IGXGlobal
An ePlus Technology, inc. Company

3 steps to avoiding SaaS disruptions

How to build resilience.

COMPROMISE NOTHING

Software-as-a-service (SaaS) platforms have become the backbone of modern business. Disruptions to SaaS services, whether caused by human error, software bugs, infrastructure outages, cyberattacks, or unreliable third-party vendors, can derail your organisation.

Here are three steps that will help you avoid falling victim to another company's problems.

1 Refresh disaster recovery and business continuity plans

Preparation is the best safeguard against disruption. Provider outages can ripple across entire organisations, causing downtime and costing tens of thousands of dollars (or more). To protect against these risks, make sure your disaster recovery and business continuity plans are updated and tested.

A strong recovery strategy includes frequent data backups, clear recovery objectives, and regular drills to ensure readiness. By practicing recovery scenarios, you can identify weaknesses and mitigate them before a real disaster occurs. The same is true for your business continuity plan. Make sure your plan has workarounds or alternate solutions that allow people to work and business to flow, even if a SaaS service is unavailable.

This combination of regular backups and tested recovery plans ensures that when problems occur, services remain available and business continuity is maintained.

2 Strengthen security and monitoring

SaaS providers are popular targets of cyberattacks, and are just as likely as any other organisation to experience security incidents. Ransomware attacks, misconfigured permissions, or unauthorised access to SaaS software could jeopardise your other systems. Strengthen your security posture by using multi-factor authentication, role-based access controls, and encryption of sensitive data to protect against unauthorised use.

Yet prevention alone is not enough. Organisations must also see what is happening in real time. Continuous monitoring of user behavior, unusual activity, and third-party integrations helps detect issues early. Tools like SaaS Security Posture Management (SSPM) provide visibility across platforms and help identify potential vulnerabilities before they are exploited.

When strong security controls are paired with vigilant monitoring, the likelihood of preventable outages is significantly reduced.

3 Tighten change and incident management processes

Even with strong security, disruptions can still happen. Human error and software bugs — ranked as the two most common causes of SaaS failures — will never be eliminated entirely. That is why a well-defined incident management process is essential.

A disciplined approach ensures that problems are acknowledged quickly, prioritised appropriately, and resolved efficiently. Metrics such as "time to acknowledge" and "time to fix" create accountability and provide insights for improvement. Communication is just as important: keeping employees and customers informed during an incident helps preserve trust. After each event, organisations should conduct root-cause analysis and update policies and systems accordingly.

Being diligent about change management is equally important. Before any change is applied to your production environment (whether by a vendor or your internal team), make sure it has been tested. Turn off automatic updates in production. Create a buffer zone. Apply changes to non-production environments first, and then simulate business operations to validate the efficacy of the update and ensure the change does not degrade performance, or cause some other problem, before promoting the new code to production.

Build trust through resilience

Avoiding SaaS disruptions requires a strategy that addresses both prevention and response. Good recovery planning ensures that SaaS failures do not halt operations. Strong security and monitoring defend against breaches and misconfigurations. Effective change and incident management processes provide the discipline needed to test changes before applying to production and to respond quickly if an incident does occur. Together, these three steps create a resilient foundation that minimises downtime, reduces risk, and builds long-term trust with customers and stakeholders.

Identify potential vulnerabilities

Start assessment