Your Data Will be Stolen!

(Affirm cybersecurity experts)

By **Julian Murguia**, CTO
Omega Krypto
March 16, 2026

The world's leading cybersecurity experts agree that breaches are inevitable and affirm that it is no longer **if** your organization will be breached but **when** will it happen and **how often**.

Add to this that the Microsoft Digital Defense Report 2025 clearly states that data collection was the primary objective in 80% of all 2025 cyberattacks; and your worst nightmare becomes true when you realize that data theft is also inevitable.

The IBM Cost of a Data Breach Report 2025 confirms that *breaches occur despite strong preventive controls*. As digital dependency grows, attacks become more frequent, more sophisticated, and more costly. And the use of Artificial Intelligence by the attackers is just get things much worse!

According to TotalAssure, the *average mean time to detect a breach in 2025 was 181 days*, while according to Palo Alto Networks' Unit 42 Global Incident Response Report 2025, *it took attackers as little as 72 minutes to exfiltrate data*.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

The feeling that your organization is already in death row, waiting for the inevitable day it will be breached and your sensitive data be stolen, gnaws your heart and mind, fearing it may bring your organization to collapse and cease to exist.

Under this mindset, the damage caused by stolen data will never be solved—because defeat has already been accepted.

What other than defeat admittance is it when they tell you that breaches (and data theft) are inevitable?

As a result, cybersecurity strategy has shifted from pure prevention to resilience: detect faster, respond quicker, recover sooner, mitigate as much as possible.

But resilience has a critical blind spot:

Some damages simply cannot be mitigated!

If a cyberattack disables critical medical devices in a hospital and patients die as a result, no mitigation strategy can undo such loss.

Death is irreversible and so is data theft.

Once outsiders have your sensitive data, the damage is already done. The data is copied, retained, and exploitable indefinitely.

It does not matter how fast a breach is detected, if detection happens after data exfiltration, it is already too late.

Recovery can restore systems—but it cannot erase stolen information from the attacker's possession.

Systems can be rebuilt, operations can resume, ransomware can sometimes be avoided, but stolen data retains 100% of its value and remains fully usable.

Even if a ransom is paid and systems are restored, attackers still retain the stolen data. The long-tail cost of breaches often persists for years, crippling organizations—or forcing them out of business entirely.

Cybersecurity operates in an asymmetrical battlefield. Attackers need only one weakness—human error, credential theft, insider access, supply-chain compromise. Defenders must secure everything, all the time.

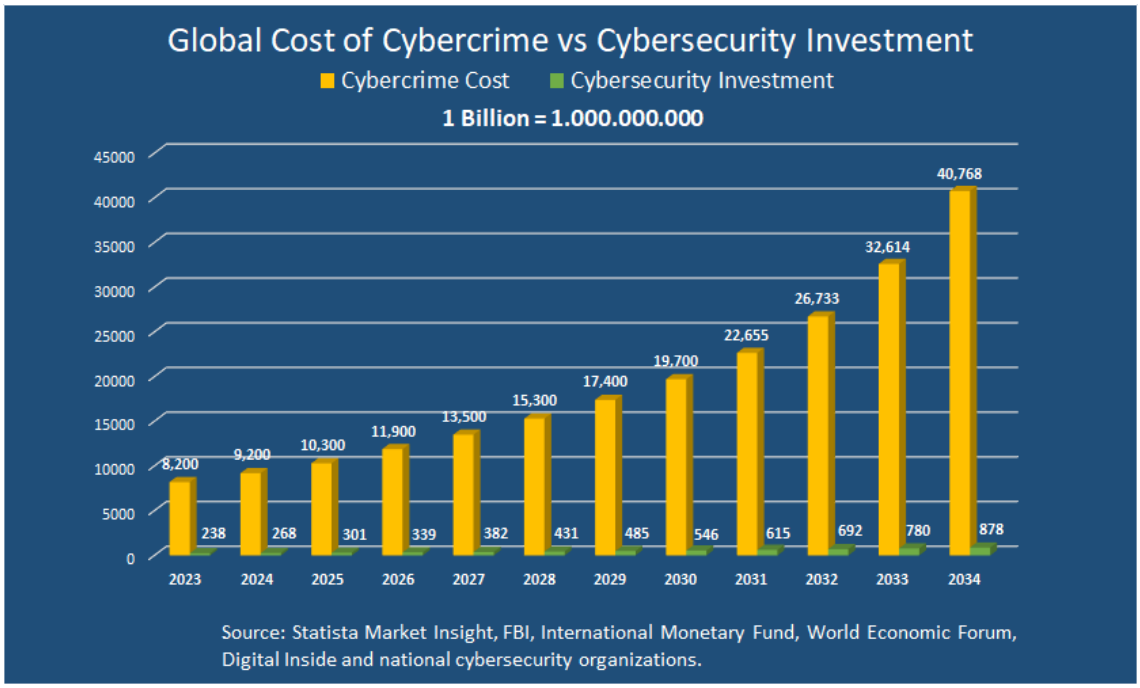
This is not a failure of cybersecurity, it is the nature of the threat landscape.

The ugly truth: Global cybersecurity investment in 2025 was about 301 Billion US Dollars, while the global cost of cybercrime for the same year was about

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

10.3 Trillion US Dollars (over 34 times bigger), positioning cybercrime as the third-largest global economy (behind United States and China).

The projections for how this battle will evolve are ominous:



Global Cybercrime Annual Cost vs Global Cybersecurity Annual Investment - Years 2023 to 2034

It is a fact that cybersecurity fails to stop data theft because it focuses on access control, not on protecting data content. Firewalls, VPNs, authentication, Zero Trust architectures—all aim to prevent unauthorized access. But once access is gained, data is readable.

At some point, repeating the same defenses while expecting different outcomes stops being optimism—and becomes insanity.

If breaches cannot be fully prevented, and data theft cannot be reversed, then stopping breach-related damage requires a fundamentally different approach.

Instead of changing the question from whether or not your organization will be breached and when and how often, we just asked ourselves a totally different question:

What if stolen data had no value?

Attackers don't break in for systems, they break in for data. And if stolen data cannot be used, monetized, or exploited, then the breach itself loses its purpose.

Let me give you an example:

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

A bank is breached and the attackers gain access to all its systems and databases.

They can see the balance of each account, but when they try to obtain the personal information of the account holder, this specific information in the database is protected in a way they cannot read it.

They have just discovered that all their effort, time, and money invested in breaching the bank were in vain, a total loss.

The data accessed is useless; they robbed the bank and stole used toilet paper.

For the bank, the incident is equivalent to a hardware failure: the affected equipment is replaced, backups are restored, and operations are quickly resumed.

No confidential data has been exposed, and there has been no impact on the bank's reputation or finances.

For the customers, nothing has happened: their money is still in their accounts, and their personal information remains confidential.

Rendering your sensitive data absolutely useless if stolen not only will prevent any damage such stolen data may cause, it also discourages future cyberattacks to try to steal it.

How do you protect the content of your data and neutralize its value if stolen?

Encryption is the only mechanism capable of neutralizing stolen data value.

But not just any encryption. Modern encryption algorithms—symmetric or asymmetric—are not unbreakable. They are only computationally difficult. Given enough time and power, they fail. Encrypted data stolen today will eventually become readable.

This is not theoretical. The Harvest Now, Decrypt Later threat—documented by Palo Alto Networks—means attackers are already collecting encrypted data, waiting for quantum capability to unlock it.

If encryption is going to be the answer, it has to be different, an alternate encryption is required.

As IBM CEO Arvind Krishna stated in 2018: "*If somebody is saying they want something protected for at least 10 years, they should seriously consider whether they should start moving to alternate encryption techniques now.*"

He said that almost 8 years ago and his claim is more valid than ever.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

To stop breach-related damage permanently, encryption must meet requirements current approaches cannot:

- Protect data content, not just access
- Securely protect structured data without breaking systems
- Work inside databases and structured storage
- Preserve data format and length
- Remain usable by existing applications
- Be quantum-resistant by design
- Neutralize stolen data indefinitely

Achieving this required an entirely new encryption technique.

Not an extension.
Not a mode.
Not a workaround.

A new approach.

We have created a technology to securely protect the content of your sensitive data that can render it useless to any attacker if stolen!

After nearly a decade of research and development, we created and patented a novel encryption technology designed specifically to solve the problem modern cybersecurity cannot: Prevent and eliminate the damage data theft can cause.

Our technology exceeds the strictest security requirements such as GDPR, DORA, NIS2, HIPAA, NIST Cybersecurity Framework, etc.; has a small footprint, low resources requirements, negligible impact on systems performance and seamless integration into any existing system or device.

It does not replace cybersecurity, it complements it by solving the most costly—and still unsolved—problem in cybersecurity: ***The damage caused by data theft.***

As we shown in our example, not all data needs to be encrypted, only the data that gives everything else meaning.

By selectively encrypting critical sensitive fields, the remaining data becomes contextless, meaningless, and useless to attackers.

Even if exfiltrated, even if decryption attempts are made, even years later.

As a result from adding our technology to your security strategy, breaches may still occur, systems may still be accessed and data may still be stolen, but, **damage stops here!**

Because stolen data without meaning, structure, or value is nothing more than noise.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

The question we ask you is:

Will you accept defeat and passively wait for your organization to be breached and your confidential data stolen, or will you act now to ensure that a breach does not end your organization?

The survival of your organization depends on your answer!

Act now, before it is too late.

We can help.

References:

Microsoft Digital Defense Report 2025:
https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=29

IBM Cost of a Data Breach Report 2025:
https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/ibm/cost-of-a-data-breach-2025-full-report.pdf#page=27

TotalAssure - Average time to detect a cyberattack 2025:
https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025#global-detection-time-benchmarks

Palo Alto Networks' Unit 42 Global Incident Response Report 2025:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf#page=25

Palo Alto Networks - Harvest Now, Decrypt Later:
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

Thales Group - Secure the Breach - Webinar:
https://cpl.thalesgroup.com/es/node/17376

Palo Alto Networks:
https://www.paloaltonetworks.com/perspectives/mastering-the-basics-cyber-hygiene-and-risk-management/

Cloudflare - Customer confidence is the best security metric:
https://www.cloudflare.com/the-net/illuminate/security-customer-trust/

Seclore – Breach is Inevitable, Data Loss Isn't - Webinar:
https://www.seclore.com/resources/videos/breach-is-inevitable-data-loss-isnt/

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com