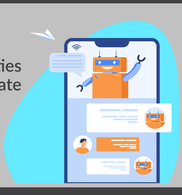
THE DO'S & DON'TS OF DATA INCIDENT AND BREACH RESPONSE

DO
Automate your incident response plan

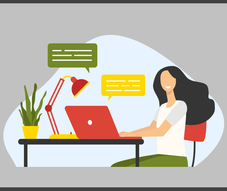
Don't
Run an incident response plan from Excel and Word

DO
Assign roles and responsibilities and automatically communicate them to participants



Don't
Waste time attempting to identify the appropriate personnel and organize meetings across timezones and jurisdictions to assign roles and responsibilities

DO
Communicate through a secure external channel that preserves the opportunity to assert privilege



Don't
Use insecure or undocumented communications with uncontrolled participation

DO
Investigate the incident using state-of-the-art forensic tools

Don't
Collect data using ad-hoc tools which cannot guarantee its integrity

DO
Use AI To evaluate data and determine what data and which data subjects and jurisdictions were affected

Don't
Fail to enable legal counsel to supervise the investigation and forgo privilege

DO
Generate jurisdiction-specific notifications automatically

Don't
Miss deadlines due to a manual notification processes

If any of the don'ts sound familiar to you, Exterro Incident and Breach Response Management can help. It is the only global incident and breach management solution with efficient process orchestration for consistent, defensible, and repeatable response decisions that minimize risk.

FIND OUT MORE

exterro