ASTARA
COMPANY LIMITED

LMA 5403

A LOST OPPORTUNITY?

July 2020

#ResilienceandRecovery

#ResilienceandRecovery

LMA 5403 – an opportunity lost

LMA 5403, issued by Lloyds on 11 November 2019, was introduced to provide clarity to the insurance market. It is a partial step in the right direction in terms of trying to make explicit the limit or extent of cyber cover. But in doing so it risks causing further confusion, with no definition of the important word "harm"; nor does it deal with negligence or accident. Furthermore, it ignores the significance of the Head Office for the cyber security of the vessel and raises serious questions about responsibility. The maritime market needs and requires better: clear policy language and affirmative cyber cover.

Goodbye CL380!

To combat the unquantifiable risk of quote silent cyber unquote, Insurers used the old CL380 text as a means excluding cyber risk from policies. CL380 was however not as clear-cut or all-encompassing as originally thought, since it only dealt with physical damage. In the shipping world physical damage caused by a cyber-attack is very rare but there are many other scenarios where CL380 would not have responded in either exclusion mode or buyback mode.

Despite this, companies have paid not insignificant sums of money to write back the CL380 exclusion into their policy so there was at least some modicum of cyber cover but with limited useful insurance cover being bought. As attacks grow in number and sophistication, the inadequacy of using CL380 is clear.

What's the issue with LMA 5403?

The wording in LMA 5403 contains the word 'harm'. This means different things to different people. The dictionary definition refers to damage or injury; The Computer Misuse Act 1990 refers to unauthorised use of computers, causing damage either material otherwise, and including creating dangers to human welfare, the environment, the economy and or national security. In other legislation, harm was defined as the physical or other injury or damage.

Also, as with CL380, LMA 5403 itself is silent on the role of the Head Office in acting as a vector for an attack from outside, a victim of an attack or the source of an attack.

Who is actually responsible?

'As a means of inflicting harm': In part there is a question about culpability. The attacker may wish to inflict harm, but can only do so if we let him. Look at these examples:

- If the user is improperly trained and ignorantly clicks on a link which releases a malware attack that cripples the company, would this be covered under a buyback of LMA 5403? By their negligence, harm has been done, even if they are not the beneficiary of the attack.
- If the company fails to patch a system that they know to be compromised, or permit access to malicious code because they have not invested in appropriate defence, who is more harmful? The short-sighted system owners or the hacker?

If you are attacked, and the attack is successful at damaging your systems, business, whatever – who is responsible? The hacker, or the executive team for failing to plug a gap they knew was there, they knew was serious and they knew was urgent.

According to Verizon in their Data Breach Investigations Report 2020, insiders – malicious or negligent – were responsible for 30% of the 3,950 breaches covered. More than two-thirds of these breaches were caused by user error.

Figure 2. What tactics are utilized? (Actions)

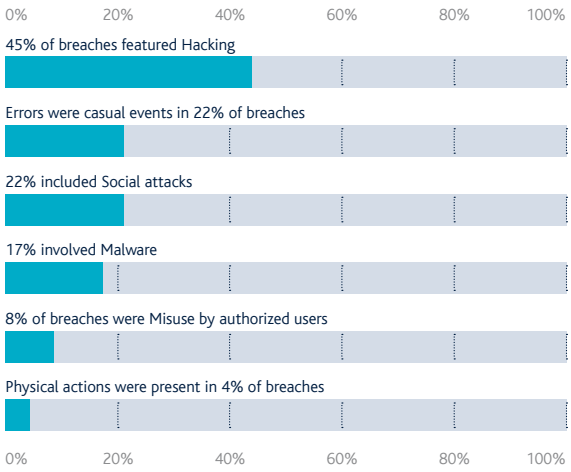
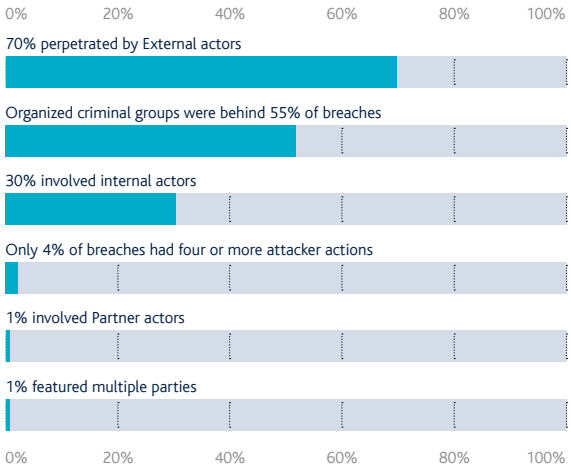


Figure 3. Who's behind the breaches?



This indicates either a lack of training and/or a lack of care in the leaking organisation. The malware numbers also suggest an endemic lack of awareness of the triggers for malware. The fact that hacking forms 45% of the total suggests that almost half of the breaches relied on exploiting vulnerabilities that already existed and which should have either been patched or segregated off the main network system vulnerable to a cyber-attack.

As a board, if your IT director/ Chief Information Officer tells you that a critical system has a vulnerability that needs to be patched urgently, there are a number of options before you.

- you could decide to ignore them and trust to luck;
- you could agree to the patch whatever the operational disruption;
- you could ask that alternative measures be taken to protect the vulnerable system short of putting the patch on

If you decide to do nothing, or to delay, you are rendering that system vulnerable to a cyber-attack.

If you are attacked, and the attack is successful at damaging your systems, business, whatever – who is responsible? The hacker, or the executive team for failing to plug a gap they knew was there, they knew was serious and they knew was urgent?

Negligence versus ignorance

Ultimately, organisations have to accept responsibility that in 30% of cases their users are a material vector for the hacker. While the intention of LMA 5403 is to push responsibility onto the originators of the attack, i.e. those who are deliberately seeking to subvert our computer defences for their own purposes, we have to accept that organisations that adopt poor cyber security habits are complicit in creating or inflicting harm on their own organisations.

This may be unpalatable, but it is incumbent on the leadership of every organisation to manage the risks to their assets, be they logical, physical, or financial, to the best of their ability.

Charts (c) Verizon2020

Leadership matters in cyber, as anywhere else

It is difficult being a leader. The weight of decision-making, striking the endless balance between opportunity and cost, all make for difficult decisions. As a leader, the responsibility for the success or failure of your business lies with you. Your people will look to you for guidance and will regard your behaviour and that of your board as the benchmark.

If your board fails to display the necessary behaviours to protect your information asset-base, you stand no chance of successfully protecting your organisation. Your people will take unjustified risks with your IT systems, and won't care if you get hit. Failure of leadership is the harm that allows the hacker to win.

Be aware – the harm may not be visible immediately

In some cases, the hacker wants the damage to be visible – maybe for bragging rights, maybe for political motives. But in other cases, particularly where intellectual property theft is concerned, the hacker may wish to move stealthily, not be identified, and be able to make their entry and exit without detection. In such asymptomatic cases, the harm may not be visible for many years. Or if it is, the cost of the harm is incalculable. In a shipping company context this may manifest itself as increasingly successful competition driven by theft of your pricing data or some other attack that erodes your competitive edge. In other words, by acting now you can prevent losses in the future

Cyber-attacks: no longer the victimless crime?

Boards find cyber security difficult: they can't tell when they are going to be attacked, and they can't tell in advance what the impact will be. All they know is that cyber security costs money, and that money detracts from the bottom line. Many boards tend to regard information losses as victimless crimes. Despite their policies and procedures, security breaches at senior levels are rarely followed up.

With new regulations in development or place, including in the UK for example the new Data Protection Act (DPA 2018), governments are increasingly able to impose swingeing fines on companies that lose personal data. An institutional shareholder therefore has to ask themselves a serious question: if one of my investments suffers a major cyber breach, their share price drops and they get hit by an enormous fine, who is responsible for the harm?

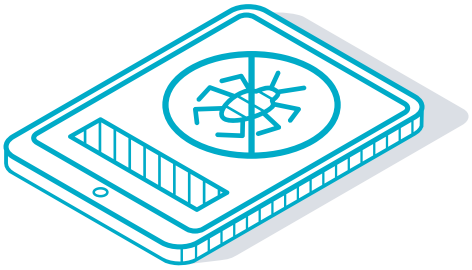
The investor might decide that the management of the company has been incompetent – or negligent - and chose to act accordingly. They may not know the identity of the hackers – but investors certainly know the identity of the CEO.

Can't prevent it – but you can manage it

The only safe assumption for a board is that their company will be hit by a cyber-attack sooner rather than later and that the attack will be serious. If they accept that hypothesis, a number of activities must follow, to create a combination of defence, resilience and response activities.

The CEO needs to be able to reassure investors, both before and in the event of an attack, that the company has the necessary resources to identify when that attack is happening, to limit the damage that an attack can do, and to recover quickly. That is the only way to minimise the harm of an attack.

If you can demonstrate that you have put procedures in place, implemented technical approaches to minimise



the spread and depth of a successful penetration of your perimeter, trained your people to react appropriately, then you have the chance of coming out the other side of an attack, able to reassure your stakeholders that business as usual has been restored and the damage has been contained within known parameters.

Minimising the harm

While it is not in the gift of the board or the IT team to predict when a cyber incident will happen, it is certainly within the gift of the organisation, led by the board, to put measures in place that will minimise the harm or the damage caused by a cyber incident.

In an environment where one knows there are bad actors looking to harm whomever has the temerity to go online, every organisation has the obligation to take the proportionate steps necessary to reduce that risk down to an acceptable level. This includes training, education and awareness raising through to modern intrusion detection & prevention systems, network monitoring and advanced threat protection activities.

Head Office needs to realise that they must also take preventive measures to ensure they cannot damage their fleet's ability to trade.

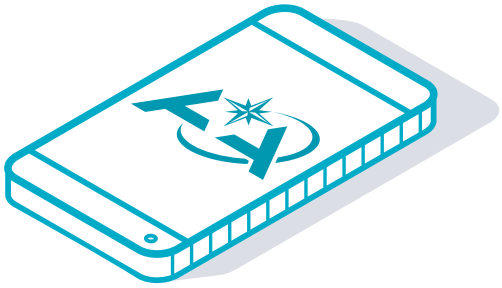
The question for the insurer is therefore not whether an attack was motivated with the intention to inflict harm, but whether the insured took the appropriate steps to defend themselves both on land and on board against something they knew was both possible and likely. In agreeing that an insured can buyback this exclusion, the insurer needs to understand the extent to which the insured is taking cyber security seriously. It's not just about the harm a hacker can inflict; it's about the harm the organisation lets them permit.

Understand what you are buying

All buyers of insurance products with reinstated cyber exclusions must remember that their policies are still subject to all other policy exclusions / restrictions - for example war and terror-caused cyber incidents may still remain excluded in the original non cyber policy. This is evidenced in a move for shipowners to transfer collision (RDC) and dock damage (FFO) coverage to P&I Clubs on the basis that the P&I Clubs do not have a cyber exclusion on the International Group P&I coverage.

Nota bene, the IGP&I coverage does not respond to claims caused or contributed to by war or terror. The most damaging cyber incidents, the most pervasive cyber threats are those which are one state against another; one state acquiring Intellectual Property from another state or private organisation; or one state inducing fear and terror, and then when you perceive you have the cyber cover you may find you do not. This is not the only industry example, it applies to hull, war, LOH, D&O and property insurance, to name but a few.

In the final analysis board members have a responsibility to take all necessary measures to protect their company. By actively managing their cyber risk to prevent a breach happening, and then from the breach becoming catastrophic, they can recover their business quickly. They owe this to their shareholders, bondholders and employees: if they cannot lead the organisation to a safe place, they do not deserve to be leading the organisation.



The Astaara view

The LMA 5403, in our view, fails the test that all modern cyber policies need to pass. The LMA 5403 perpetuates confusion, therefore increases uncertainty and inefficient insurance purchase. There is only one party that loses out, and that is the buyer of insurance.

Has this clause achieved any of its stated aims? In our opinion, no – the clause does not do away with silent cyber, and perhaps more disturbingly does not facilitate affirmative cyber. On the back of this clause, non-cyber underwriters are writing cyber risk blind, which reinforces market indiscipline, and again the buyer is getting second best from the existing insurance market.

The corresponding obligation of the insurance industry is to be bolder and clearer, and with the marine industry there is a real solution – AstaaraCyber. Talk to us about affirmative, clear, calibrated cyber insurance designed for the maritime market that will make a difference between just surviving an incident and coming out the other side stronger.

ASTAARA
COMPANY LIMITED

www.astaara.co.uk

robert.dorey@astaara.co.uk william.egerton@astaara.co.uk james.cooper@astaara.co.uk tom.graham@astaara.co.uk