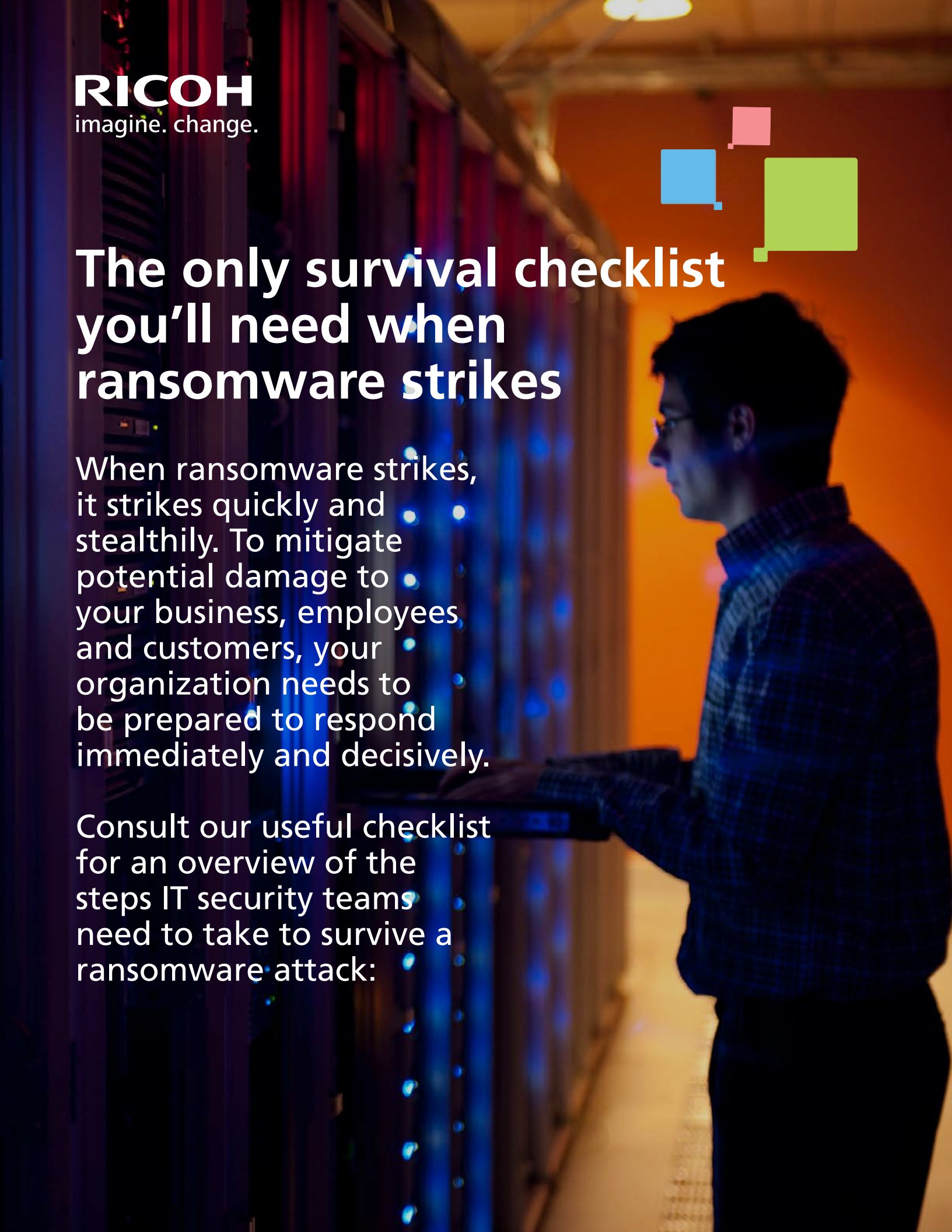
RICOH
imagine. change.

The only survival checklist you'll need when ransomware strikes

When ransomware strikes, it strikes quickly and stealthily. To mitigate potential damage to your business, employees and customers, your organization needs to be prepared to respond immediately and decisively.

Consult our useful checklist for an overview of the steps IT security teams need to take to survive a ransomware attack:



1. Contain the attack - if it's not too late

Save an image of the ransom message and immediately lock down the entire network until you've traced the attack. Ransomware moves fast, with some strains encrypting only a portion of each file to optimize efficiency. According to BullWall, a global ransomware security innovator, many strains of ransomware encrypt an average of 6,000 - 10,000 files in under a minute.

Containment software can detect and instantly stop encryption in its tracks, immediately shutting down the source and eliminating the need to shut the whole network down.

Learn about automated ransomware isolation and containment

2. Execute your incident response plan

Immediately inform executive management and consult your incident response plan. If you don't have one, now is the time to start planning. The Canadian Centre for Cyber Security offers a helpful guide.

A robust incident response plan should include steps to contain, investigate, remediate, communicate, and recover. Continue following this checklist as an introduction to the process.

3. Contact the authorities

Canada's Communications Securities Establishment strongly recommends that victims of ransomware contact local police immediately and report it to the Canadian Anti-Fraud Centre. It's important that you understand your obligations under the law; there are prohibitions against paying ransom to specific groups.

In some circumstances, Canadian businesses are also legally required to report breaches to the Office of the Privacy Commissioner.

4. Contact your insurer

Consider notifying your insurance provider right away to determine what coverage you have and any assistance they can offer. Many agencies offer 24/7 incident response support and can refer you to services such as forensic IT specialists and professional negotiators.

5.Assess the damage

Trace the attack back to the original source and determine how many files have been compromised. Understand when the breach occurred – ransomware will sometimes lay dormant in a network for days or weeks, in other cases it strikes within minutes.

Working with the authorities or with a forensic specialist can help you identify which ransomware strain you're dealing with, enabling you to understand how it behaves and how you need to react.

6. Assess the immediate business impact

The ransom demand has been made and the clock is ticking - the executive team needs to know the extent of potential damages in order to make an informed decision and mitigate risk.

How does this impact business-critical operations? Is there risk to customers, employees, IP and other assets or third-party vendors? Are the attackers threatening to leak sensitive information? What impact would this have on your organization's reputation and business?

7. Inform internal stakeholders

Inform your CFO, legal and public relations teams so they can begin to prepare. Establish a formal reporting structure that enables you to communicate information to a designated point person who can field questions while you focus on containing the attack and mitigating further damage.

8. Decision time: should you pay up?

A recent report shows half of Canadian businesses victimized by ransomware are paying the full ransom, with the help of a professional negotiator.

If you've been infected, and you don't have a good set of backups, should you pay? If you do, you embolden the attackers. If access to the data becomes a matter of life and liberty, you may have to pay and hope that you're dealing with an ethical digital gangster who will return your data, intact.

These situations are a big reason why cyber liability insurance has become so popular, but not all policies guarantee ransom coverage, or there may be very specific terms to follow – be sure to check with your insurer.

9. Prevent further attacks

Experts are seeing an increasing number of second-strike attacks, predicting this will continue in future.

Identify the initial attack vector and reinforce the weak point. The three most common vectors are remote desktop protocols, phishing emails and software vulnerabilities. Conducting a comprehensive security assessment is advised and outsourcing to an experienced partner is further recommended as they can point out any blind spots or gaps in your security posture.

Assess any system or human opportunities where the attack could have been stopped and update your incident response plan. If the access point was enabled by a member of staff, consider running cybersecurity awareness training and testing sessions.

10. Begin data recovery

Refer to the ransom note left by the attackers to help your recovery team identify the ransomware strain. This will enable them to understand its behaviours and search for known decryption keys.

Ensure your backup technology wasn't affected and that it's still operational. Verify that your online or offline backups are available for recovery. When restoring a drive, thoroughly examine it for traces of malware that could reintroduce ransomware later. Run an anti-malware package on all recovered files.

Your safest bet is to install an automated ransomware detection and containment solution like RansomCare, should it emerge again from infected backups.

Don't let it get to this point: invest in ransomware prevention and containment

The global average cost of recovery from a ransomware attack more than doubled from $970,722 CAD in 2020 to $2.3M CAD in 2021. Productivity loss, financial loss and reputational harm can be devastating for a business.

The good news is, a proactive ransomware strategy will ensure you'll never have to face this harrowing experience. And if you've already been victimized by a ransomware attack, you can appreciate how valuable this protection can be.

Start by talking with an experienced security partner who has professional teams in place to test your network, build an incident response plan, and provide IT forensics and recovery services.

Ensuring strong endpoint protection is a critical first step, but even the most sophisticated anti-virus protections aren't enough to beat ransomware. Consider adding a second layer of protection to stop ransomware in its tracks should it get in.

Whatever you decide to do, do it now - the cyber criminals are counting on your delay.

Learn more about RansomCare – your last line of defence

RICOH
imagine. change.