# The Response Checklist

## REMEDIATION STRATEGY

Shelter from the Storm

In the event of a ransomware infection, you would of course immediately implement your existing cyber security incident response plans and procedures would typically include the following practices.

| ✓ | |
|---|---|
| ☐ | Immediately secure system operations to stop additional data loss. |
| ☐ | Determine which systems were impacted and immediately isolate them. If several systems appear impacted, take the network offline at the switch level. If taking the network temporarily offline is not immediately possible, locate the network (e.g. Ethernet cable) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection. |
| ☐ | If affected devices cannot be removed from the network or the network cannot be temporarily shut down, power infected devices down to avoid further spread of the ransomware infection. Note: this step should be carried out only if necessary because it may result in the loss of infection artefacts and potential evidence stored in volatile memory. |
| ☐ | Triage impacted systems for restoration and recovery. Prioritise based on criticality. |
| ☐ | Confer with your team to develop and document an initial understanding of what has occurred based on preliminary analysis. |
| ☐ | Engage your internal and external teams and stakeholders to inform them of how they can help you mitigate, respond to and recover from the incident. Strongly consider requesting assistance from a reputable third-party incident response provider with experience in data breaches. |
| ☐ | If no initial mitigation actions appear possible, take a system image and memory capture of a sample of affected devices. |
| ☐ | Collect any relevant logs as well as samples of any “precursor” malware binaries and associated observables or indicators of compromise. |
| ☐ | Do not destroy forensic evidence and take care to preserve evidence that is highly volatile in nature — or limited in retention — to prevent loss or tampering. |
| ☐ | Implement notification requirements as outlined in your cyber incident response plan. |