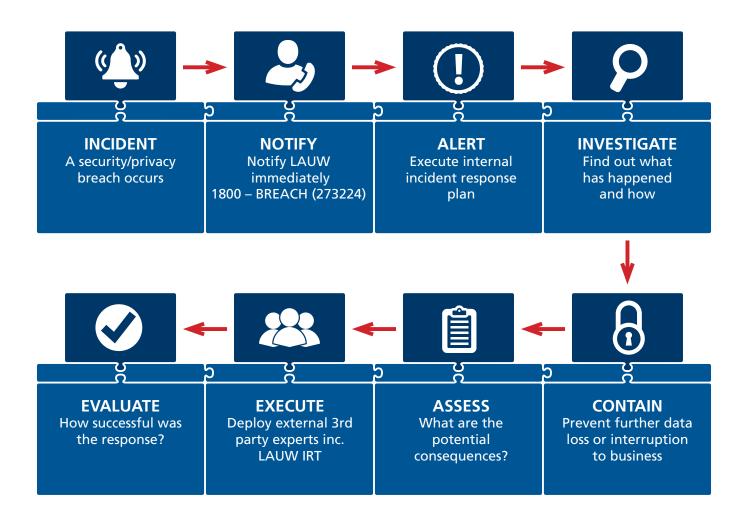
# LAUW eRisks: How we assess and manage urgent claims

#### You learn of: An actual incident (e.g. a security breach or data extortion); Or Something which could be an actual incident (but which requires further investigation before you can be sure); Or • An event which might, later on, lead you to make a claim under your eRisks policy (e.g. an employee loses a company laptop in a public place) Notify LAUW as soon as possible, via: • Form on our website (http://www.lauw.com.au), or We will confirm in writing that we have received • Telephone (1800 273224 - 1800 BREACH), or your notification. • Your insurance broker, or • Email (cyberclaims@LAUW.com.au) LAUW and its agents will promptly assess: 1. Is this a claim, or are you advising us of something **NOT COVERED** that could become a claim? There will be no cover under the policy. We will 2. If a claim, is it clearly covered? 3. Is your loss ongoing? (If it is, we will almost advise you of this promptly and can, if you wish, refer you to our panel firms for assistance. Any assistance they provide will be at your own expense. certainly treat your claim as urgent.) 4. Is the claim urgent for other reasons? 5. Is there media coverage of the incident, or other REPUTATIONAL RISK We will appoint experts in reputational risk to assist you. **Urgent Claims: Crisis Management Phase** We will appoint appropriate members of our Incident Response Team (IRT) to assist you. Members of the IRT will endeavour to make contact with you as soon as possible. They will, at this time, provide preliminary advice on containing any incident that is ongoing. Initial report to you and to LAUW provides IRT begins or continues work in order to: information upon the incident and upon Contain the incident (if not already contained) containment and rectification (if any). • Eliminate any residual threats to the system Analyse the causes and scope of the incident Restore systems to pre-incident statusQuantify and assess your loss Subsequent reports expands upon initial report and discusses the incident and its causes and effects in more detail. Crisis Management phase ends when: 1. Incident is contained 2. Systems are restored to pre-incident levels Investigation phase ends when: 1. Causes of incident are identified Final reports are submitted. They contain recom-2. Scope of incident is known mendations as to how you may remediate any 3. Any losses you may have suffered are quantified to system vulnerabilities uncovered during the investigation. The costs of this remediation are not LAUW's satisfaction covered by the eRisks policy. Coverage decision is conveyed to you and your LAUW makes a coverage decision and assesses insurance broker. the amount that you are entitled to under the eRisks policy.

# eRisks Incident Response Roadmap

#### Security/Privacy Breach - Summary Steps



### LAUW Incident Response Team (IRT):

LAW FIRMS	IT FORENSICS	BUSINESS INCOME ADJUSTING	PUBLIC RELATIONS	IT SECURITY & DATA EXTORTION
Cbp	McGrathNicol	axiom FORENSICS	Ca <b>)</b> ))duspr	azurium
HWL EBSWORTH LAWYERS	Building a better working world	Forensic ADVISORY SERVICES	ROYCE business & communication strategists	ZIRILIO