

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

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

Enterprise Storage

What Does 'Appropriate and Proportionate' Cyber Resilience Actually Look Like?

Eric Herzog



Eric Herzog
Chief Marketing Officer
Infinidat,
a Lenovo company

Biography

Eric Herzog is the Chief Marketing Officer at Infinidat (https://www.infinidat.com), a Lenovo company. 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.x

Keywords Enterprise Storage, Cyber Resilience, Cyber Security Regulation, Data Protection, Storage Infrastructure, Ransomware Resilience, Business Continuity, Regulatory Compliance
Paper type Reference

Abstract

The UK's evolving Cyber Security and Resilience Network and Information Systems Bill places increasing emphasis on the implementation of 'appropriate and proportionate measures' to manage cyber risk and safeguard the continuity of critical services. For enterprises, this raises important questions about the security and resilience of the storage infrastructure underpinning business-critical data and operations. In the absence of prescribed technology architectures or specific technical controls, organisations must demonstrate that their enterprise storage environments provide protection commensurate with the risks and potential consequences of disruption. In this article, the author examines the implications for enterprise storage strategy, exploring how security, data protection, availability and recovery capabilities contribute to cyber resilience, and how CIOs and CISOs can assess and evidence the adequacy of their measures in an increasingly demanding regulatory environment.

Introduction

The UK recently published further guidance on its evolving cyber security and resilience requirements. This forms part of the Cyber Security and Resilience Network and Information Systems Bill, which requires enterprises coming within the scope of these regulations to take 'appropriate and proportionate measures' to



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

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

manage cyber risk. It also means that enterprises need both effective protection and the resilience to minimize disruption when incidents occur.

So how can CIOs and CISOs be sure that they have done enough? Have they taken the required appropriate and proportionate measures? These are important questions for enterprises because the Bill does not prescribe a single technology architecture that every organisation must implement. For the enterprises themselves, this omission creates a challenge. Rather than simply demonstrating that particular security products have been installed, they need to consider whether the measures protecting the systems on which their critical services depend are appropriate to the risks and potential consequences of disruption – and be ready to defend that position.



From compliance checklist to evidence of resilience

Delving a bit deeper into the issue, the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) 4.0[1] provides some useful insight into what this means in practice. b It doesn't include a technology checklist, but, instead, it sets out key objectives and principles expressed as outcomes. The emphasis is on what needs to be achieved rather than prescribing exactly how it should be done. The NCSC also makes clear that enterprises should consult their industry regulator for guidance on meeting their individual regulatory requirements.

For CISOs, CIOs, and CTOs, this changes the question from "Have we installed the right technology?" to "Can we demonstrate that our technology enables us to



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

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

achieve the resilience outcomes appropriate to our risk?" When it comes to enterprise storage, what would this evidence look like?



Consequences of losing critical data

According to the CAF's data security principle, enterprises should know where data important to the operation of essential systems is stored and understand the consequences if it becomes unavailable, or is accessed without authorization, modified or deleted.

From an enterprise storage perspective, this means going further than just having a backup. IT and cyber security executives should be asking whether critical data is adequately protected from alteration or deletion, whether protected copies would remain available following a cyberattack, whether those copies are usable, and whether the organization could restore its systems within the timeframe its essential functions require. This is cyber resilient enterprise storage.

In practical terms, it involves the use of immutable snapshots that cannot be altered or deleted, even during a cyber threat, together with logical air gapping. It is an approach that also incorporates a fenced forensic environment, providing an isolated area in which snapshots can be analysed and a known-good copy identified before restoration.



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

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

These exact technologies are not mandated by the Cyber Resilience Bill, but they are examples of best practice measures that can help an enterprise to address specific storage cyber security risks, as identified through a risk assessment.



Expectations for recovery and backups

Enterprises should also be prepared to restore essential functions within a suitable time frame. This requires appropriately secured backups, routine testing and comprehensive backup arrangements that are created, tested and performance reviewed. What constitutes an appropriate timeframe will depend on the enterprise, service and risk. However, recovery performance can be measurable. Infinidat, for example, guarantees recovery of any size dataset, even if the dataset is 10s of petabytes (PB) in under one minute on its InfiniBox and InfiniBox SSA primary storage platforms.

So, have you done enough?

Unfortunately, there is no universal answer to this question, because there is no universal level of risk. Every enterprise is unique. The most useful way for CISOs, CIOs, and CTOs to interpret and demonstrate “appropriate and proportionate” is to identify an enterprise storage partner that prioritizes comprehensive enterprise cyber storage resilience and recovery. And to work with that vendor to answer these critical questions:

1. What would be the consequence of critical data becoming unavailable or compromised?



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

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

2. What controls protect it?
3. Can protected data survive an attack?
4. How quickly can it be recovered?
5. And, crucially, how can we demonstrate these capabilities?

In conclusion

Immutable snapshots, logical air gapping, forensic analysis of protected data and demonstrably rapid recovery all contribute to the evidence an enterprise can use to show that it has taken appropriate and proportionate steps to secure its critical data.

The stronger the evidence that critical enterprise data is protected, recoverable, and recoverable within an appropriate timeframe, the stronger the enterprise's position for demonstrating that its approach to cyber storage resilience is both considered and proportionate.

Ultimately, appropriate and proportionate cyber resilience is about being able to demonstrate that the measures in place reflect the risks an enterprise faces. For CISOs, CIOs, and CTOs, this means looking beyond whether enterprise data is simply backed up, to knowing whether it is protected, recoverable and recoverable quickly enough to minimize disruption. In an increasingly demanding regulatory environment, these are cyber resilience capabilities enterprises must have to be able to demonstrate and not just assume.

Reference

[1] https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf