+44 345 094 0945
www.waterstons.com

Article

Aug 2023

# From Panicked to Prepared: Strengthening Organisational Resilience

Every organisation, during their lifecycle is bound to encounter unforeseen challenges which put their resilience to the test. At times, your strength is stretched to its limits, and failures can be more common than we might like to admit...

Every organisation, during their lifecycle is bound to encounter unforeseen challenges which put their resilience to the test. At times, your strength is stretched to its limits, and failures can be more common than we might like to admit.

Technology plays a pivotal role in driving profitability and growth. Organisations continue to heavily rely on their tech and cyber teams to safeguard against potential disaster.

The steps to protection are technical in nature and can often lack structured processes. Which leaves gaps in ownership and makes the evaluation of resilience a daunting task. Avoiding this assessment is widespread, as the cyber landscape is often filled with technical terminology, never-ending acronyms to learn and an absence of guidance.

However, it's not all doom and gloom.

One critical solution which organisations are using to ease this burden and empower themselves to proactively safeguard themselves is: incident response.

**Here's an overview of Incident Response Below:**




The process of incident response is an easy-to-digest process which leads organisations through proactive, preventive and reactive recovery measures. The ever-changing cyber threat landscape is becoming rapidly more intelligent, as is the complexity of managing them. Preparation with a stable foundation is the crucial component to enable a swift recovery, in the event things go awry.

Organisations are lured into a false sense of security when provided a report such as those which indicates a green check against their data's backup health. While it is vital that backup health has a green check, it won't do your organisation much good if the right processes for your organisation are not in place to support in the event of an incident.

Incident response planning goes beyond the mere containment and eradication of cyber threats; it serves as a powerful business resilience tool that unlocks a seamless path to recovery.

**It's Not Just About The Tech**

Whilst the technology and cyber expertise is a vital component business continuity and resilience, it's not the only important element. Your people are your biggest asset and proactively preparing your people with a cyber partner is pertinent to creating a cyber conscious culture that is resilient for the future.

**Key Takeaways**

- With the implementation of an incident response plan, organisations gain a well-orchestrated play-by-play process that outlines precisely how they will execute recovery from not only cyber incidents but also disruptive events.
- Unforeseen challenges which affect your organisation happen, but preparation is the key to resilience in a cyber-conscious economy.
- Reports are great, but a false sense of security can be garnered from these, a process and a plan with a partnered organisation is the key to resilience.
- It's not just the tech, your people and the right processes are a pivotal role in business continuity.

Strengthening organisational resilience in the face of unforeseen challenges and cyber threats requires a proactive approach. Incident response planning, with its emphasis on a well-structured process and involvement of the right people, plays a crucial role in enabling swift recovery and business continuity. While technology and cyber expertise are essential, a cyber-conscious culture and partnership with the right organisation are equally vital in ensuring a resilient future. Reports alone cannot guarantee security; it is the preparation and implementation of a comprehensive plan that truly empowers organisations to weather the storms of a cyber-conscious economy.

Empower your organisation today, get in touch with one of our team members - 24/7

**info@waterstons.com.au | 02 9160 8430**