EMBARGOED UNTIL 24 OCTOBER 2025 1730HRS SGT

GUIDANCE FOR ORGANISATIONS TO BUILD SUPPLY CHAIN RESILIENCE AGAINST RANSOMWARE

Cover Note/Statement

1. Members of the Counter Ransomware Initiative[1] and its Private Sector Advisory Panel[2] are joining together to issue guidance for organisations on building resilience in their supply chains against ransomware threats.

2. **The guidance aims to reduce the likelihood of a ransomware incident having a critical effect on an organisation** by:

a. Raising awareness of the ransomware threat across an organisation's supply chain
b. Promoting good cyber hygiene to protect supply chains
c. Ensuring supply chain vulnerabilities are factored into an organisation's risk assessment and decisions, including on procurement

3. We recommend organisations review the following guidance and consider implementing the recommendations in collaboration with supply chain operators, both existing and future. **The aim is to ensure organisations do not leave supply chains vulnerable to ransomware attacks.**

4. Being prepared for any incident is key and will help lessen the impact if one happens. In 2024, the CRI, alongside insurance bodies, published guidance for organisations during ransomware incidents[3]. This guidance is designed to build on this 2024 product, being specifically targeted at organisations and their supply chains.

5. This guidance is non-binding in nature and does not override specific laws and regulations, or national level cyber security guidance, that may apply across CRI member jurisdictions.

---

[1] Albania, Argentina, Armenia, Australia, Austria, Bahrain, Belgium, Brazil, Bulgaria, Cameroon, Canada, Chad, Colombia, Costa Rica, Council of Europe (CE), Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Economic Community of West African States, Egypt, Estonia, Finland, France, Germany, Global Forum for Cyber Expertise (GFCE), Greece, Hungary, INTERPOL, Ireland, Israel, Japan, Jordan, Kenya, Latvia, Lithuania, Mexico, Republic of Moldova, Morocco, Netherlands, New Zealand, Nigeria, Norway, Organisation of American States (OAS), Papua New Guinea, Philippines, Poland, Republic of Korea, Romania, Rwanda, Sierra Leone, Singapore, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom, Uruguay, Vanuatu, Vietnam, World Bank

[2] Panel members consist of: Arctic Wolf, BlackBerry, CyberCX, Ensign Infosecurity, Institute of Science and Technology, Microsoft, Royal United Services Institute

[3] See CRI guidance for organisations during ransomware incidents - GOV.UK or Singapore Contributes to Ransomware Guidance for Organisations | Cyber Security Agency of Singapore

Main Guidance

About the ransomware threat

1. Ransomware is a colossal, collective challenge, posing a key threat globally to organisations due to its ability to significantly disrupt business operations and essential services, impacting our daily lives.

2. Apart from the disruptive effects of ransomware, the direct costs of a ransomware attack to a victim can be tremendous. IBM's Cost of a Data Breach Report 2025 estimated that the global average cost of a ransomware attack was USD $4.44m[4]. There are also other significant indirect costs, such as when ransomware actors try to compel victims to pay the ransom by publishing exfiltrated data on data leak websites, resulting in reputational damage or having confidential/personally identifiable information (PII) leaked which could be considered a breach of personal data protection laws. Victims of ransomware can also face secondary or triple extortion threats.

3. Ransomware threat actors have been observed to target supply chains in a bid to maximise the impact of their operations. By exploiting victims' suppliers and partners as conduits of a single compromised vendor can serve as an entry point for threat actors to move upstream or downstream in the supply chain.

4. For example, in June 2024 a cyber criminal group executed a ransomware attack on Synnovis; a pathology supplier to several major NHS Trusts in the UK, which led to substantial disruption across several hospitals. The incident impacted 10,152 acute outpatient appointments and 1,710 elective procedures at the two most affected hospital trusts in the four months after the incident[5].

What are supply chain risks?

5. There can be cyber security risks that arise from an organisation's interactions with suppliers. In the context of ransomware, principal risks for suppliers are not being able to deliver a service due to an incident and data loss.

6. Wider supply chain risks can arise from:
   a. **Third-Party Services:** Managed service providers (MSPs) being compromised to target customers.
   b. **Interconnected Systems:** Organisations may also have interconnected systems or trusted connections with suppliers which provide suppliers with privileged access. Also, an organisation's system architecture may not be sufficiently safeguarded against risks.
   c. **Privileged data**: Organisations may have provided sensitive data to suppliers without adequate controls.

7. These risks can be exacerbated by:

[4] Cost of a data breach 2025 | IBM
[5] NHS England — London » Update on cyber incident: Clinical impact in south east London – Thursday 26 September 2024

a. **High concentration/dependency risks**: Risks may be exacerbated by a heavy/disproportionate dependence on the provision of services from a small number of suppliers, potentially compounding the impact of a ransomware incident. Diversification of supply chains, where appropriate, can mitigate such risks.
b. **Low visibility of their supply chains**: Organisations cannot defend what they are unaware of.
c. **Inadequate assurance mechanisms:** Organisations that do not check their suppliers' security accreditations, both at point of contract and throughout the life of the contract, risk unsecure supply chains.

Approach to Supply Chain Security

8. This guidance sets out principles to help organisations develop an approach to improve their supply chain security posture against ransomware risks:

Step 1 – Understand why supply chain security is important *("why")*

a. In a global digital economy, businesses are more reliant than ever on supply chains to operate. Such interdependence has also made supply chains a prime target for cyber attackers. For this reason, it is important for organisations to secure their supply chains to prevent disruption, safeguard sensitive information, and maintain operational efficiency. Ensuring robust cyber security is built into supply chains, particularly through contractual requirements, will reduce the vulnerability of individual organisations and interconnected supply chains and mitigate risks to critical infrastructure and other important systems.

Step 2 - Identify your key supply chain partners and their levels of access *("who")*

a. Develop an inventory of your suppliers to understand the sensitivity and/or value of the information/assets they will be holding as part of a contract, and assess their:

- Cyber security maturity (e.g. presence of multi-factor authentication, patch management, backup practices, certifications)
- History of data breaches
- Use of subcontractors
- Incident response and recovery plans
- Insurance arrangements

b. You should map out the networks and systems which your suppliers have access to or have privileged roles. This allows you to have better situational awareness of the digital terrain in which you are operating in and can facilitate faster incident containment and recovery.

Step 3 - Develop a strategy and implementation plan for supply chain security *("what")*

a. It is vital to think about the level of protection you need suppliers to give to your assets and information, as well as the products or services they will deliver to you as part of a contract.

(I) Select suppliers based on the necessary cyber security controls commensurate to the risk levels of the activities they are participating in.

a. Based on your assessment of your procurement options, choose suppliers that have the necessary cyber security controls in line with the risks associated with the activities they will be undertaking.

b. You can consider taking a risk-based approach to supply chain security, where there are more stringent expectations on supply chain partners participating in higher-risk activities, whilst those participating in lower-risk activities may be able to proceed with lower levels of cyber hygiene.

c. Analysis of the attack vectors often found in ransomware attacks shows that five controls consistently implemented across an organisation's system will significantly reduce the risk of a successful cyberattack. They are:

- Network segmentation and protection (e.g. firewalls),
- Secure configuration (e.g. removing unused software),
- Security update management (e.g. regularly patching and updating all software and systems),
- User access control (e.g. multi-factor authentication [MFA]) and,
- Malware protection (e.g. anti-virus, endpoint detection and response tools).

d. These are considered the minimum needed to achieve basic cyber hygiene, and is supported by academic research, insurance data and case examples. Additionally, backing up essential data and storing them separately from the production environment supports impacted organisations in their recovery.

e. For example, although not directly equivalent, the UK's Cyber Essentials and Singapore's Cyber Essentials schemes, Cyber Fundamentals Framework, and Germany's Top 10 Ransomware measures, can provide assurance to customers that suppliers have implemented fundamental technical controls.

f. For higher-risk activities, the cyber security posture of suppliers should go beyond cyber hygiene and adopt higher standards commensurate to their risks. Examples of national standards that adopt a risk-based approach include Singapore's Cyber Trust, which is tiered with 5 levels. Additionally, there are also international standards and processes such as ISO/IEC 27001.

(II) Communicate Your Security Expectations to Suppliers:

a. Clearly explain your minimum standards regarding ransomware prevention and recovery.

(III) Build Security into Your Contracting Processes

a. You can consider:

- Ensuring that all systems which support the delivery of goods and services are resilient against common ransomware vulnerabilities. This can be evidenced by relevant certificates, business recovery plans and confirmation that such plans are exercised at set interval periods.
- Right-to-audit provisions
- Notification obligations for ransomware incidents
- Penalties for non-compliance

(IV) Gain assurance from the supplier the appropriate measures have been taken.

a. This can be achieved through independent audits, testing or external accreditation including provided by a national cyber technical authority.

(V) Cyber insurance

a. Cyber insurance can be an important risk management practice. CRI members recognise the important role that cyber insurance can play in helping to build resilience to cyber attacks, including through supporting the companies they insure to improve their protective measures.

b. Organisations may like to encourage their supply chains to take out a cyber insurance policy and should understand their suppliers' policy coverage in relation to the data that their suppliers have access to. However, having cyber insurance does not replace the need for organisations to implement cyber hygiene measures to safeguard against ransomware attacks.

Step 4 - Review and refine your approach

a. Ransomware tactics evolve rapidly—supply chain security need to keep pace. Your organisation, together with your suppliers, can jointly:

- Review incidents and near misses for lessons learned
- Regularly exercise response plans
- Share threat intelligence and best practices
- Update contracts and policies to reflect new threats

b. You can also establish a supplier cyber security forum or working group with similar organisations (e.g. within your sector) to drive dialogue and coordination.

Conclusion

9. **No organisation can be fully insulated from supply chain risks, but proactive measures can significantly reduce the likelihood and impact of ransomware incidents.** By following these four steps—understand, identify, develop, and review—organisations and their supply chains can build resilience, not just within their own operations, but across their broader ecosystem.