Willis Towers Watson

Cyber Insurance 2021

Guidance on a successful cyber insurance placement

Decode secure

This page intentionally blank

General guidance for a successful cyber insurance placement 2021

Over the last few years, the world has seen a material increase in cyber incidents such as network security breaches, data breaches, extortions (ransomware) and DDoS attacks. As a consequence of this, the demand for cyber insurance is increasing rapidly for smaller as well as for large companies. Due to the development on the claims side, insurance companies are increasingly hesitant to provide certain covers, particularly cover related to ransomware, which for many companies is the main reason for buying cyber insurance in the first place. Those insurance companies that still do offer full cover for ransomware related incidents require more information before offering terms than what they have historically. This applies for current buyers of cyber insurance as well, albeit not to the same extent. Renewal offers typically come with premium increases, often between 20% - 60% compared to current premiums, sometimes even more than so.

This document is meant to clarify which requirements typically are considered important to insurance companies, in order for prospective buyers to understand if they meet the expectations of insurers. This will enable such companies to prepare themselves for a tender process for cyber insurance, without disclosing sensitive information before it is necessary and to avoid presenting themselves to the insurance market as a less than optimal risk.

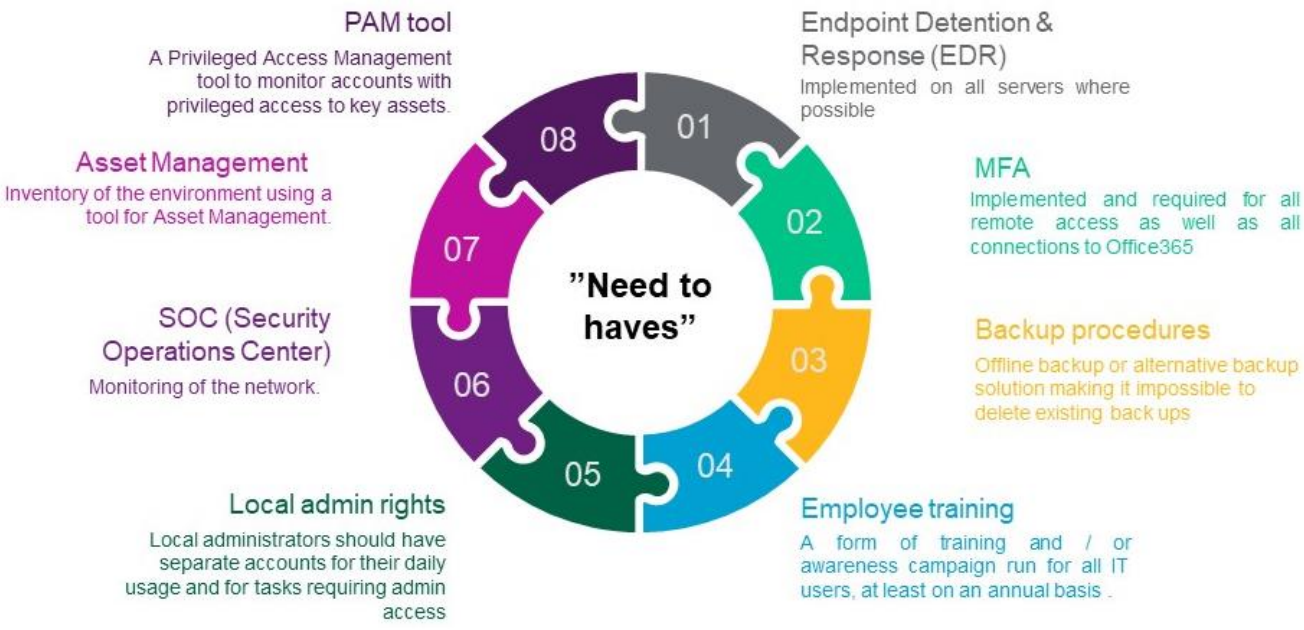
It is also provided to existing buyers of cyber insurance, to help prepare for a successful renewal process. Some insurers will require that additional technical measures be put in place to offer renewal terms. Such measures may take some time to implement, and it's important to review the cyber posture against the requirements from each insurer.

The requirements outlined in this document are based on what insurance companies have outlined as important points in their cyber underwriting processes for Scandinavian clients. The requirements are relevant as of Q2 2021, and will likely change as the frequency, severity and complexity of cyber-attacks continue to evolve. Meeting these requirements will first and foremost make the companies stronger from a cyber security perspective, but also enable customers to successfully negotiate with insurers in acquiring cyber insurance. Meeting these requirements does not guarantee that all companies will be provided quotes for cyber insurance, but it certainly increases the possibility.

It's also important to note that meeting these requirements does not guarantee that a company will be safe from cyber-attacks, but it will make the company stronger and more resilient and help in the battle against cybercrime.

General requirements (“need to haves”):

The list below comprises a high-level summary of requests for information that most insurance companies currently see as minimum requirements for large companies. In short, large companies that don’t have the below controls and technical solutions in place risk being considered below average from a risk perspective. They base this position on experience from thousands of insured cyber incidents, looking at which risk mitigating actions, tools and technical solutions that have real effect on the ability to prevent and withstand cyber-attacks.



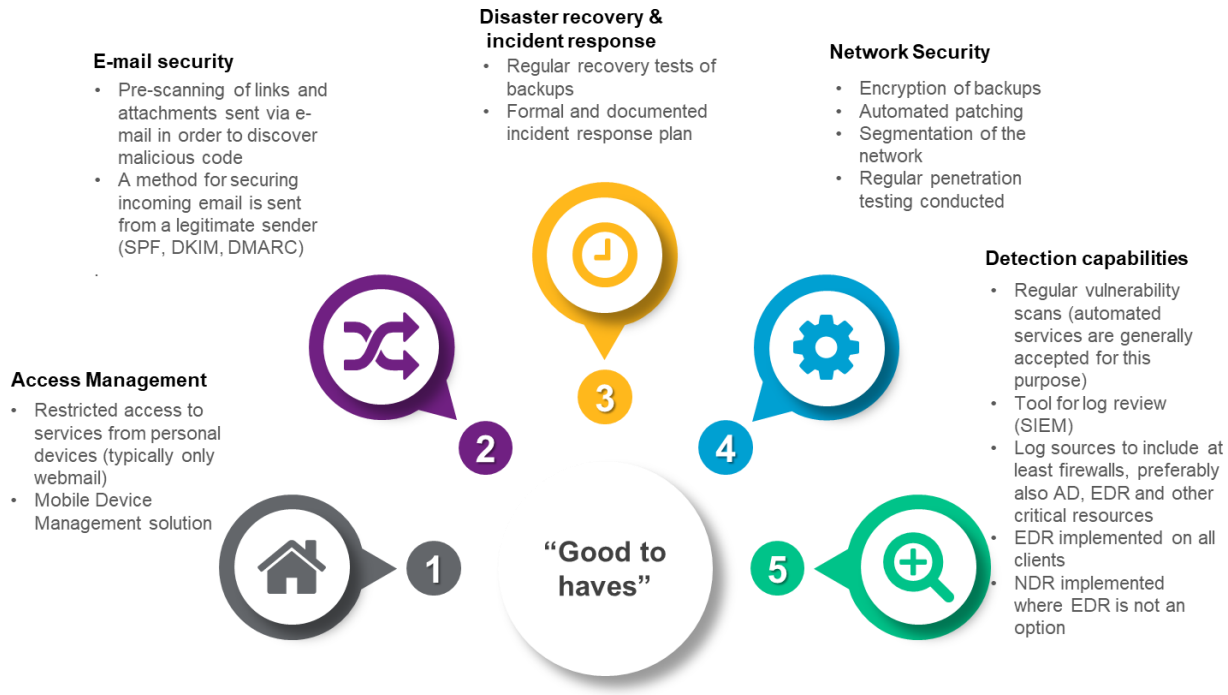
1. An Endpoint Detection & Response (EDR) solution is implemented on all servers where possible
2. Multi-factor authentication (MFA) is implemented and required for all remote access the corporate network as well as all connections to Office365.
3. Backups are stored off-site and offline, completely separated from your production environment.
4. Some form of training and / or awareness campaign is provided and mandatory for all IT users, at least on an annual basis.
5. Local administrator privileges are either issued on a temporary basis, or users with such privileges should have separate accounts for their daily usage and for tasks requiring elevated privileges.
6. Monitoring of the network is performed by a Security Operations Center (SOC) *
7. Inventory of the environment is conducted using a tool for Asset Management.
8. A Privileged Access Management tool (PAM) is implemented to monitor and control accounts with privileged access to key assets in the IT estate. *

* SOC monitoring and PAM tools are not necessarily required for companies with revenues below 1 billion SEK/NOK/DKK or equivalent, or with no presence outside of Scandinavia in order to qualify for cyber insurance, but these measures are still valuable for all companies regardless of size in order to reduce cyber risks.

General “good to haves” measures:

In addition to the necessary requirements, there are a number of points that are normally not seen as definite requirements, but as risk improving measures that the insurers will take into consideration in their underwriting. The more of these improvements can be shown to have been completed or in progress, the better the possibilities for a successful tender.

Recently, insurers have begun requesting that their clients implement and follow up on a cyber security baseline, ensuring cyber hygiene throughout the organization. We believe that this is a very useful step for organisations to take, and we have worked with several of our clients to establish such baselines.



1. Pre-scanning of links and attachments sent via e-mail is done in order to discover malicious code and websites.
2. Regular vulnerability scans are done on all websites and external facing assets.
3. Logs are reviewed using an automated tool for log review (SIEM).
4. Log sources reviewed in the SIEM include at least firewalls, preferably also AD, EDR, Domain Controllers and other critical assets.
5. EDR is implemented on all clients throughout the network.
6. A Network Detection & Response (NDR) solution is implemented where EDR is not an option.
7. A method is deployed for securing that incoming emails are sent from a legitimate sender (such as SPF or DKIM, or domain protecting protocols such as DMARC).
8. Access to services from personal devices (BYOD) is restricted. If BYOD is allowed, a very limited number of company assets is available (ie webmail).
9. A Mobile Device Management (MDM) solution is implemented on all phones and tablets.
10. Backups are encrypted at rest.
11. Regular recovery tests are conducted on large parts of the network, not just individual files.
12. Patching is done on an automated basis, wherever possible.
13. The network is segmented in sections to ensure that a single incident doesn’t affect the entire estate.
14. A formal and documented incident response plan is in place and approved by the board and/or executive management.
15. Regular penetration testing is conducted on various assets across the estate.

This document has been prepared for general purposes only and does not purport to be and is not a substitute for specific professional advice. While the matters identified are believed to be generally correct, before any specific action is taken, specific advice on the circumstances in question should be obtained.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Willis Towers Watson