

ESTABLISHING MINIMUM VIABILITY FOR HIGHER EDUCATION

AFTER A CYBER INCIDENT HITS YOUR INSTITUTION, THE PRESSURE IS ON TO RETURN TO NORMAL ASAP.

But given that a ransomware attack can knock you offline for days or weeks, it is imperative to figure out the fastest way to get your most critical assets back online and resume a minimal state of operations.

WHAT IS MINIMUM VIABILITY?

Minimum viability refers to the minimum set of

SYSTEMS	DATA	PROCESSES

you **must recover** to remain operational after disruption.

BUT HOW DO YOU GET THERE?

STEP 01

IDENTIFY CRITICAL ASSETS

SYSTEMS	DATA	PROCESSES
<ul style="list-style-type: none"> IT infrastructure and networking Mission-critical apps and comms tools, like email and learning mgmt systems Physical systems, including security and facilities Third-party platforms 	<ul style="list-style-type: none"> Student data, including financial and health records Research and intellectual property Operational data Compliance data Backup data 	<ul style="list-style-type: none"> IT and security Business operations such as enrollment, admissions, registration, and financial aid Student engagement Basic user support

STEP 02

KNOW THE IMPACT OF AN OUTAGE

Every minute you are down affects all members of your campus community, interrupting class time, research, and productivity – and risks potential damage to your brand and reputation.

Understanding the effects of downtime on each of your critical assets is vital to decision-making and helping prioritize their recovery.

\$3.65M

The average cost of a breach in the education sector¹

\$14,056

The average cost of each minute of downtime across all industries²

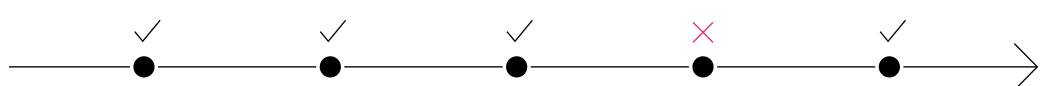
~11 DAYS

The average downtime after a ransomware attack in education, from 2018–2024 – at an average cost of \$550K per day³

STEP 03

MAKE A PLAN AND TEST IT

Once you’ve identified your most critical assets, you need to create a plan for how you will restore them in order to reach minimum viability. This is the state that will keep your university running while you work toward restoring full operations.



THE PLAN

CRITICAL CUSTOMER WORKFLOW



WRAPPING UP

BEST PRACTICES FOR RECOVERING TO MINIMUM VIABILITY



SECURE AIR-GAPPING

Keep air-gapped copies to enable faster recovery of clean data.



TESTING THE PLAN

Test frequently to confirm that your plan works and that your staff knows what to do.



CLEAN RECOVERY

Validate that you are recovering a clean copy of your data.



ISOLATED FORENSICS

Conduct forensics in an isolated recovery environment.

Want to learn more about what it takes to recover from an attack and maintain continuous business at your university? Read our [Guide to Minimum Viability](#) to learn recommended practices.

1 - Cost of a Data Breach Report 2024, IBM

2 - IT outages: 2024 costs and containment, Enterprise Management Associates

3 - Statista