Hey! What's New? 2025-11

How To Prepare for An IT Outage

A recent article in *INTHEBLACK*, written by Rosalyn Page, says that wide-scale IT disruptions highlight how cyber incidents and tech failures can cripple organizations, leading to downtime and financial losses. But, adds Page, "there are important steps finance businesses can take to review their readiness, resilience and recovery in preparation for an IT outage or other tech disruption.

Organizations today depend heavily on IT systems across all areas of their business, Page points out. "Unexpected IT outages can cause downtime, resulting in substantial financial losses, harm to the company's reputation and frustration among employees. Businesses should, therefore, take steps to plan for potential IT and internet disruptions. Being prepared means considering network design from the outset and having a business continuity plan in place."

According to Jim Kay, founder and CEO of IT Networks, "every business needs to have a thorough disaster-recovery plan that sets out what steps to take if business systems are compromised. Organizations need well-defined procedures to handle outages or other incidents, especially with cyber security breaches where the entire network may be quarantined, halting essential functions like invoicing and communication with clients."

This should, adds Kay, "include fallback processes, particularly for manual operations, to continue essential business activities during an electronic system failure. Without these alternative methods, companies may find themselves unable to conduct basic transactions."

The article emphasizes that a business continuity plan clearly outlines the actions to take before, during and after unexpected events, and should provide actionable steps to address a range of potential disruptions. The plan should cover these five key points.

1. Identify potential causes of IT outages and other disruptions, as well as the likelihood of these events via a risk assessment.
2. Classify critical business systems, data and applications, and consider the potential impact on these functions, as well as business reputation and regulatory requirements.
3. Develop a communications plan and identify the roles and responsibilities of the people who will need to be involved if an incident occurs.
4. Have in place back-up and recovery measures that are regularly checked and tested.
5. Establish manual workarounds, contingency plans and incident responses procedures.

Page then suggests a plan for mitigating an internet outage. She quotes Craig Wilson, managing director of 36-400 IT Solutions, as advising that "businesses should have an uninterruptible power supply (UPS) to ensure they can continue powering devices as well as a 5G modem – preferably from an alternate provider – to keep all these systems functioning, according. Organizations should ensure their backup processes include offsite storage to guard against disasters affecting cloud and/or physical locations."

When planning for potential IT and internet outages, businesses also need to consider archives, which are not the same as backups. Archives are essential for compliance and recovery, Wilson

says. “While backups capture the current data state, archives maintain data history over time, which some industries require for extended periods – up to 25 years in certain cases.”

When it comes to cyber resilience, Wilson believes that a layered security approach needs to include firewalls, backups, antivirus software and potentially intrusion detection. At the device level, he recommends running an ad blocker, such as uBlock Origin on a browser to avoid exposure to potentially harmful ads.

Organizations must assess their risk level and data types while considering regulatory requirements, particularly for financial entities that hold sensitive information, says Kay. “Financial businesses in particular need to identify if they hold sensitive data, such as tax file numbers, MyGov details or passport information, which would require stricter security measures.”

“A data-retention policy identifies the data held, secures it and limits its retention period, allowing for a structured approach to data security,” says Kay.

Learn more at How to prepare for an IT outage | INTHEBLACK.