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**

IT Security

Three Key Cyber Resilience Messages that Channel Partners need CISO Clients to Understand

James (JT) Lewis

James (JT) Lewis
Director of Channels
EMEA and APJ
Infinidat

Biography

James (JT) Lewis is the Director of Channels EMEA and APJ at Infinidat (https://www.infinidat.com). He is an experienced international Sales Director with a proven track record in the enterprise IT, storage, and network security industries. His broad industry experience includes roles involving cyber security, Storage Area Networks (SAN), enterprise storage, IT service management, IT strategy, professional services, cloud computing and virtual computing environments.

Based in Frankfurt, JT has responsibility for Infinidat's EMEA and Asia Pacific regions, including Japan. JT served in the US Military before embarking on his technology sales career, more recently he worked for Data Interchange as Head of Channel Sales and was the Strategy and Growth Officer for Altdata Technology Solutions, focusing on the cyber security market. He also spent 15 years at EMC and RSA, based in London and Frankfurt, where he built up comprehensive experience in the recruitment, enablement, and leadership of channel partners and distributors.

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

Keywords Data, Cyber attacks, Digital crime, Cyber resilience storage, Channel partners, Ransomware, Cyberthreats
Paper type Research

Abstract

As the digital economy grows, digital crime grows with it. All industries face greater exposure to cyberthreats due to increasing digitization, yet research shows that companies continue to lack the readiness to respond to ransomware attacks. The overarching challenge for chief information security officers (CISOs) and cybersecurity teams is protecting their institutions against cyberthreats while maintaining business continuity. As such it is increasingly falling to the IT channel to help end user enterprises to appreciate the need for cyber resilient storage. In this article, the author discusses three key cyber resilience messages that Channel Partners need CISO clients to understand.

Introduction

Pretty much every CISO will believe that cyber threats are the number one challenge facing their organizations. It's not surprising that they have a vested interest in it, their jobs depend upon it. But they are not the only ones in the C-suite worried about cyber vulnerabilities. CEOs also rank cyber threats very highly.

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**

Cyber-attacks rank in second place amongst the most serious of all possible economic, social, political, business, and environmental threats. This is according to PwC's 24th Annual Global CEO Survey[1]. Within the UK CEO subset, the level of threat was deemed very high with 91% of CEOs saying that cyber protection was their key priority.

Many channel partners are aware of what the threat of a cyber-attack means in terms of a market opportunity and have rightly been investing in their cybersecurity operations. They appreciate that enterprises do not always have the internal cyber-skills to ensure a rapid bounce back if they encounter an attack and even if they could afford to buy in the necessary skillsets, recruiting those people is another matter. It is why 'cybersecurity as a service' is now one of the fastest growing new business areas within the enterprise IT channel. It is also one of the most valuable subsets of an industry worth US$2 trillion, based on estimates published by McKinsey[2].

As with all developing industries, education will inevitably be an important component of any cybersecurity managed service provision, and this includes helping end user enterprises to appreciate the need for cyber resilient storage.

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**

Here are three key messages which every channel vendor needs to be sharing with their CISO and CISO client base, to help them understand what's at stake and how they can protect their organizations.

1. **Not if, but when** – It's mind-blowing to think that every 39 seconds, an organization somewhere in the world suffers a cyberattack. If intrusion attempts are happening with such frequency, it's no wonder that CEOs are scared. The question is not if your enterprise will suffer a cyberattack, but when and how often – and if penetrating the firewall is a given, this also means it's highly likely that primary and secondary data being stored by an enterprise will be compromised at some point too.

2. **Cyber criminals are patient beasts** – There's a perception that cyber attackers have a smash and grab mentality, but the statistics tell a different story. When cyber attackers target an enterprise, they don't immediately pounce, but wait for a while before demanding a ransom. Sometimes they will have planned their eventual move for over six months. Research conducted by the Ponemon Institute[2] verifies this, suggesting that the average number of days before a data breach is identified can be as high as 287. It means the hackers have a much greater chance of their ransomware demands being met because without the right controls in place, the data stored can be fully compromised. In that timeframe, data could have been exposed to all kinds of criminal activity.

3. **Prevention is always better than cure** – Data is one of an enterprises most important strategic assets and why McKinsey[4] has coined the phrase 'data-driven enterprise.' It describes an organization with data embedded into every decision, interaction, and process. If effective cyber security is about being ready to thwart the problems that arise from a security breach, what should enterprises be doing differently to protect their data? It means thinking beyond the traditional toolkits of firewalls or cyber management software and being ready with an antidote to stop the damage from spreading.

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**

Time to protect data, but how? Key ingredients of cyber resilient storage

Today's cybercriminals are technology experts. They are highly skilled at exploiting data vulnerabilities inside enterprises that do not understand the importance of cyber resilient storage and have left either primary storage infrastructure or secondary/backup/disaster recovery storage exposed. Maybe even both.

When it comes to securing an enterprise's data storage, there are some essential ingredients to building a storage cyber defence strategy that channel partners should understand. These include ensuring the immutable nature of the data, recovered from a copy you can trust. Air-gapping to separate the management and data planes to protect the data. A secure forensic environment, to analyze the data thoroughly and ensure the fastest recovery speeds possible is critical. Each of these elements needs explaining to enterprise end users.

Immutable snapshots are like the vital 'secret sauce' of storage cybersecurity. They allow the end user to effectively roll back the clock and recover guaranteed, uncorrupted copies of their data, before the execution of any malware or ransomware code introduced by an attacker. Immutable snapshots ensure data integrity because they prevent data copies from being altered or deleted by anyone. Even internal systems administrators are locked out of immutable snapshots manipulation. It means that the enterprise can be confident that any disruption or damage caused by the intrusion can be kept to an absolute minimum.

Logical air gapping adds a further layer of security, by creating a safe distance between the storage management layer and the immutable snapshots. There are three types of air gapping. Local air gapping keeps the data on premises, remote air gapping makes use of a remotely hosted system and hybrid air gapping combines the two.

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**

Fenced forensic environments help speed up the recovery process by providing a secure area to perform a post-attack forensic analysis of the immutable snapshots. The purpose here is to carefully curate data candidates and find a known good copy. The last thing an enterprise wants to do after an attack is to start restoring infected data that has malware or ransomware infiltrated within it. Once the forensic analysis is complete, it is safe to restore a copy to primary storage systems.

The right cyber storage resilience solution is part of a "set it and forget it" process. Once the immutable snapshots, logical air gapping, fenced forensic environment and cyberattack recovery processes have been established, the whole restoration will progress like clockwork. This is all part of being an agile enterprise, one that's cyber resilient as well as cyber secure. Significantly very few enterprise storage vendors can offer this level of cyber resiliency on primary data, which if part of an overall cybersecurity as a service offering, would become an important differentiator for a channel vendor.

It is clear that all channel partners have an important role in educating their enterprise customers that securing primary and secondary storage is an essential part of their overall corporate cyber resilience strategy. Data is one of the most important strategic assets an enterprise owns and critical to long term business success. Yet too many enterprises have not fully integrated a cyber storage resilience program. It's a fantastic business opportunity for channel partners and those who are early to market with a strong cyber resilient storage offering will reap plentiful rewards.

Reference

1 24th Annual CEO Survey: UK CEOs plan a 'no regrets' recovery. PwC. Available at https://www.pwc.co.uk/ceo-survey/24th-ceo-survey.html

2 Aiyer, B., Caso J., Russell P., Sorel M., New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers (27 October 2022). McKinsey. Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

3 The Cost & Consequences of Ransomware for Small to Large-Sized Enterprises (23 February 2022). Poneman Institute. Available at: https://info.convergetp.com/hubfs/Cybersecurity-Info/Reports/Converge-Ponemon-Ransomware-Report-2022.pdf.

4 The data-driven enterprise of 2025 (28 January 2022). McKinsey. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025#/