



CYBER SECURITY – THE INCREASING THREAT TO YOUR BUSINESS

At the last count, it was estimated that Friday's cyber attack impacted upon 200,000 victims in at least 150 countries. The attack used "WannaCry" malware to disable computer systems and present users with a ransom demand. The systems which suffered the attacks are said to have been vulnerable as they were operating outdated legacy software and because security upgrades had not been properly installed. At the time of writing this article, there is concern that the actual scale of this attack may not yet be known.

There has been a tendency by some in the shipping, ports, offshore and logistics industries to suggest that cyber security is not a real concern and that a cyber attack on their business is unlikely. However, this attack did not discriminate between the private and public sectors and it is likely that a number of shipping companies have been affected. Known victims of the attack are said to include:

1. The British National Health Service where 48 trusts were affected and seven are still trying to restore systems (at the time of publication).
2. Renault who halted manufacture at plants in France and Romania to prevent the spread of the malware.
3. The German rail operator Deutsche Bahn who reported that some electronic announcement signs were infected.
4. International express business FedEx Corp which said that some of its systems were breached.
5. Telecommunications companies including Telefonica in Spain and Telecom in Portugal.

For these companies and many others, the weekend will have been spent frantically trying to identify where their operations were exposed, patching and restoring systems using back-ups, mitigating the risk of further breaches and trying



It is now clear that no industry, however sophisticated, can consider itself immune from a cyber attack. The shipping, ports, offshore and logistics industries, with their reliance on electronic operations, have long been identified as being particularly vulnerable.

MATTHEW MONTGOMERY, SENIOR ASSOCIATE

to reassure customers and contractual counterparties that matters are under control. For many companies, repairing the damage of this attack may take several weeks if not months. Repairing the damage to a company's reputation may take even longer.

It is now clear that no industry, however sophisticated, can consider itself immune from a cyber attack. The shipping, ports, offshore and logistics industries, with their reliance on electronic operations, have long been identified as being particularly vulnerable. If the industry needed a wake up call then perhaps this was it.

Shipping and logistics operators, offshore suppliers and ports and terminal operators should now be scrutinising their systems and operations to ensure that they have taken the necessary precautions to protect their business. Although there is little by way of national or international cyber legislation, there are now various guidelines, principles and recommendations that can assist with this process. Taking a pro-active response to risk also involves reducing

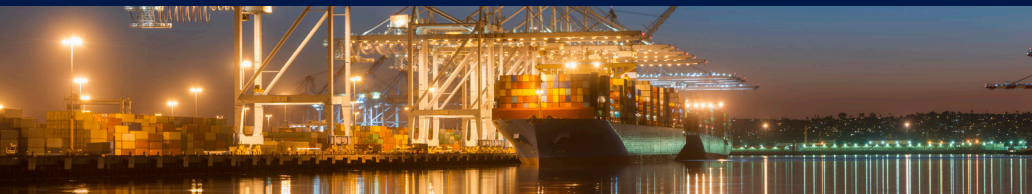
the 'human threat' by educating employees and crews about the threat and how it may manifest itself. Identifying the risk and mitigating it should go hand in hand.

If they have not done so already, shipping, offshore, ports and logistics companies should be:

1. Identifying the areas where they are exposed to cyber risks and vulnerabilities in the supply chain.
2. Developing and testing written information security and incident response plans.
3. Putting the incident response team through simulated exercises to see where the 'gaps' are.
4. Making sure that suitable insurance (or contractual protection) is in place to cover any 'gaps' in cyber security.

Depending on the nature of the breach, there may be also be mandatory regulatory requirements which will need to be understood and acted upon.

HFW is a leading sector focused law firm with particular expertise in maritime crisis management and is able to assist you with your cyber security needs. We can help with crisis planning to avoid breaches and minimise their effects after a breach has occurred.



For more information, please contact the author of this briefing:

Matthew Montgomery

Senior Associate, London

T: +44 (0)20 7264 8403

E: matthew.montgomery@hfw.com

HFW has over 450 lawyers working in offices across Australia, Asia, the Middle East, Europe and the Americas. For further information about shipping issues in other jurisdictions, please contact:

Craig Neame

Partner, London

T: +44 (0)20 7264 8338

E: craig.neame@hfw.com

Toby Stephens

Partner, London

T: +44 (0)20 7264 8366

E: toby.stephens@hfw.com

Peter Schwartz

Consultant, London

T: +44 (0)20 7264 8171

E: peter.schwartz@hfw.com

Stanislas Lequette

Partner, Paris

T: +33 1 44 94 40 50

E: stanislas.lequette@hfw.com

Pierre Frühling

Partner, Brussels

T: +32 (0) 2643 3406

E: pierre.fruhling@hfw.com

Michael Buisset

Partner, Geneva

T: +41 (0)22 322 4801

E: michael.buisset@hfw.com

Dimitri Vassos

Partner, Piraeus

T: +30 210 429 3978

E: dimitri.vassos@hfw.com

Ziad El-Khoury

Partner, Beirut

T: +961 3 030 390

E: ziad.elkhoury@hfw.com

Wissam Hachem

Partner, Riyadh

T: +966 11 276 7372

E: wissam.hachem@hfw.com

Rula Dajani Abuljebain

Partner, Kuwait

T: +965 9733 7400

E: rula.dajaniabuljebain@hfw.com

Yaman Al Hawamdeh

Partner, Dubai

T: +971 4 423 0531

E: yaman.alhawamdeh@hfw.com

Paul Apostolis

Partner, Singapore

T: +65 6411 5343

E: paul.apostolis@hfw.com

Christopher Chan

Partner, Hong Kong

T: +852 3983 7638

E: christopher.chan@hfw.com

Nick Poynder

Partner, Shanghai

T: +86 21 2080 1001

E: nicholas.poynder@hfw.com

Hazel Brewer

Partner, Perth

T: +61 (0)8 9422 4702

E: hazel.brewer@hfw.com

Gavin Valley

Partner, Melbourne

T: +61 (0)3 8601 4523

E: gavin.valley@hfw.com

Stephen Thompson

Partner, Sydney

T: +61 (0)2 9320 4646

E: stephen.thompson@hfw.com

Glenn Legge

Partner, Houston

T: +1 (713) 706-1941

E: glenn.legge@hfw.com

Jeremy Shebson

Partner, São Paulo

T: +55 (11) 3179 2903

E: jeremy.shebson@hfw.com

Lawyers for international commerce

hfw.com

© 2017 Holman Fenwick Willan LLP. All rights reserved

Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice.

Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you. To correct your personal details or change your mailing preferences please contact Souhir Jemai on +44 (0)20 7264 8415 or email souhir.jemai@hfw.com

Houston São Paulo London Paris Brussels Geneva Piraeus Beirut Riyadh Kuwait Dubai
Singapore Hong Kong Shanghai Perth Melbourne Sydney