The Ransomware Decision Guideline

When to negotiate vs. when to pay

REDWOOD
CYBER SECURITY

HopgoodGanim
LAWYERS

Foreword

Ransom and cyber extortion attacks have been crippling for Australian organisations, including private business, not-for-profit organisations and public sector departments or agencies.

These attacks leave behind a host of legal, reputational and financial consequences, both for the impacted organisation itself, its stakeholders, and individuals such as current or former employees and their families, customers or service users.

The Australian Government, Australian Cyber Security Centre (ACSC) and the Department of Home Affairs are firm in their policy stance that organisations or individuals should not pay a ransom.

We do not condone paying a ransom or extortion demand.

Some organisations may adopt a strict position of refusing to pay a ransom demand in any circumstance. The corollary to which is, its board of directors must fully support and fund the organisation's cyber risk management, readiness and incident response strategies. A failure to do so may breach the directors' duties, including duty of care and diligence.

A reality is however, that an organisation may have no option but to consider negotiating or paying if doing so would allow the business to obtain key information about the cause of a cyber incident, unlock its critical data or systems, keep the business operating, preserve confidential or proprietary information from becoming public, or prevent risks to high-value personal information.

This guideline will help inform your strategy on when to negotiate and when to pay, if your organisation faces a ransomware or cyber extortion event.

Mitch Redshaw

Director, Readiness
Redwood Cyber Security

Steven Hunwicks

Head of Cyber Security
HopgoodGanim Lawyers

Table of Contents

Ransomware decision making

The ransomware decision is often summarised as a single binary question:

To pay, or not to pay?

However, if ransomware were a story of decisions, it would also include:

- How much do we invest in cyber?
- Which controls do we invest in?
- What assurance do we have that our controls are working?

And the list goes on…

Managing ransomware risk requires forward investment in prevention as well as response, and guidance already exists to help organisations plan this way. This guide will instead focus on helping you understand the right way to frame decisions during a ransomware attack.

A New Approach

The ransomware decision should instead be framed as a set of strategic options:

Whether to negotiate, and what for?

You don't just have to negotiate for a better deal. You can negotiate for:

- Time.
- Information.
- Control.

All of which can save your organisation money in response, investigation and recovery efforts without even considering a ransomware payment. Ransomware is designed to restrict your choices, but you may have more options at your disposal than you think.

Supporting the Board in ransomware decision-making

During ransomware crises, often the Board will accept or reject management's recommendation on whether or not to pay a ransom demand. Such payments are at times treated similarly to a 'deed of release', with direct involvement and authorisation from the Board. It is important that the Board can trust that management's recommendations on ransomware payments are based on a clear, rehearsed strategy.

Some Boards or management teams may adopt a clear "do not pay" approach, where negotiating with an adversary for a better deal is off the table. This approach is commendable. With the payment option removed, management must consider whether its cyber security programs are adequately funded and resourced to bring alternative options to the table. For example, "have we invested enough to ensure we have 100% reliable backups?", or "have we got enough of the right people to see us through a ransomware crisis with confidence?" are questions which must be asked in turn.

Preparing for Ransomware Decisions

The decision to negotiate or pay a ransom demand is unique to every organisation. Negotiating might be viable where costs and impacts are unacceptable, whereas the decision to pay might be considered where costs and impacts of not doing so are un-survivable. Both choices come with significant risk.

Determining these thresholds and rehearsing your organisation's strategy to ransom demands should not be done when the stakes are high. It's important your organisation realistically assesses when and how it will consider negotiating (or even paying) a ransom demand, well before such a situation arises.

The time to prepare for a crisis is not during a crisis.

Ransomware Decision Making

Whether to Negotiate vs Whether to Pay

Negotiating a ransom demand is different to paying one.

Both choices introduce risk and the decision to pursue either option must be informed by experts, including legal advice specific to the situation. The decision can be informed by understanding whether the current situation poses **unacceptable** vs. **un-survivable** impacts.

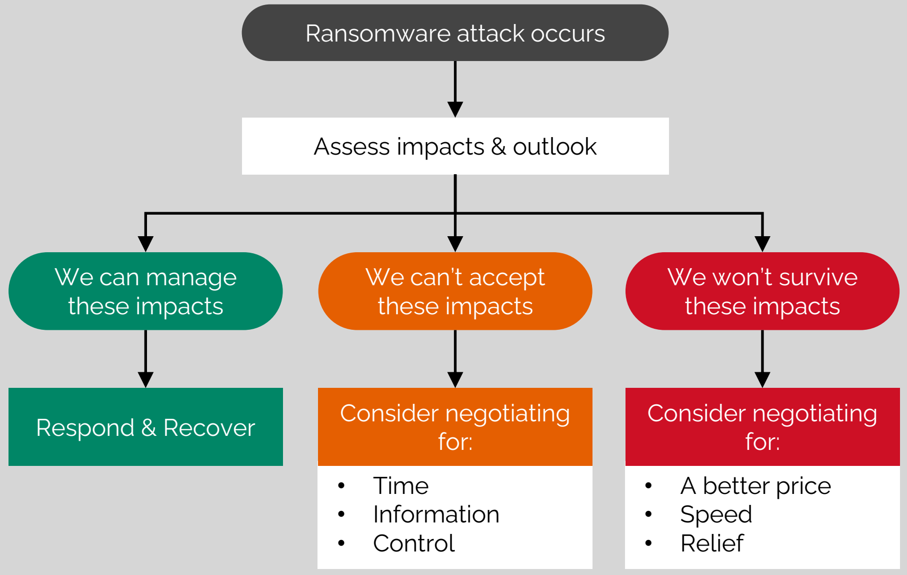
If the situation poses costs or impacts which are unacceptable to the organisation, it should be considered whether negotiation could reduce these impacts into acceptable thresholds. Paying a ransom demand might be considered if the costs or impacts are so severe that the organisation will not survive without doing so.

Whether to Negotiate

- Impacts or costs are unacceptable.
- Negotiation could realistically reduce costs & impacts into acceptable thresholds.
- Negotiation experts recommend it.

Whether to Pay

- The organisation will not survive the costs or other impacts of the cyber incident.
- Paying could reduce risk to life and safety, or is in the interest of a 'greater good'. Consider directors duties and different interests of individuals whose information is at risk, and of shareholders or other stakeholders.
- Whether payment may be unlawful, and legal implications of paying are understood.


Ransomware attack occurs

Assess impacts & outlook

We can manage these impacts → Respond & Recover

We can't accept these impacts → Consider negotiating for:
- Time
- Information
- Control

We won't survive these impacts → Consider negotiating for:
- A better price
- Speed
- Relief

⚠ Warning

Paying a ransom could be illegal
Factors such as international or domestic sanctions, laws in your jurisdiction, the nature of the situation and specific payment circumstances could mean paying a ransom is illegal. Seek legal advice.

No way to enforce terms
When negotiating with criminals you have no way to enforce terms and there are no guarantees that you will get the negotiated outcomes.

Don't do it yourself
Engaging in ransom negotiations must be undertaken by skilled experts (not talented executives, lawyers or cyber experts alone).

Be wary of fake 'recovery' specialists
Many ransomware groups work secretly with 'recovery' companies who 'guarantee' decryption, using their fees to simply pay the ransom.

When To *Negotiate*

Negotiating doesn't mean paying. Many ransomware victims negotiate with adversaries to buy time, or aid investigations by gaining more information about the attack, the affected data or personal information, or the threat actor's tactics, techniques and procedures. Negotiations might also seek to understand more about the criminal group responsible, including (among other things) the likelihood that the group will honour their terms for unlocking data or preventing publication. These negotiation outcomes can provide useful context to incident responders, saving time and money without ever paying a ransom demand.

Negotiation should be considered when the projected cost of a ransomware attack is unacceptable and realistic negotiation outcomes could bring these costs into acceptable thresholds. Not all negotiations are successful, and they should be carefully considered with expert advice and legal counsel.

Assume that any communication with a criminal group **will become public.**

Remain respectful and unemotional, **treat negotiations as a business deal.**

Never negotiate on your own behalf, **engage a ransomware negotiation expert.**

Benefits of effective negotiation

Prior Experience
Negotiators may have dealt with the criminal group before and might know (among other things) the likelihood that they will honour terms

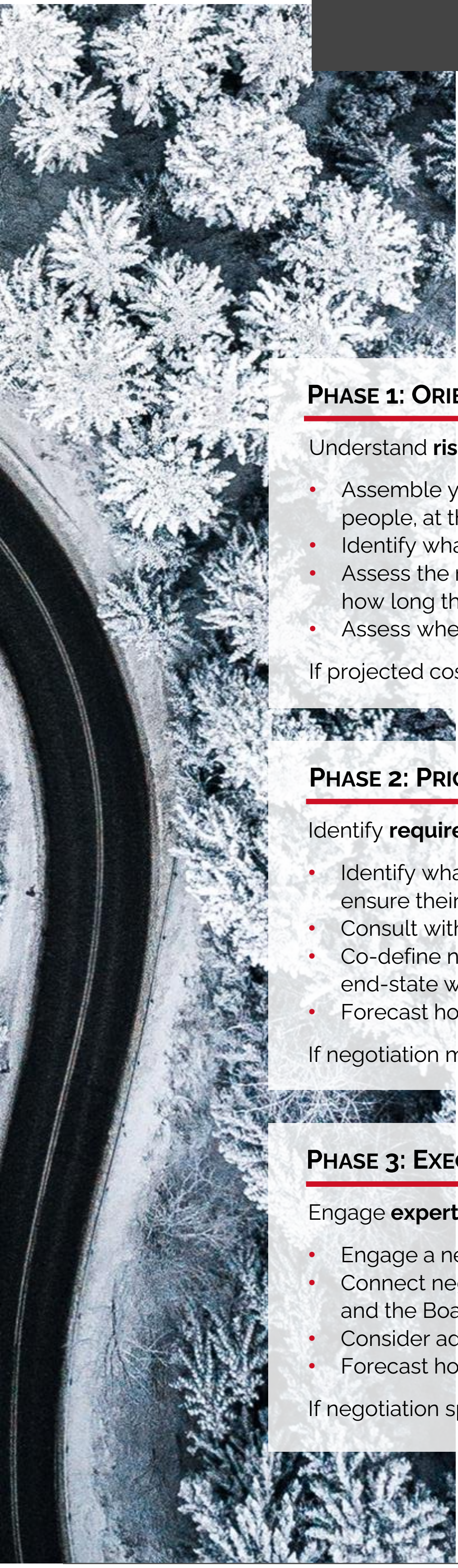
Speed Up Investigations
Negotiators may learn information about how the attack occurred

Slow Down Deadlines
Negotiators may delay payment or response deadlines

Reduce Demands
Negotiators may reduce ransom demands by significant amounts

When to Stop
Negotiators may know when further communication is futile

When to Negotiate



Organisations should not engage with a threat actor until it has worked with its cyber security advisors to verify that its systems have been secured.

Negotiation should only be considered if it's necessary to bring the costs and impacts of a ransomware attack into acceptable thresholds, and negotiating is realistically likely to achieve this.

We've outlined a three-phased approach to help you assess whether negotiation should be considered.

Phase 1: Orient

Understand **risks, impacts and costs**.

- Assemble your Crisis Management Team to get the right information to the right people, at the right time.
- Identify what critical data is impacted, your ability to recover it, and by when.
- Assess the risks, impacts and costs of critical business function downtime (including how long this may last), and what data has been / is being breached.
- Assess whether downtime & breach costs, impacts and risks are acceptable or not.

If projected costs, impacts and risks are unacceptable, begin Phase 2.

Phase 2: Prioritise

Identify **requirements**.

- Identify what technical incident responders need to learn from negotiations to ensure their efforts are as effective and efficient as possible.
- Consult with management and the Board to define an envisioned end-state.
- Co-define negotiation priorities which will support your organisation in achieving this end-state whilst optimising technical incident response efforts.
- Forecast how successful negotiation outcomes will reduce risk, impact and costs

If negotiation may reduce costs, impacts or risks to acceptable levels, begin Phase 3.

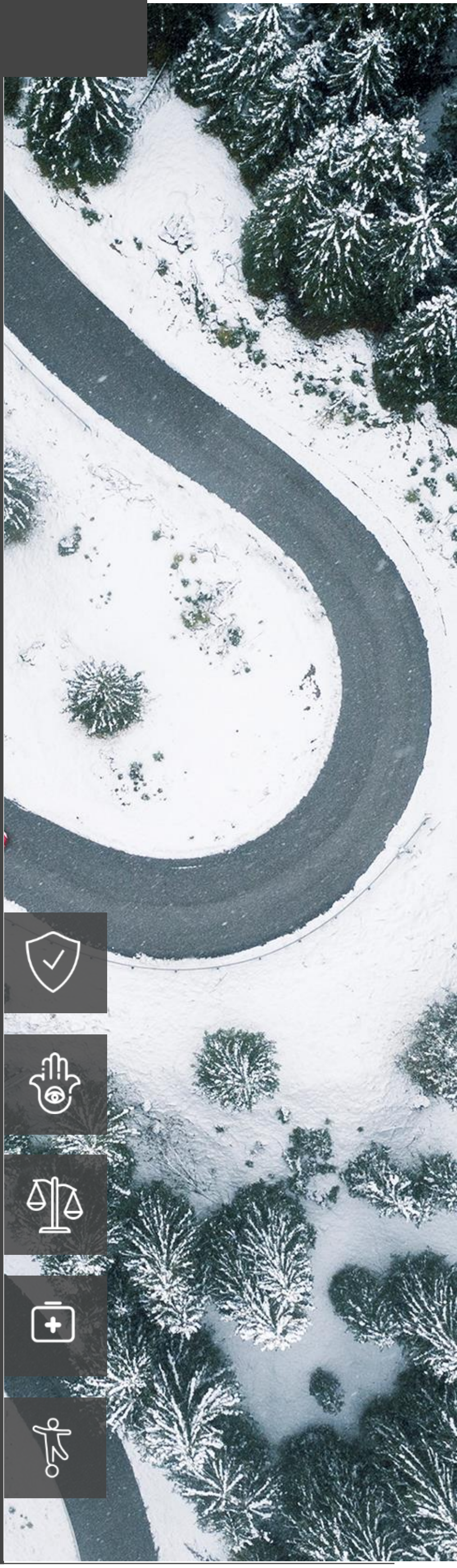
Phase 3: Execute

Engage **experts**.

- Engage a negotiation specialist and share negotiation priorities.
- Connect negotiator with incident responders, subject matter experts, management and the Board to build situational awareness.
- Consider advice from the negotiator and experts, and refine priorities as necessary.
- Forecast how refined negotiation outcomes will reduce costs if achieved.

If negotiation specialist recommends proceeding, commence negotiations.

When To Pay



Under extreme conditions, some organisations determine that paying a ransom demand is justified.

These situations vary widely between victims. In some cases, real risks of serious harm to life and safety are likely if a ransom demand isn't paid. In others, business survival is seriously threatened by the reputational, financial or other impacts of complete and prolonged disruption to critical processes.

Whether to pay a ransom demand cannot be determined without situation specific legal and expert advice. However, if the decision is made, it can be informed by key considerations.

You are dealing on good faith with criminals and have **no means to enforce terms.**

Paying a ransom demand **does not guarantee restoration or deletion of data.**

Authorities cannot relieve the situation or recover funds, and **paying may be illegal.**

Key Considerations

Life and Safety
Whether paying might reduce real and serious risks to life

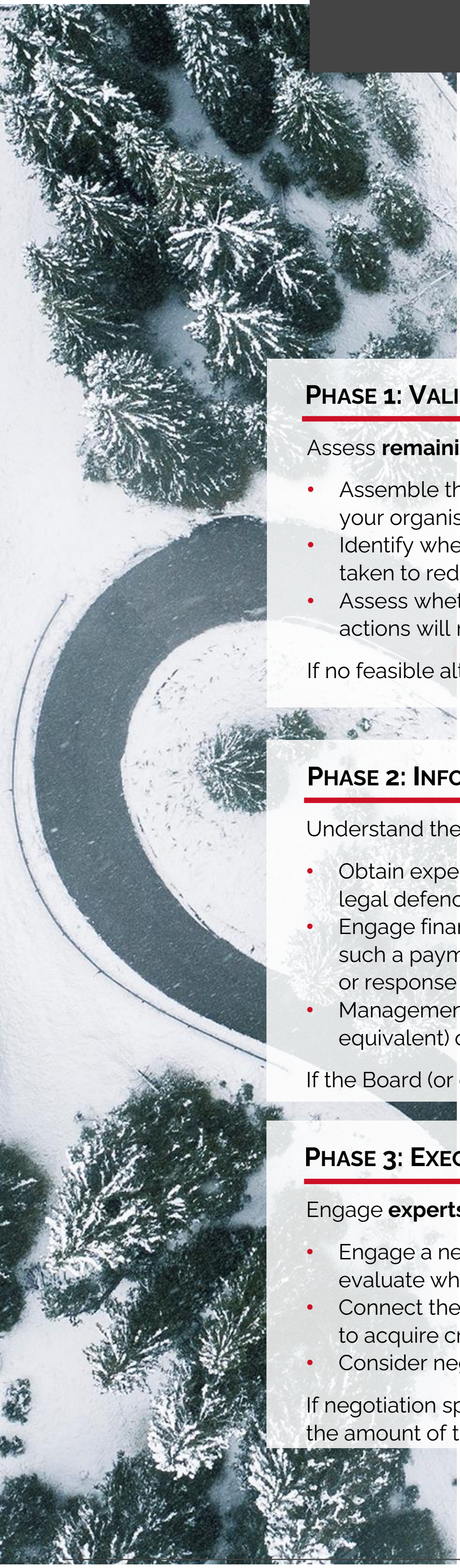
Self-Preservation
Whether business survival is a realistic probability without paying

Legal Risk
Whether paying might violate sanctions, laws or legal obligations

Harm Reduction
Whether paying is likely to benefit the 'greater good'

Balance
Whether paying might shift the balance towards 'better' results

When to Pay



Paying a ransom demand is a complex area of significant risk. If you're considering paying a ransom demand, it is important that your decision-making process is informed by privileged legal advice.

We've outlined a three-phase approach to help you assess whether payment of a ransom demand should be considered.

Phase 1: Validate

Assess **remaining options**.

- Assemble the crisis management team, management and the Board to agree on your organisation's thresholds for considering to pay a ransom demand.
- Identify whether these thresholds have been met, and what response options can be taken to reduce and control impacts or move away from these thresholds.
- Assess whether available options will mitigate the need for payment, how long these actions will require, and whether they are feasible to pursue.

If no feasible alternative response actions exist, begin Phase 2.

Phase 2: Inform

Understand the **impacts**.

- Obtain expert and privileged legal advice on the risks, possible consequences and legal defences of paying the demand.
- Engage finance team to understand how cryptocurrency might be obtained, how such a payment might be accounted for, and whether your organisation's insurance or response retainers provide coverage for such circumstances.
- Management to consider impacts and make a recommendation to the Board (or equivalent) on whether to pay.

If the Board (or equivalent) decides to pay the demand, proceed to Phase 3.

Phase 3: Execute

Engage **experts**.

- Engage a negotiation specialist to commence assessment of the situation and evaluate whether it's viable to attempt to reduce the amount demanded.
- Connect the negotiator with your organisation's legal and finance teams to prepare to acquire cryptocurrency and facilitate payments if necessary.
- Consider negotiator and subject matter expert advice as the situation unfolds.

If negotiation specialist recommends proceeding, commence negotiations for reducing the amount of the ransom demand.

Have a Strategy

Ransomware decision strategies deserve to be thoroughly planned before the stakes are high. Your organisation's strategy to ransomware decisions will have long-term implications and requires balance in its design. It should be informed through deep consultation with management, the Board, and critical technology decision-makers who will form part of your crisis management team.

Ransomware decision strategies should be ratified by management, endorsed by the Board (where applicable), and integrated with wider business resilience arrangements. As part of its preventative measures to manage ransomware risk, your organisation should have a robust, regularly tested cyber security incident response plan, disaster recovery plan and business continuity processes. Your ransomware decision strategy should align with and complement these plans and arrangements to allow rapid activation.

Your organisation's ransomware decision strategy should distil the positions of the Board, management and decision-makers into clear, practical thresholds. These thresholds should trigger clear actions for your organisation to engage the right people, with the right information, at the right time, and guide successful ransomware decision outcomes depending on the situation you face.

Determine Decision Thresholds

In designing your organisation's ransomware decision strategy, you will need to establish thresholds of impact and cost at which negotiation, and even ransom demand payment, will be considered.

Your organisation's enterprise risk management framework should define the ways risk is interpreted, assessed and managed. This should include a risk consequence matrix defining what constitutes 'low', 'moderate', 'high' or 'critical' risk impacts. This is a great place to start designing your strategy.

Determining Unacceptable Impacts

- What level of risk typically requires Board review?
- What thresholds trigger our crisis management plans?
- What's our appetite for different types of risk impacts (financial, operational, reputational etc.)?

Determining un-survivable impacts

- How long can we survive total business disruption before costs become unmanageable?
- What level of loss would require us to downsize, restructure or cease trading / operating?
- How will we know we're approaching these losses?

Establish Relationships with Experts

Technical Experts

- Who will help us contain, eradicate and recover from the technical impacts of a ransomware attack?
- Who will help us with post-breach remediation to avoid re-occurrence?
- Who will provide us privileged legal advice about negotiating or paying a ransom demand?
- Who will help us negotiate with a cyber criminal?

Business Support

- Who will help us manage internal, market and public relations throughout this situation?
- Who will help us notify affected individuals, whether they're local or overseas?
- Who will help us manage insurance and finance?
- Who will help us with notice to compliance with regulatory compliance or data breach obligations?

No organisation can be expected to navigate a ransom demand on its own. It takes a team of experts who know the nature of your business, its strengths and the situation to fully inform ransomware decisions.

Your organisation's advisors will be best positioned to help you execute your ransomware decision strategy if they understand your business, critical assets, corporate structures and key stakeholders. Establishing these relationships ahead of time gives your organisation breathing room during a ransomware crisis.

KEY INSIGHTS

When your IT systems have been compromised and sensitive business data or personal information has been downloaded, deleted or put out of reach due to encryption, the questions of when to negotiate and whether to pay a ransom demand to regain access or prevent data from being published, are crucial and carry significant risks.

Negotiating or paying a ransom or extortion demand can offer no guarantee of resolving the immediate cyber event or its consequences; they may leave your business open to further exploitation in future; be contrary to your own principles or ethics; and it carry a risk that you or your business could be prosecuted for making the payment. Additionally, the Australian government has signaled that it intends to introduce new laws requiring Australian businesses to disclose when they have suffered or paid a ransom or cyber extortion demand.

Conversely, your business may not have time to restore its data, operations or services before the uncertain impact of harms caused by a cyber incident are felt by your users, customers or the general public. So in some cases, paying a ransom demand may allow your business to restore its data or systems, mitigate risk of potential further harms to individuals, customers or stakeholders, and outweigh the costs or risk of not paying.

To assess whether a proposed payment may be prohibited under Australian law, you should (after ruling out other options) consider:

- Your business's reasons for negotiating or paying – whether to obtain information; to reduce the risk of publication, or prevent harm to individuals if the data is published; or for another purpose, such as to obtain a decryption tool;
- If possible, the identity of the payee and other parties in the ransom or extortion chain;
- The likely uses to which your payment may be put, such as whether it is likely to be proceeds of crime;
- Whether the recipient or a party to the ransom payment transaction is on a list of persons or entities listed under United Nations or your country's financial sanctions laws;
- Obtaining professional advice on the legality or otherwise of making a ransom payment;
- If you or your organisation were prosecuted for making a payment, the extent that a defense such as duress may be available; and
- The terms of your business or cyber insurance, to assess whether and how your policy may assist you to defray the costs of the ransom payment.

Cyber attacks can be costly to your business. When ransomware or cyber extortion occurs, it is essential a prompt and strategic response is initiated. The right cyber and legal advisors can help your business get back to full operational capacity fast, working alongside your insurers, accountants and internal IT team.

Read on for information on how to contact Redwood Security and HopgoodGanim.

About Redwood Security

Who we are

Established by former global leaders of a top 5 worldwide consulting firm, Redwood Security is a young Australian company providing cyber security risk and readiness advisory services to Australia's public and private sectors.

With over 15 years of cyber security consulting and advisory experience, we pride ourselves on our trusted-advisor relationships with State and Federal Government, critical infrastructure and private industries across Australia.

Redwood Security has built its foundation on a shared commitment to help our industries develop bespoke cyber security solutions to solve complex organisation-specific, state-wide and nation-wide cyber security challenges. We bring big business insights to client-centric relationships.

Our experience

Our people work within Australia's public and private sector communities to design and implement cyber security strategies for large and global organisations, implement rigorous cyber security compliance frameworks for critical infrastructure operators, and implement nation-wide and state-wide cyber crisis readiness outcomes for State and Federal Government entities, as well as private sector industries.

Our people play critical roles in shaping effective cyber outcomes nationally and internationally, every day, for the greater good.

Our Readiness Services

Governance

We design and implement governance initiatives to support organisations in managing their cyber security risks.

- Cyber security strategy and planning
- Governance design
- Roles and responsibilities
- Policies and procedures.

Risk

We identify cyber security risks to help public and private sector organisations better manage them.

- Threat and risk assessments
- Risk tolerance and appetite
- Awareness training programs
- Cyber risk reporting & dashboards

Compliance

We help organisations demonstrate or achieve compliance to standards, frameworks and legislation.

- ISO 27001
- Essential 8 and ISM
- SOCI & Notifiable Data Breaches
- State and sector-specific standards

Our risk services

Plans

We develop tailored incident response plans and playbooks for government, critical infrastructure and private sectors.

- Ransomware decision strategies
- Cyber incident response plans and technical response playbooks
- Cyber crisis management plans
- Disaster Recovery & Business Continuity Planning

Exercises

We run world-class, engaging cyber exercises for technical, tactical management and strategic audiences.

- Tabletop discussion exercises
- Functional drill exercises
- Boardroom exercises
- Hybrid 'basement-to-boardroom' exercises

Assessments

We help organisations identify their crown jewels, the threats they face, and the best ways to manage them.

- Critical asset identification
- Threat exposure assessments
- Ransomware readiness assessments
- Penetration tests and vulnerability assessments

About HopgoodGanim Lawyers

HopgoodGanim is a high performing mid-tier legal practice based in Brisbane and Perth. The firm was founded in 1974 and for nearly 50 years has enjoyed a strong history of sustainable growth.

Of our 300 staff, over 150 are legal practitioners and the remaining staff include paralegals, administrative personnel, and legal operations specialists.

We deliver exceptional outcomes to our clients in most areas of commercial legal practice while also housing one of Australia's leading and largest private client legal teams.

Areas of Practice

- Corporate and Commercial
- Disputes
- Family and Estates
- Insurance
- Intellectual Property, Technology and Cyber Security
- Property, Construction, Planning and Environment
- Resources and Energy
- Workplace and Employment

Markets

HopgoodGanim's key client markets include:

- Energy, renewables and mining
- Real estate and development
- Technology and digital economy
- Government
- Private clients

The firm's **Data Privacy and Cyber Security** experts keep up with the rapidly evolving legal landscape to offer cyber security education and risk mitigation advice tailored to their clients' businesses. They work to identify cyber threats and minimise the likelihood of a cyber incident occurring.

HopgoodGanim assist businesses and government agencies to navigate cyber security, data and privacy issues. These include local and international compliance obligations, data security in cloud and outsourcing arrangements, information governance and risk policies, and preparing for and responding to data breaches. Find out more at HopgoodGanim's website or contact cybersecurity@hopgoodganim.com.au

HopgoodGanim Advisory Group

The HopgoodGanim Advisory Group is the non-legal consulting arm of HopgoodGanim which includes Effective Governance, a leading specialist corporate governance advisory firm.

Effective Governance works with clients on their governance, strategy and risk needs across all industry sectors throughout Australia and New Zealand, including both large and small companies, listed and unlisted, family business, non-for-profit groups, member-based and public sector organisations including university councils. Their consulting services include:

- Board evaluations
- Director contribution assessments
- CEO assessments
- Governance reviews
- Strategic planning
- Risk assessments
- Board establishments
- Professional development/training

REDWOOD
CYBER SECURITY

Cyber Security Advisors

1800 845 155

www.redwoodsecurity.com.au

info@redwoodsecurity.com.au

HopgoodGanim
LAWYERS

Cyber Security legal solutions

(07) 3024 0433

www.hopgoodganim.com.au

cybersecurity@hopgoodganim.com.au

This publication has been prepared with care, but it provides general commentary only. Cyber security, risk and legislative landscapes change quickly and as such, the information within this publication is subject to change at any time. Because of this, we give no warranty of completeness, accuracy or reliability in relation to the statements, representations made by, and the information contained within this publication. As such, you should not act, or refrain from acting, upon the information within this publication without obtaining relevant and specific professional advice. Please contact us to discuss these matters further.