MARSH

Being held to ransomware? Here's how to move forward

The pace of technological change is increasing, and dramatically transforming the global business environment. At the same time, the potential cyber and technology exposures that businesses face continue to expand, presenting businesses with the possibility of substantial economic losses.

Marsh's deep experience in the field means that we are in a position to **offer best practices** to **help companies** better **understand, measure and manage** ransomware risk.

1. Understand: what are we talking about?

Ransomware attacks aim to hold company data hostage (for instance by encrypting it or by threatening to make the data public) – asking for a ransom payment in exchange.

Attacks are becoming more **frequent,** aided by new types of ransomw are and malware.

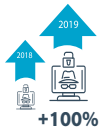
COVID-19-related topics in phishing emails are targeting remote workers.

With more people working in less secure **cybersecurity environments**, attacks are more successful.

Based on all cyber claims that Marsh analysed, **67%** of attacks **were malicious.**

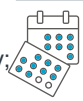
Operational and financial **severity** are rising sharply: ransom demands, related costs, and operational downtime are all growing exponentially.

The number of ransomware claims notifications **doubled** during 2019.



Length of this **business interruption**
A "simple" cyber-attack:
1 week to full recovery.

An "advanced" cyber-attack:
3-4 weeks to core infrastructure recovery;
6 weeks to data re-import.



Source: The Changing Face of Cyber Claims, 2020

MARSH & McLENNAN COMPANIES

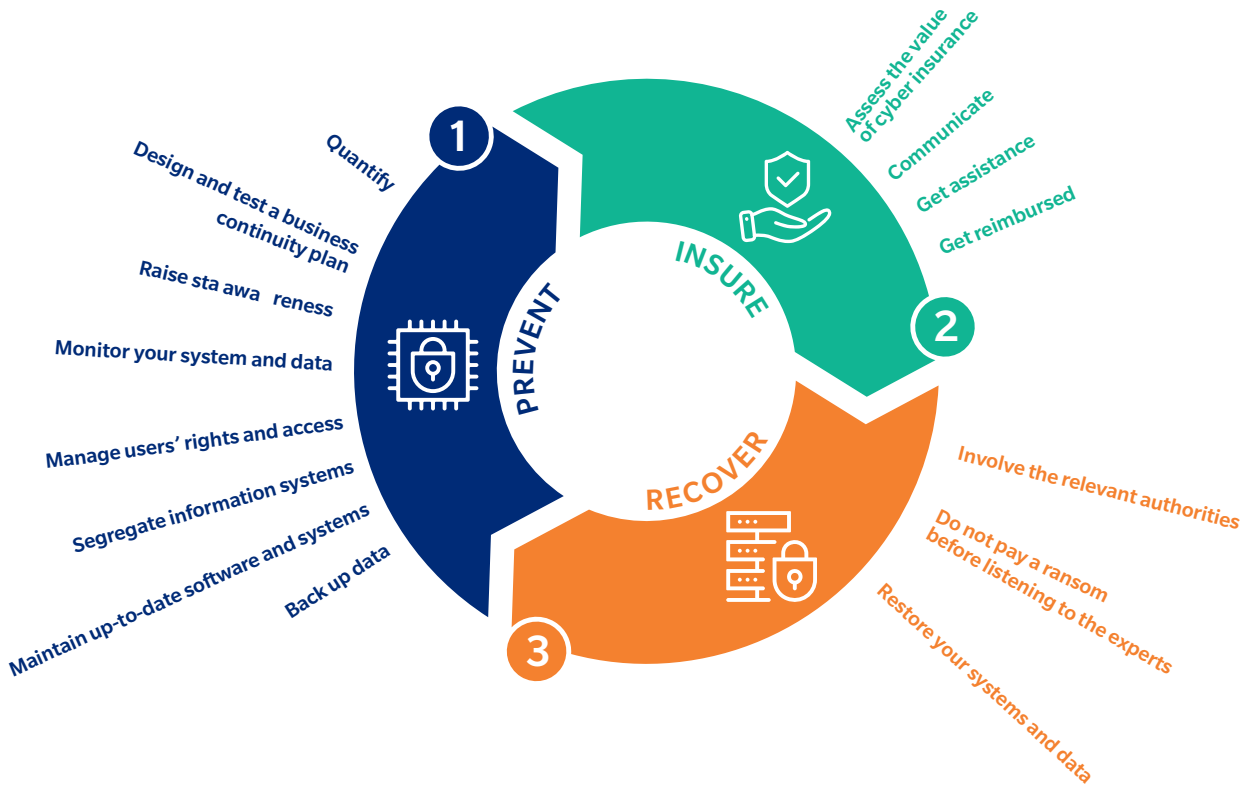
2. Measure: what is the cost of such event

There are two types of ransomware:

- **Untargeted ransomware.** Randomly sent to millions of email addresses and mainly hitting SME and individuals. The mechanism is basic and the ransom amount limited (averaging around 300€, in bitcoin) but the return on investment for hackers is huge, based on the sheer number paying the ransom. Volume is the focus here.
- **Targeted ransomware.** These attacks, far less numerous, are prepared well in advance by hackers, usually thanks to social engineering. Large companies are targeted (> 500M€ turnover) and hackers purposely pull the trigger at the worst possible moment for the company. We are talking of ransoms up to several dozens of millions of euros.

3. Manage: prevent, insure, recover

The following tips can help protect your assets from these very real threats:



PREVENT

1. **Backup data:** the purpose of most ransomware is to prevent you from accessing your data and paying for its recovery. It is essential for your business to make regular backups and to keep it safe. And regularly test the accuracy of your backups!
2. **Maintain up-to-date software and systems:** your information system is vulnerable and its weak points are used by hackers to spread the virus and encrypt your data. By updating it, including our antivirus software, you are more secure.
3. **Segregate information systems:** some parts of your data and information systems are more critical or sensitive than others. Make sure these elements are well protected so the hackers are not handed easy entry.
4. **Manage users' rights and access:** not every employee or partner should be able to get into your system. Good admin and housekeeping is king.
5. **Monitor your system and data:** so you can detect as soon as possible any abnormal behaviour on your systems – meaning quicker reaction times and greater prevention from harm.
6. **Raise staff awareness:** Make your people your best weapon against threats. Ransomware attacks often start because a member of the team opens a malicious attachment or lands on a malicious web page.
7. **Design and test a business continuity plan:** attacks are destabilising. Fail to prepare means prepare to fail: the best way to deal with them is by preparing, including setting up incident response planning and procedures.
8. **Quantify:** knowledge rules, so find out how much a cyber-attack could cost you. This will help you manage the risk at board level, and transfer it to third parties such as insurers.

INSURE

to help you through a crisis and support your financial recover

1. **Assess the value of cyber insurance:** cyber insurance can get you quick assistance during and after the attack, and also seek out compensation for your financial losses.
2. **Communicate:** after a security event, companies need to gain back the trust of their clients, employees and partners. Specialists are best placed to help rebuild a robust reputation.
3. **Get assistance:** many companies do not have the internal resources or the expertise to manage a security incident. Specialist service providers help you to minimise the damage and get you back to business as quickly as possible. Forensic analysis of larger events can help you understand the root cause of why the attack was successful, take appropriate measures to recover – and also help you be more robust in the future.
4. **Get reimbursed:** cyber insurance will mitigate the impact on a company's P&L.

   It can help them avoid a profit warning - or even bankruptcy following the most severe cyber events.

RECOVER

improve yourself!

1. **Involve the relevant authorities:** they can assist you in investigating and recovering from an incident. Most of our clients in that situation have indeed moved to file it.
2. **Do not pay a ransom before listening to the experts:** there's no guarantee that the criminals will hand over the encryption key when you pay up – they are crooks after all! Moreover, if your organisation is seen to be willing to pay, that will probably encourage more attacks, either by the same group or others – and they will be even more sophisticated.
3. **Restore your systems and data:** it is best to restore your system and data from trusted sources and update your passwords. It is essential to check that the data you restore is integral.

For more information about Cyber insurance and other solutions from Marsh, visit marsh.com, or contact your local Marsh representative.

SIMON BELL
Financial and Professional Lines Leader
Middle East and North Africa
+971 50 450 1935
Simon.Bell@marsh.com

PEPIJN DE JONG
Cyber Resilience Practice Leader
Middle East and North Africa
+971 50 489 0486
Pepijn.De-Jong@marsh.com

SARAH HAMLAT
Cyber Insurance Specialist
Middle East and North Africa
+971 56 388 0865
Sarah.hamlat@marsh.com

ABOUT MARSH

Marsh is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services.

Marsh is a business of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue approaching US$17 billion and 76,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer, and Oliver Wyman.

Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube , or subscribe to BRINK.