

A cyber incident is inevitable... becoming a headline doesn't need to be!

The old approach is flawed

- The "Old School" approach was to write a massive document that no one could easily follow, they never read, nor did they ever practice it in the event it was needed.
- If the plan was ever practiced, it required people flying into a central location to meet physically in a room for a half-day 'gab fest'.
- Meeting notes might have helped identify opportunities to improve, but there were never any measures to evaluate the effectiveness, and the exercise became a distant memory only days later.
- The challenge became greater with COVID and 'Work From Home' requirements.

The TrustedResponse platform is right for the times:

- ✓ a purpose-built crisis simulation digital platform, that
- ✓ translates a Cyber Incident Response Plan into a logical 'business process' flows, focusing on actions and decision makers, which
- ✓ facilitates simulation / war gaming across geographies, functions, or third parties. So you can,
- ✓ compare the 'PLAN' against 'REALITY' to significantly improve your ability to respond more effectively.

Just as a leading sports team must practice for a successful 'game day' - organisations must practice the ability to respond to a cyber incident.

They must understand their roles, responsibilities, decisions... and then practice them to execute successful 'plays' when a cyber 'game day' happens.

Trusted**Impact** is well known for its 15+ years of specialist cybersecurity consulting. The firm stands out from its peers by its unique ability to align strategic thinking, practical business objectives and deep technical expertise in the highly specialised discipline of cybersecurity.

cinten is an Israeli-built computerised crisis simulation platform that helps organisations face potential crises and deal with them in “simulated” real time – better preparing for the “real thing.”

Combined, the Trusted**Response** platform (cinten + Trusted**Impact**) allows you to:



Create an actionable Cyber Incident Response Plan



Extract analytics and insights (expected vs reality)



Import the plan into business process steps



Improve with workflows and checklists



Test your plan via simulated scenarios



Exercise across geographies and/or third parties

“A poor response can be far more damaging than the attack itself.”
(McKinsey & Company)

(<https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/playing-war-games-to-prepare-for-a-cyberattack>)



Analysis



Simulations



Prediction



Insights

To talk about your Cyber Incident Response Plan, contact us at: info@trustedimpact.com

To get more information on the cinten platform, contact us at: creator@cinten.com

www.trustedimpact.com | www.cinten.com