Ransomware
The Cyber Legal Playbook

Infecting systems with ransomware has become a solid revenue model for criminals in recent years. Security measures are crucial, but can never reduce the risk to zero. To help organisations prepare for a potential attack, we list five action points that should be included in your cyber legal playbook.

1. Arrange legal privilege
The risk of claims or administrative fines almost always exists when you are hit by ransomware. Either because the continuity of business operations is threatened, or because data is stolen. Discuss the incident and the plan of action in a privileged setting with an attorney-at-law.

2. Prepare trigger list
Identify which obligations, both statutory and contractual, apply to the incident. For example, the obligation to report the incident to regulatory agencies, law enforcement, the insurer, data subjects, and customers and suppliers. Secure evidence and document your decision making.

3. Negotiate, if necessary
You have considered the availability of backups and the use of decryption software and decide to negotiate with the attackers. Keep in mind that demands are generally negotiated down, request proof of encryption keys and stolen data, and make a test payment first.

4. Perform sanctions check
In 2020, the EU imposed the first-ever sanctions regime against organisations that carry out cyber attacks. Facilitating ransomware payments carries the risk of violating these regimes. Always perform a sanctions check before making ransomware payments.

5. Evaluate and coordinate findings
Keep in mind the reports of forensic IT consultants can leak and end up with third parties. Before these reports become final, evaluate whether the content is accurate and balanced and whether it can lead to liability.

For more information:
Jeroen van Helden
Attorney-at-law IT, Privacy & Cybersecurity
j.vanhelden@declercq.com
www.declercq.com

DECLERCQ
Advocaten · Notariaat