JNW STRATEGIC CONSULTING

BPR BUSINESS PROCESS RISK Conversations

Cyber Risk is Real – Will You Be Held to Ransom?

RANSOMWARE

On 12 May 2017, a ransomware program called WannaCRYPT or WannaCRY infected more than 230,000 computers in 150 countries. The program locked out users from accessing their data by encrypting it, in order to demand a ransom to allow access again. Essentially it's a method of 'kidnapping' your data and holding you to ransom. In Australia, it is estimated cyber-attacks cost $1 billion per year.

Is Cyber Risk in your risk register? Does your business continuity depend on accessing your data?

What to do when you are hit

1. Update your systems and security software as per items 1. and 2. below.
2. Isolate infected systems and remove the ransomware (e.g. email). If necessary completely rebuild the infected systems from trusted sources.
3. Restore the affected data from the most recent backup.
4. Leave paying the ransom as a last resort. While not in any way palatable, sometimes a situation may exist where the loss of the data to your organisation is too great and you have no other way to gain access to the data. Be aware though, that paying the ransom, is no guarantee that the perpetrator will actually give you the decryption code once you pay, although this is not a common practice.

Boards, Audit Committees and Executive...

If you don't want to be held to ransom it is time to revisit your IT security risks.

Hints on how to protect your business

1. Ensure you keep all systems/hardware updated in a timely manner with vendor issued updates such as Microsoft's April and May security updates. This will help remove vulnerabilities so that ransomware cannot exploit them to gain access to your data.
2. Ensure your anti-virus and intrusion prevention features are fully enabled and configured to automatically conduct regular scans. This will help you detect the presence of ransomware in your environment and hopefully block or remove it.
3. Restrict user access rights according to data sensitivity and importance. This will limit the amount of data that may be affected.
4. For those store who data in the cloud, seek assurances from your provider that the patches are up-to-date and the datacentre annual audits have been undertaken. You should also confirm your IT service agreements are signed and data back-up times fit your IT recovery requirements.
5. Educate your users on how to identify, report and treat suspicious emails and websites.
6. Subscribe to a vulnerability and threat alerting service such as the AusCERT Security Bulletin Service at https://www.auscert.org.au/services/it-security-advice. This will give you early warning of vulnerabilities and threats that may impact your organisation.
7. Maintain regular offline data backups. These will provide you with a mechanism to restore data that has been locked up by the ransomware. But note it must be kept safely offline so ransomware cannot lock this up as well.
8. Have a reputable IT security company assess your IT environmental security controls, to help you identify weaknesses and recommend improvements.
9. Review your insurances. The likelihood of becoming a victim is very real and very immediate. The cost of recovering from an attack is likely to be significant. It is usual that Cyber Insurance is a policy extension. You should check to confirm that your policy covers cyber theft, extortion and business interruption.

Certitude
TECHNOLOGY RISK SERVICES

Have concerns about cyber security? *Eric Keser, CEO of Certitude supports JNW clients manage their IT risks. Certitude is a specilist IT security consulting company that helps businesses identify and manage IT security threats. It's consultants each have over 20 years experience in IT security across all industries and size. Contact Eric on* ***(03) 8610 6700*** *or visit www.certitude.com.au.*

JNW STRATEGIC CONSULTING
Business Process Risk Professionals

Valued Risk Insights through:
- Experience
- Professionalism
- Industry Expertise
- Personal Delivery

Contact Us: Jeff Webb
Managing Director
m. +61 0437 539 015
e. jeffwebb@jnwstrategic.com.au
w. jnwstrategic.com.au

Take a look at our website:
www.jnwstrategic.com.au