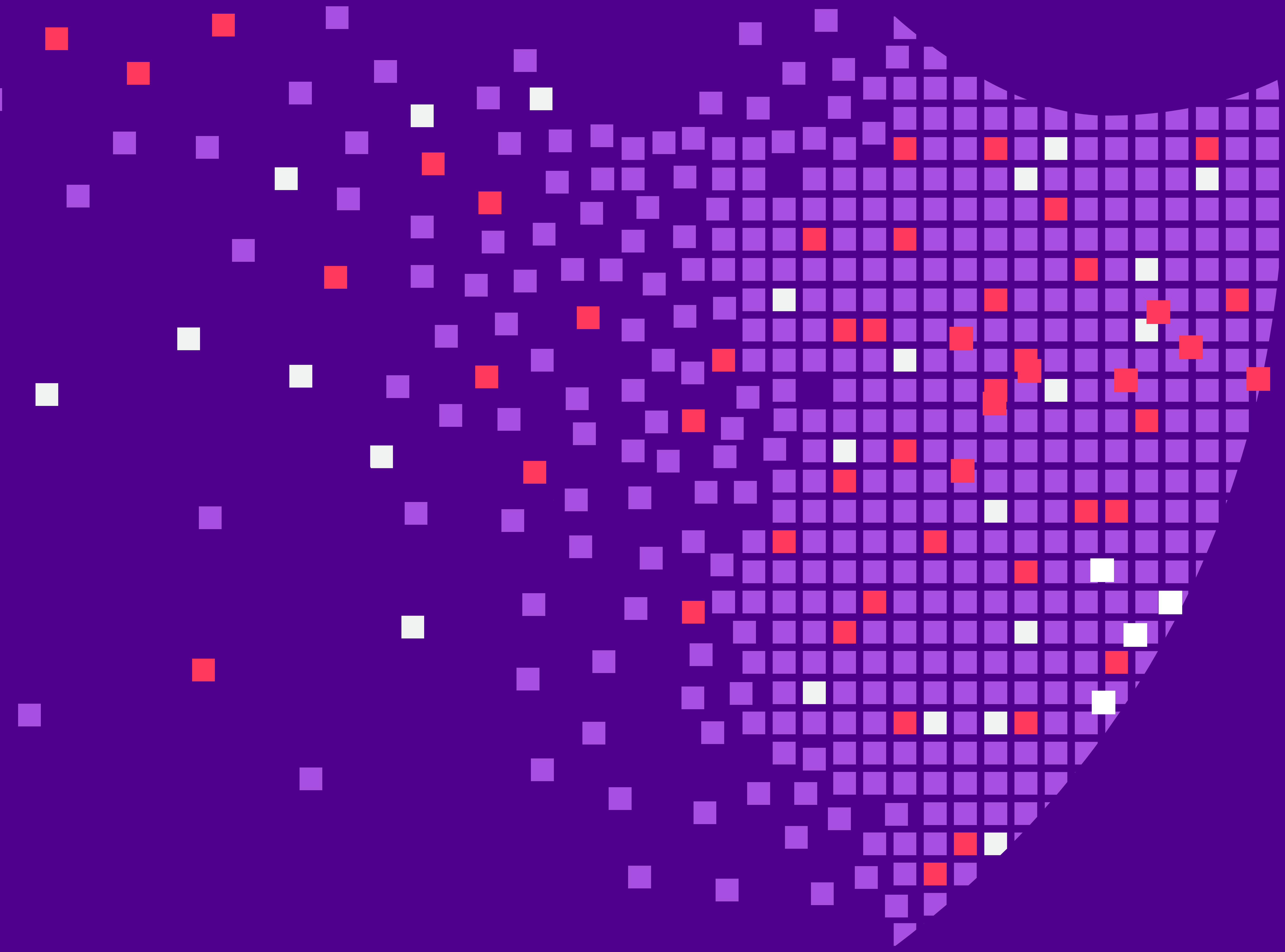
- infrastructure rebuilds from ground up
- system architecture redesign
- comprehensive staff retraining

reputational

- PR crisis management
- customer credit monitoring programs
- stakeholder communications campaigns

estimated cost

these hidden costs quietly add up to an average of USD $2.7 million[8]



preparedness pays

here's how stc Bahrain's AI-driven cyber defense centre helps:

- proactively monitors, hunts, and identifies threats early
- contains critical threats in 30 minutes or less
- deep forensic investigations to trace root causes and prevent repeats
- regulatory-ready reporting aligned with Bahrain's PDPL, NCSC baseline controls, and CBB cyber guidelines requirements
- free your teams to focus on strategy instead of 24/7 monitoring

don’t budget for ransoms. invest in immunity.

build resilience
with stc Bahrain.

references

[1] Acronis Cyber Threat Report

[2] How Downtime Drives up the Cost of a Ransomware Attack

[3] Nearly Half of Customers Stop Buying After a Hack

[4] What's the Damage? The Truth About the Cost of Data Breaches

[5] The role and responsibilities of the authority and penalities and sanctions.

[6] Cost of a Data Breach Report 2025

[7] Cyber Insurance Challenges: Why Premiums Are Rising, and Coverage Is Harder to Obtain

[8] Ransomware Payments Increase 500% In the Last Year, Finds Sophos State of Ransomware Report