KPMG

Ransomware Advisory Services

Be in a defensible position.
Be cyber resilient.

Ransomware is not a new phenomenon and has in fact been around for over 20 years. However, it is growing in prevalence and the latest variants are so advanced and malicious, they could completely cripple your business. Have you done enough to protect yourself?

What is Ransomware?

Ransomware is a type of malicious software that typically infects your machine or device and renders the device (or the data on the device) unusable until a ransom is paid. The data is typically rendered unusable by encryption, which is a process of scrambling the information so you can only regain access to the data or device if you pay a sum to the cyber criminal that caused the infection.

The sum requested varies, although often has to be paid within a specified time-frame (often 3 days or 7 days), otherwise the data is destroyed and typically lost forever.

The latest variants of ransomware can also encrypt entire websites, any backup data you may hold, and even system files in your computer. Some ransomware not only stops you from gaining access to your data, but also threatens to create a privacy issue for you and unless the ransom is paid, it will upload your data to the public Internet.

Should I be concerned?

Like all Cyber issues, ransomware can affect any organization at anytime, in any sector. KPMG's Cyber Team have seen a significant increase in these attacks throughout the world as criminals realize this can be a highly lucrative way of generating revenue.

Typical questions on Ransomware?

There are many questions that organizations have on ransomware, together with a number of myths. Our view is the following:

Question: I have anti-virus/anti-malware solutions in place. Aren't I protected?

These solutions offer some protection and should continue to be used but most ransomware is written to evade these tools. Most organizations that have been affected by ransomware had up-to-date anti-malware in place at the time of infection.

Question: My organization regularly creates back-ups of our data. Does this mean we are protected?

With older, more basic versions of ransomware, you could simply restore your machine using back-up data. The latest variants of ransomware can stay on your systems for a number of months, encrypting all your back-ups. After a specified period of time, the ransomware demand will then appear and trying to restore from a back-up will be futile.

Question: If my organization is infected by ransomware, I've heard that you can download a tool to get your data back. Is this true?

It is possible that with some older versions of ransomware, various tools can be used to get your data back. However, this typically relied on the ransomware creators making mistakes in their coding. Like businesses, cyber criminals learn by their mistakes and typically write their codes so well that it is not possible to get your data back.

Question: I've heard about shameware. Would your service help reduce the risk of this too?

Yes. KPMG's Cyber Team conducts a review of the prevention, detection and reaction capabilities your organization has for dealing with ransomware, but also shameware and other extortion-driven attacks.

Question: If I get infected by ransomware, should I pay?

It depends, as there are multiple factors to consider including:

- What strain and version of ransomware do you have?
- How widespread in your infrastructure and data is it?
- Have your back-ups been infected, and how far back?
- When is your ransomware payment deadline?
- How long would it take for you to resume your services if you do not pay?
- By paying, could an organization be accused of funding terrorism?

KPMG's Cyber Team recommendations proactively preventing ransomware in the first place, but also to have clear approaches and methodologies in place to respond.

These approaches can then be applied to other similar extortion attempts, such as shameware, denial of service attacks, or other similar cyber challenges.

Ransomware Advisory Services

Our unique Ransomware Advisory Services are specifically designed to review your ability to prevent, detect and react to a ransomware incident. Some of the latest ransomware issues require very specific and cutting-edge approaches to address them, and this is what we bring. Due to its holistic nature, the KPMG Ransomware Advisory service provides a proactive assessment of your capabilities:

- **Process review:** Reviews your organization to ensure you can manage current and emerging ransomware.
- **Technical review:** Understand whether your technical capabilities are sufficient to deal with the risk.
- **People assessment:** Identify whether there are any changes you could make to help prevent staff from accidentally or deliberately infecting you.

We also provide reactive ransomware capabilities: we can help detect whether there is evidence of compromise from ransomware and if you have been compromised, we are able to help support you through the incident, navigating you through to minimize the impact and limit the damage to your organization.

Contact us

Srisucha Limtong
Partner
Head of Management Consulting
T: +66 2677 2677
E: srisucha@kpmg.co.th

Prathan Phongthiproek
Manager
Information Protection and Business Resilience
T: +66 2677 2000 x 4902
E: prathan@kpmg.co.th