Guide

Top 10 Ransomware Questions for Executives & Directors

Getting to know your ransomware risk

Huntsman®
Defence-Grade Cyber Security

Ransomware Risk Management

“Victims talk of negotiating a ransomware attack as a frantic and highly stressful process with competing advice coming from a myriad of ‘interested’ stakeholders.”

Ransomware is one of the hottest topics in cyber security today, and right now the scale and frequency of attacks are continuing to accelerate. As a consequence, the risk of a ransomware attack on your organisation is something that every senior executive and director needs to have high-level visibility of.

Cyber security has become a normal part of the board risk agenda, and in 2021 the sheer volume of ransomware attacks has heightened its importance. Demonstrable cyber risk management processes are now an important component of effective cyber security oversight; and when it comes to ransomware, it’s recommended in many jurisdictions.

In the US there is advice from the White House[1] and a draft report from their National Institute of Standards and Technology (NIST)[2] (IR 8374). In the UK, the National Cyber Security Centre (NCSC)[3] offers its own recommendations as does the Australian Cyber Security Centre (ACSC)[4]. In concert, there are moves across many jurisdictions to prevent or restrict the payment of ransoms which will significantly reduce the usefulness of traditional risk management tools like cyber insurance.

The payment of ransoms is seen by some as simply perpetuating the ransomware industry. An added dilemma for management, particularly those that have been effectively shut down by an attack, is whether after receiving the ransom the attackers will provide decryption keys to enable the full recovery of systems and data. Victims talk of negotiating a ransomware attack as a frantic and highly stressful process with competing advice coming from a myriad of ‘interested’ stakeholders.

Managing the Ransomware Risk

In some jurisdictions clarification is being sought around the extent of senior executives’ and directors’ responsibilities for cyber security. Right now it is reasonable to assume that with the digital transformation of business functions everywhere, accountability for the digital operation and security of those activities remains with senior executives and directors.

As a result, boards and senior executives need ongoing visibility of cyber risks, including any vulnerability they may have to a ransomware attack. This includes the ability to **prevent** the initial infection or attack; to **contain** or minimise the spread or impacts of that attack and to then **recover** to BAU. The key to the successful risk management of cyber security is to build systems and processes to systematically measure the state of key security controls to provide visibility and assurance to responsible stakeholders, through frequent and timely reporting.

To help you better understand your organisation’s ransomware readiness, we have compiled the following Top 10 Ransomware Questions for Executives & Directors, to assist you and your operational teams improve your ransomware resilience.

[1] https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf
[2] https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf
[3] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[4] https://www.cyber.gov.au/sites/default/files/2020-12/ACSC_Prevention-And-Protection-Guide_1.pdf

> “Every question you can’t confidently answer highlights a weakness in your cyber security delivery or reporting capability around ransomware risks and readiness.”

1. What experience with, and knowledge of, ransomware exists within your team?
2. Do you know what capabilities your security team has in place to prevent an initial ransomware infection and the processes and assurances around these?
3. Could your business contain a ransomware outbreak if it were to gain a foothold? For example, what segmentation or separation facilities are available?
4. If your systems stopped operating due to a ransomware attack, what would the effects be on your operations, revenues, customers and reputation?
5. Do you have the ability to restore and recover systems, data, domain controllers and applications and has the reinstatement of systems been tested (e.g. from backups)?
6. How do your cyber security controls stack up against those recommended by the NCSC, NIST, The White House or ACSC, and how do you map the effectiveness of those controls against your chosen framework?
7. Do you have a cyber insurance policy, and does it provide cover for ransomware attacks - covering ransom payments and other clean-up costs? Do you receive premium relief for effective and demonstrable cyber risk management processes?
8. Are your plans to manage a ransomware incident well-documented and tested?
9. Do you regularly conduct ransomware education and awareness programs, or conduct tests, such as phishing, to quantify exposures and assess awareness about ransomware and ways to limit its risk?
10. What reports, assurance and oversight do you and fellow executives have of your cyber security controls and their effectiveness? For example, does the board have regular visibility of your current risk of ransomware attack and your degree of exposure?

Every question you can’t confidently answer highlights a weakness in your cyber security delivery or reporting capability around ransomware risks and readiness.

A quick check of ransomware readiness or a risk assessment is a practical way to gather valuable insights into the state of your current cyber defences and maturity. By measuring your cyber security controls against recommended government cyber security advice, you can get a clear picture of those controls and a measure of your ransomware readiness.

By regularly measuring your cyber security and ransomware risk metrics with Huntsman Security’s SmartCheck, you can measure your risk of ransomware attack and identify those weaknesses in IT governance efforts that require attention.

Want to find out more?

Contact Us

Or contact your local Huntsman Security office (listed below) to talk to one of our team today.

About Huntsman Security

Since 1999, Huntsman Security has been on the cutting-edge of cyber security software development, serving some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: **+61 2 9419 3200**

e: **info@huntsmansecurity.com**

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA

t: **+44 845 222 2010**

e: **ukinfo@huntsmansecurity.com**

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA

t: **+81 3 5953 8430**

e: **info@huntsmansecurity.com**

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman