

Guide to Cyber Recovery Preparedness in Higher Education

LEARN HOW TO REMAIN RESILIENT IN
THE FACE OF CHALLENGES

CONTENTS

03 Higher Learning,
Higher Risk

04 Building a Cyber
Recovery Curriculum

05 NCSC Cyber Assessment
Framework (CAF)

06 Preparing for
the Unexpected

07 Minimum Viability:
The First Step to Cyber Recovery

08 The Fastest, Most
Complete Recovery

HIGHER LEARNING, HIGHER RISK

When it comes to data, few environments are as complicated to protect as a university. Thousands – sometimes tens or hundreds of thousands – of students, faculty, and staff, all with personal devices connecting to different systems, creating an ever-increasing attack surface.

Campuses large and small are home to siloed, disparate departments implementing their own applications and solutions. Staffing shortages and budget shortfalls have resulted in legacy systems chugging along with little support for needed upgrades. And at some institutions, the commitment to academic freedom and openness comes in direct conflict with the need to beef up security.

On top of that, student data privacy is in the spotlight. Universities house intellectual property as well as personal and financial records of faculty, staff, alumni, students, parents, applicants, and donors. Payment systems, student health records, transcripts; the list of data and inherent compliance challenges goes on and on.

Given all that valuable data and the potential vulnerabilities, colleges and universities are an attractive target for hackers. Findings from Sophos' State of Ransomware in Education 2024,¹ which surveyed a global audience, bear this out:

- Sixty-six percent of Higher Education institutions reported suffering a ransomware attack in 2024, down from 79% in 2023.
- That decline was tempered by dramatically increasing recovery costs: The mean cost to recover in Higher Ed jumped from GBP £780K in 2023 to GBP £2.97M in 2024.
- The average ransomware payment from Higher Ed respondents was GBP £3.26M.
- About two-thirds (67%) paid more than the original ransomware demand.
- Higher Ed is the sector most likely to pay more than the original demand.

BUILDING A CYBER RECOVERY CURRICULUM

These challenges have put the focus on cybersecurity for Higher Education. In Higher Ed and beyond, many organisations' security, IT, and operations teams have considered cyber recovery and disaster recovery to be the same – but a one-size-fits-all approach isn't the answer. Cyber recovery, especially in a sector governed by so many data and privacy regulations, is more complicated than regular disaster recovery. The variability in attacks have shown that cyber recovery plans need to consider:

- **Unpredictability and evolving threats:** Unlike a natural disaster, cyberattacks are malicious and attackers have gone to great lengths to try to hide their actions and movement. Because of this, it can be hard to pinpoint exactly when the attack began, what systems are affected, or the full extent of the damage.
- **Secondary attacks:** Attackers have been seen planting code to launch secondary attacks during the recovery process or creating persistent backdoors that are automatically opened upon a restore action.
- **Compromised backups:** Ninety-five percent of educational organisations (comprising primary, secondary, and Higher Ed) hit by ransomware reported that their backups were targeted.² Attackers are also known to attack backups specifically to make recovery efforts ineffective. This makes the need to pay a ransom to recover production data more real.
- **Time constraints:** Universities often face immense pressure to get back online quickly after a cyberattack. Downtime has been shown to cost organisations across all industries an average of GBP £10,405 a minute, rising to GBP £17,580 for large organisations of more than 10,000 employees.³ And to make things worse, rushing recovery can lead to restoring already-compromised systems, further amplifying the damage.
- **Resource drain:** Cyber recovery at colleges and universities can be a resource-intensive process, requiring expertise from IT, security, legal, compliance, and potentially even law enforcement teams. This can strain already-stretched resources, and can distract security and operations teams from other possible cyber threats and limit their ability to focus on key development initiatives.

By understanding these challenges, educational institutions can use some foundational elements of disaster recovery to build a cyber recovery plan that anticipates these difficulties and helps them bounce back more effectively from an attack.

NCSC CYBER ASSESSMENT FRAMEWORK (CAF) AS A GUIDE

The United Kingdom's National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF)⁴ serves as a cybersecurity guidance framework specifically designed for organisations that play vital roles in the UK's daily operations, with particular focus on essential functions and critical national infrastructure.

The framework is built around four key objectives, each of which has several cyber security principles and guidance associated with them.

1. **Managing Security Risk.** Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions. This objective covers the principles of governance, risk management, asset management, and supply chain.
2. **Protecting Against Cyberattacks.** Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyberattacks. This objective covers the principles of service protection policies and processes, identity and access control, data security, system security, resilient networks and systems, and staff awareness and training,
3. **Detecting Cybersecurity Events.** Capabilities exist to verify that security defences remain effective in detecting cybersecurity events affecting or potentially affecting essential functions. This objective covers the principles of security monitoring and proactive security event discovery.
4. **Minimising the Impact of Cybersecurity Incidents.** Capabilities exist to minimise the adverse impact of a cybersecurity incident on the operation of essential functions, including restoring those functions where necessary. This objective covers the principles of response and recovery planning, as well as lessons learned.



PREPARING FOR THE UNEXPECTED

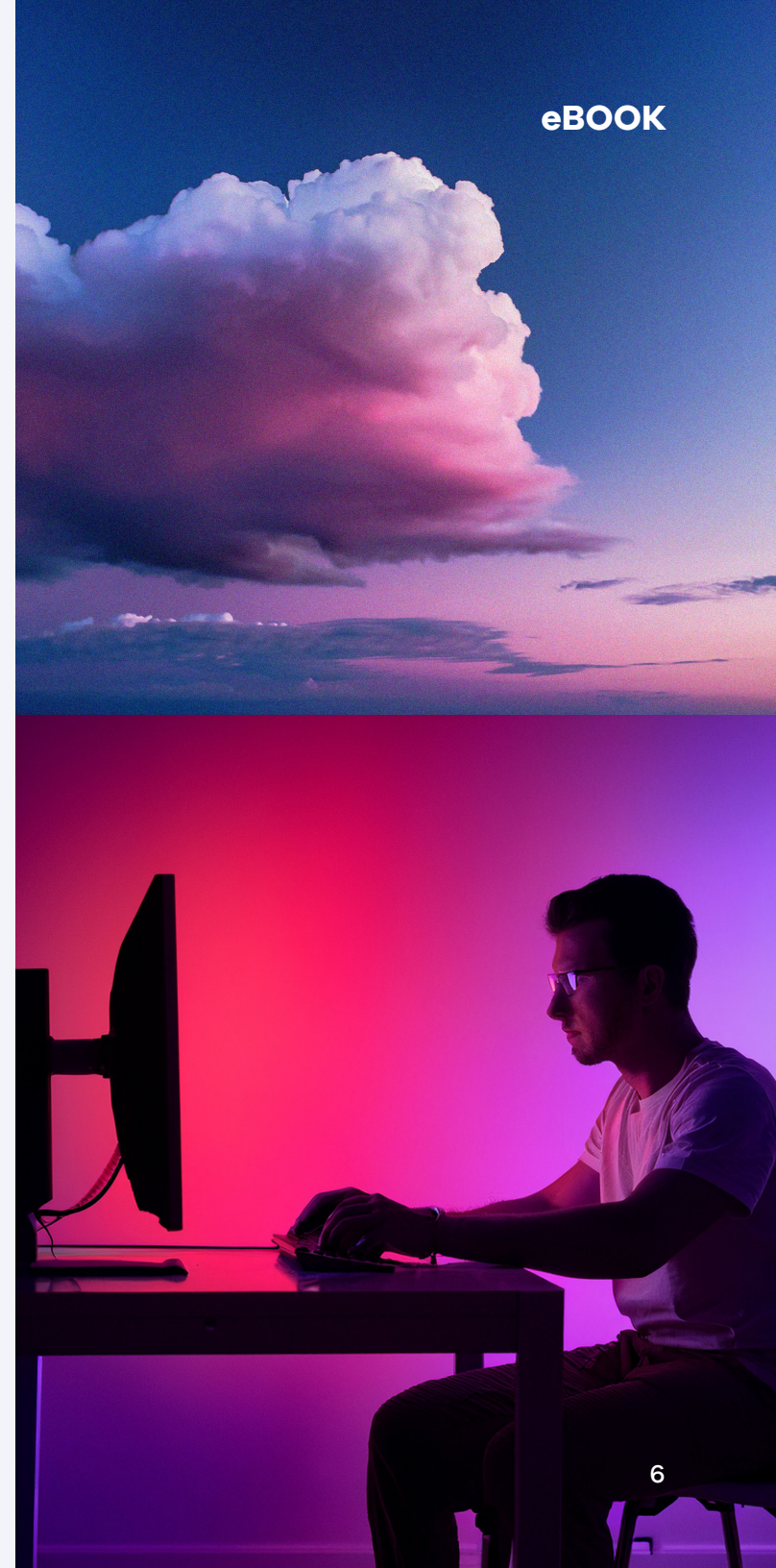
By their very nature, cyber incidents are often covert attacks orchestrated behind the scenes for days or weeks before destruction or havoc takes place.

194 days, or more than 6 months

the average dwell time – the amount of time an attacker has actually been inside an organisation during an attack⁵

Organisations have long conducted penetration tests to highlight areas where their defenses are weak and tabletop exercises to test disaster recovery. But with the variability in cyberattacks, the practice needs to take into account that almost nothing can be implicitly trusted in a true cyber recovery scenario. Additionally, cyber recovery testing has been time-consuming, costly, and complex – making it difficult for institutions to identify vulnerabilities and validate recovery plans effectively.

Backups need to be scanned for persistent malware. Infrastructure must be cleaned to confirm only authorised users are present. And applications and data need to be checked for back doors and restored to a pre-attack (or pre-infiltration) state.



MINIMUM VIABILITY: THE FIRST STEP TO CYBER RECOVERY

Once your institution has been hit by a cyberattack, you're under immense pressure to return to normal as soon as possible. The best way to resume operations quickly? Just restore to minimum viability – the most critical assets you need to maintain continuous business. That way, you can continue to carry on the most vital aspects of your organisation while a full restoration is underway.

Once you identify your most critical systems, processes, and data that will enable you to return to minimum viability, you'll need to make a plan for how you will restore them in the event of an incident. You need to understand the impact of downtime, and you must test and update your plan as needed.

Read [The Ultimate Guide to Minimum Viability](#) to learn more about the steps to restore your regular operations and our recommended practices.

THE FASTEST, MOST COMPLETE CYBER RECOVERY

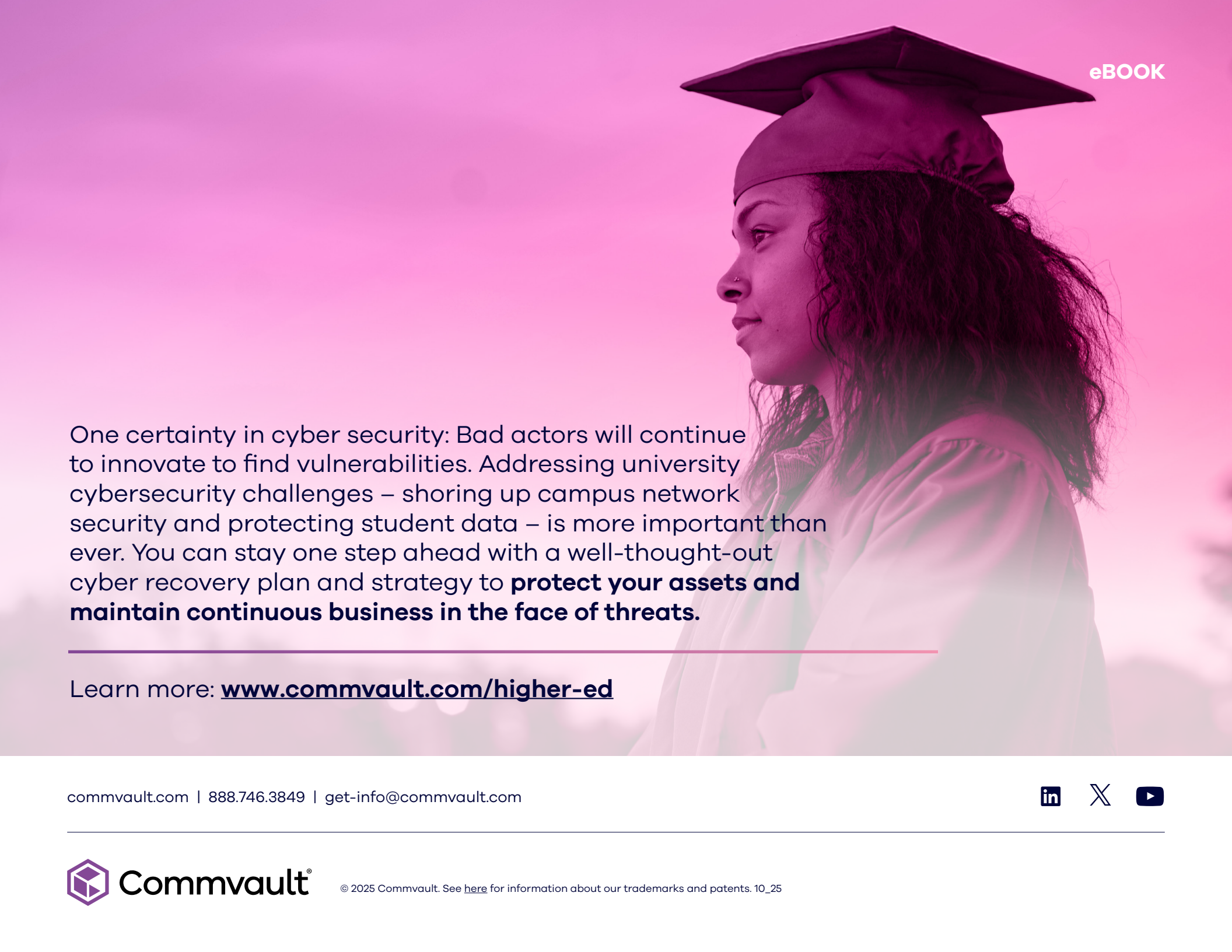
Commvault provides solutions to protect, test, and recover your data, apps, and workloads – delivering comprehensive recovery and true cyber resilience.

Commvault® Cloud Cleanroom™ Recovery lets you test and recover in a safe, on-demand, cloud-based environment. You can easily recover applications and data, and conduct forensics after an event. You'll have an isolated recovery environment for business continuity in the event of an attack.

Commvault Cloud Rewind™ enables near-instant recovery and automatically writes code to recover data and rebuild applications so you can be back in business within minutes of a failure – all without the need for manual intervention.

Commvault Cloud for Active Directory Enterprise Edition delivers rapid recovery for AD and Entra ID environments. It helps automate and orchestrate the recovery of forest-level ADs after an incident, enabling you to get back to minimum viability quickly.





One certainty in cyber security: Bad actors will continue to innovate to find vulnerabilities. Addressing university cybersecurity challenges – shoring up campus network security and protecting student data – is more important than ever. You can stay one step ahead with a well-thought-out cyber recovery plan and strategy to **protect your assets and maintain continuous business in the face of threats.**

Learn more: www.commvault.com/higher-ed