IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cybersecurity

Cybersecurity Awareness Month 2025

Eric Herzog

Eric Herzog
Chief Marketing Officer
Infinidat

Biography

Eric Herzog is the Chief Marketing Officer at Infinidat (https://www.infinidat.com). Prior to joining Infinidat, Herzog was Chief Marketing Office and Vice President of Global Storage Channels at IBM Storage Solutions.

His executive leadership experience also includes: CMO and Senior VP of Alliances for all-flash storage provider Violin Memory, and Senior Vice President of Product Management and Product Marketing for EMC's Enterprise & Mid-range Systems Division.

Eric blogs at https://www.infinidat.com/en/blog

Keywords Storage administrators, Cyber attacks, Cybersecurity, Storage, Immutable snapshots, Enterprise data
Paper type Opinion

Abstract

Organizations are now encountering more than 1,650 cyberattacks per week, as perpetrators leverage artificial intelligence and advanced extortion strategies, including double and triple forms of extortion. October is widely recognized as Cybersecurity Awareness Month. This period serves as an opportunity for organizations to re-examine the security of their IT infrastructure and critical corporate data. Against this background, "Is your organization's storage infrastructure sufficiently protected against cyberattacks?" asks the author of this article.

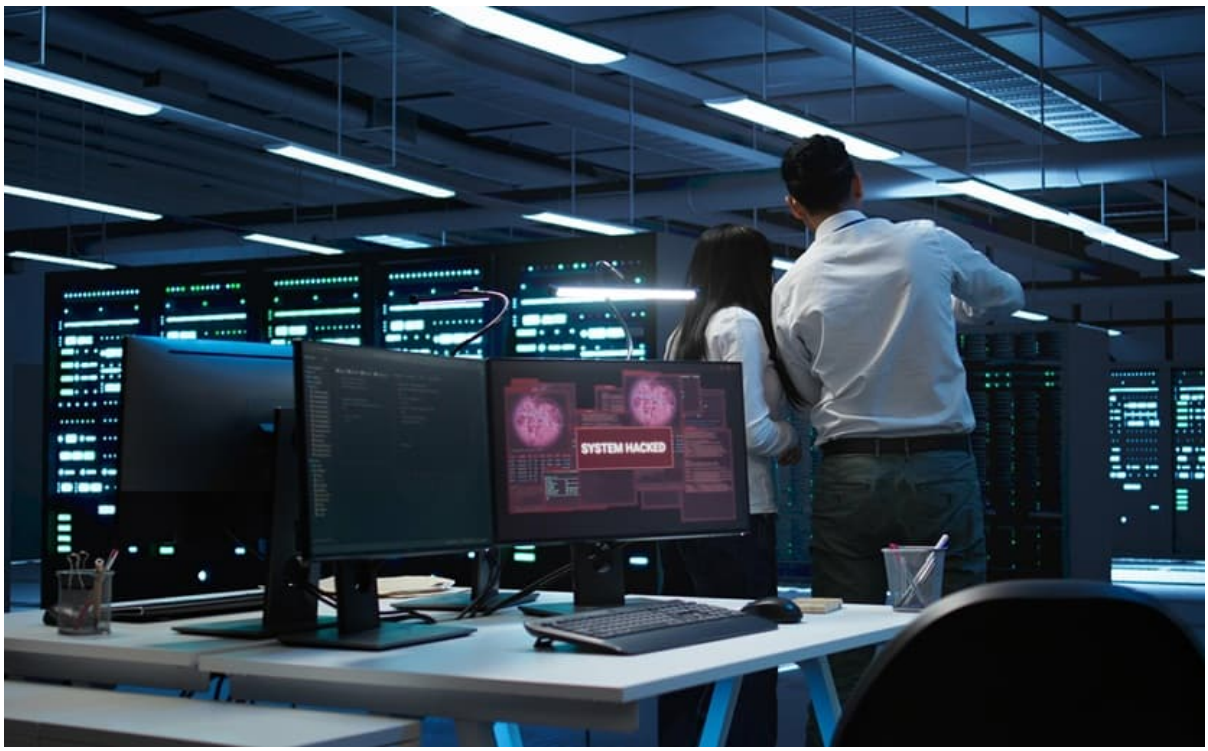
Introduction

October has become synonymous with "Cybersecurity Awareness Month." It's that time of year when enterprises are called upon to re-evaluate how they are securing their IT infrastructure and their critical corporate data. The key question at hand today is: Is your enterprise's storage infrastructure protected enough from cyberattacks?

Your answer to this question determines your next move. And how do you know when "enough" is enough?

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**



Preparedness for digital disaster recovery

The average enterprise suffers more than 1,650 cyberattacks a week. Cyber criminals are finding new and creative ways to exploit weaknesses in enterprise IT infrastructure. The ransomware threat landscape, in particular, continues to get exceedingly dangerous, characterized by the increasing use of artificial intelligence (AI) and more sophisticated, multi-layered extortion methods, including double and triple extortion.

Cybercriminals are advancing their own ransomware tactics to get around, override and power through many existing cyber defences that the majority of enterprises currently deploy. You may not know what you don't know until it's too late – and ransomware has taken your data hostage and, as a result, crippled your business.

The rules for securing your enterprise storage infrastructure have changed. The way that data is managed and protected in 2025 is so different than what was commonly done just a couple of years ago. Digital disaster recovery is the new disaster recovery: because the attack plane has evolved, not only have we needed to rethink the problem as an industry, but we have also needed to redefine and retool "preparedness" for addressing the onslaught of cyberattacks that are unleashed on enterprises of all sizes daily.

During Cybersecurity Awareness Month, companies have the opportunity to decide how to advance the security of their enterprise storage infrastructure and ensure business recovery is within minutes of a ransomware or malware attack – if they are to establish a new normal. It's time to regain your leverage over the cybercriminals who are attacking your business.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

New rules for success in defending against ransomware and malware

The first new rule is to embrace a cyber-focused, recovery-first approach that makes recovering a known clean copy of data as routine and "business as usual" as possible. Recovery Time Objective (RTO) is the key. Being able to recover your business-critical data rapidly – in a near-instantaneous fashion – ensures speedy business recovery.

According to a recent survey[1] conducted by The Register / Blocks & Files, over 30% of large enterprises surveyed said that their recovery time objective is either "under 30 minutes" or, at most, "under one hour." Another 30% of respondents indicated that it's somewhere between one and 12 hours. The remainder indicated "under 24 hours."

Rapid recovery is the outcome of the latest advancements in next generation data protection. To make this happen, data protection recovery has to be as close to the source data as possible. Data is already in the storage systems, so you don't have to run the data across a network when restoring it. Enterprise storage systems have turned into powerhouse cybersecurity-enhanced lines of defence against these vicious attacks. You will never look at an enterprise storage array the same again!

The level of resilience of your enterprise storage infrastructure will determine how successful – or unsuccessful – you will be in recovering from a ransomware or malware attack. As a new rule for success, cyber storage resilience must be comprehensive, guaranteed, and delivered through a cyber stack that provides immutability, speed, forensic analysis, seamless integration across the data centre cybersecurity environment, data validation and automation.

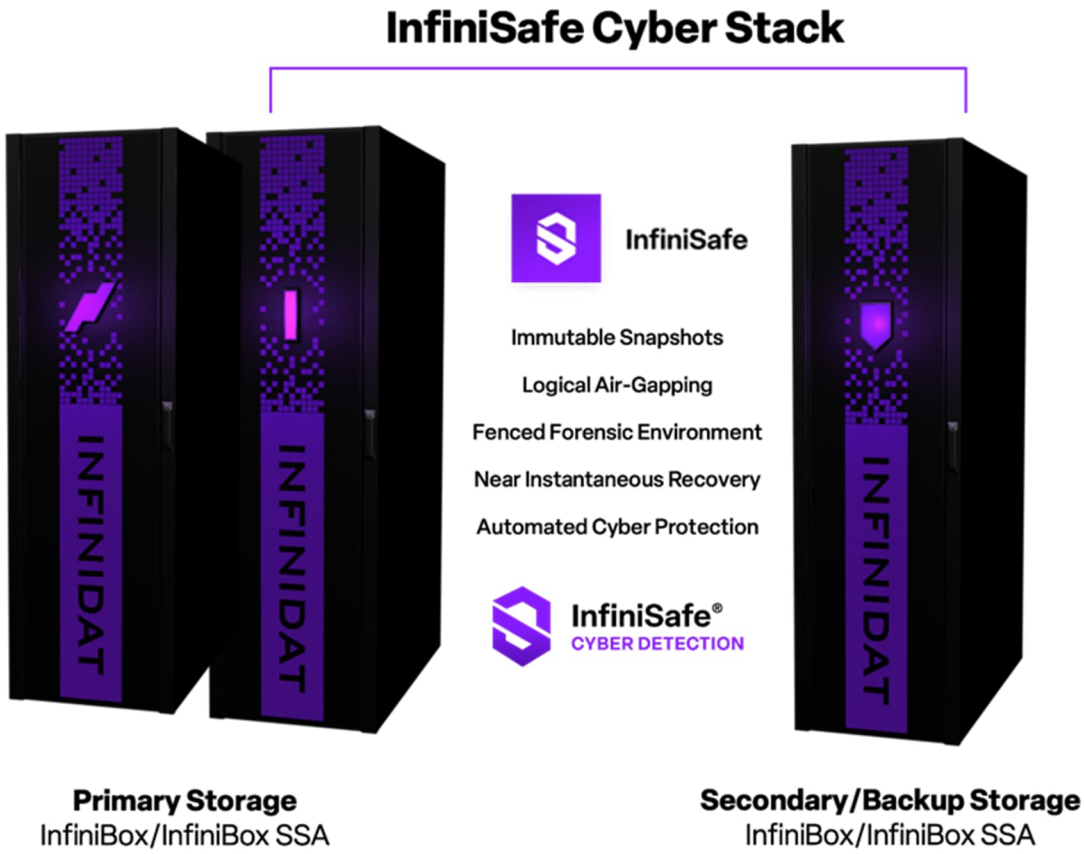
IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The most effective strategy for incorporating cyber storage resilience into an enterprise data infrastructure is to adopt next-generation data protection, which Infinidat pioneered as an advancement over modern data protection and traditional data protection.

The power of Infinidat's cyber stack for cyber storage resilience

Let's take a close look at the cyber stack that serves as the building blocks of next-gen data protection.



All elements of this cyber stack are readily available through InfiniSafe®, which is Infinidat's award-winning software-based enterprise cyber storage solution that uniquely delivers next-generation data protection. The InfiniSafe cyber resilience software portfolio empowers enterprises to optimize their next generation of data security with true immutability, predictive capabilities, and proven recovery strategies, while mitigating risk and the effects of cyberattacks.

Built into Infinidat's enterprise storage platforms, the comprehensive cyber resilience and recovery capabilities of InfiniSafe dramatically improve the ability of an enterprise to combat and protect against ever-increasing cyberattacks. Infinidat guarantees an RTO of 1 minute or less, regardless of dataset size, in the

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

InfiniBox™ SSA and InfiniBox® primary storage systems, and on the InfiniGuard® purpose-built backup appliance (PBBA) an RTO of 20 minutes or less, regardless of dataset size.

With InfiniSafe, you can click a mouse and recover a snapshot. But it's not just any snapshot. It's an immutable snapshot, unique to Infinidat's high-end cyber stack that some of the world's most important enterprises are already using. Unlike our competitors, our immutable snapshots have no backdoor. They're locked. Cybercriminals cannot break in and change the immutability – and we guarantee it!

Another new rule for success is validating the integrity of the data to be restored. Data validation has emerged as extremely important in this day and age. It's imperative to have a cyber detection capability integrated into your storage infrastructure to forensically analyse whether the data that will be restored is, indeed, clean – in other words, free of corruption, free of malware. The orchestration of this data validation matters as well.

InfiniSafe Cyber Detection is infused with powerful AI and machine learning. It combines 200+ analytics with data observations that get more intelligent over time with more observations. It enhances Infinidat's core cyber stack resilience and response capabilities by enabling security and IT teams to detect ransomware and malware attacks with up to 99.99% accuracy and enable near-instantaneous recovery of data from clean, known good copies on the InfiniBox and the InfiniBox SSA platforms.

> **During Cybersecurity Awareness Month, you have the opportunity to plan out how to advance the security of your storage infrastructure and ensure business recovery within minutes of a ransomware or malware attack – establishing a new normal. It's time to regain your leverage over the cybercriminals who are attacking your business.**

Reducing the threat window of cyberattacks is also now a new rule of cyber success, and Infinidat developed a capability that does exactly that. It's called InfiniSafe Automated Cyber Protection (ACP), which is a first-of-its-kind cybersecurity integration.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Our InfiniSafe ACP capability, which is the newest element of our cyber stack, seamlessly integrates with an enterprise's SOC or with their SIEM or SOAR cybersecurity software applications. If these non-storage cybersecurity data centre solutions see a cyber threat, InfiniSafe orchestrates the automatic taking of immutable snapshots of data, at the speed of compute, to stay ahead of cyberattacks by decisively cutting off the proliferation of data corruption. It unlocks the full potential of an enterprise's security posture and maximizes the investments that an enterprise has made in protecting the business.

Infinidat's proven, impactful solutions solve the challenges of ransomware and malware. Make sure you snap up InfiniSafe!

In conclusion

Organizations that adopt enterprise storage system-based cyber recovery solutions featuring advanced data protection, such as Infinidat's InfiniSafe®, will position themselves for a significant competitive advantage. The distinction between robustly securing a data infrastructure and not doing so can have substantial implications for operational integrity and resilience. Maintaining high standards is essential when it comes to the protection of critical data assets.

Reference

1 Flanagan, C. (14 August 2025) 'Large Enterprise Survey Results Affirm Rapid Cyber Recovery as a Top Priority'. Infinidat. Available at: https://www.infinidat.com/en/blog/large-enterprise-survey-results-affirm-rapid-cyber-recovery-top-priority