ARTICLE

Shipping and the perversity of remote working – a cyber criminal's dream we must make a nightmare

Summary

Covid-19 is material. It is forcing all businesses, including maritime companies, to operate differently. Employees are working remotely on a mass scale for the first time globally. This is the implementation of Business Continuity Planning (BCP) / Disaster Recovery (DR) planning on scale never seen before, with the added uncertainty of not knowing when the crisis will end.

Whilst shipping is a global business and remote working is a way of life – ships are the definitive example of a remote office, the Covid-19 restrictions mean that many activities, for example crew change, marine warranty survey or superintendent spot check will be done differently or just may not happen.

This means maritime business are more vulnerable. Criminals realise this and do not care about the human cost of Covid-19, or their crimes. They are not interested in the morality of their action. Instead they are interested in disruption and making money; they see Covid-19 as an opportunity.

The irony of a head office working remotely and the remote operating officers confined mean that owners and operators have to rely more on digital platforms than ever before. Digitisation should come of age in this crisis as being the only way to operate effectively with management exerting, and evidencing, control over operations.

What we know:

- Disruption caused by the virus leaves systems, properties and data at heightened risk
- Expect attacks on systems to increase as the disease progresses

We can take active steps to respond to this

- Working at home doesn't mean forget security
- Recognise the threat and be more vigilant to phishing and spoofing
- Deploy as mandatory multifactor authentication for payments
- Review, improve and update your BCP/DR as you learn how to work remotely
- Heed your own IT Department, they are there to help you and your business
- Keep your devices up-to-date, basic cyber hygiene is paramount
- Ensure you use a VPN
- Your children (and family) should not use work computers for their own purposes.

Detail

Wherever there is human misery, there are profiteers exploiting it. Criminals see opportunity in ways most right-thinking people simply would not - the recent ransomware attack on a Czech hospital at nearly peak capacity dealing with Covid 19 patients is the depressing evidence of this despicable behaviour. Opportunity takes many forms, but the motive is singular and morality-free: profit at lowest cost.

The global pandemic caused by COVID-19 is no different. With the emphasis on no social contact, schools and universities closing, pubs and bars emptying, life is moving inexorably from the physical domain to the virtual. BCP/DR has been invoked – instead of Bring Your Own Device (BYOD), it's Take Your Laptop Home (TYLH) time.

Thereby hangs the problem: working at home, whatever the public health benefits, is less secure than working in an office environment. Hackers welcome home-working: it isolates workers, breaks up teams, changes peoples' mentalities, and weakens organisational security. Home technology environments are rarely as robust as corporate infrastructures. While use of Virtual Private Networks (VPN) is growing fast (54.3% growth YoY 2018-2019)[1],

[1] top10vpn.com

security controls in a domestic environment are likely to be weaker than in an office, since the risk is perceived as lower.

There are likely to be major gaps in, for example, access control, network security, clear desk policies, back-ups and data storage. And these will be the gaps that criminals will try to exploit - to gain access to core systems to allow them to spoof, false invoice, generally socially engineer their way into corporate bank accounts or databases to steal intellectual property residing thereon.

Be aware; heed your IT team

Staff dispersal need not be a problem. It is moments like these when the IT team can become the heroes of the piece rather than the villains. Although themselves dispersed, most IT teams have the capability to monitor activity on corporate systems and are well placed to monitor system usage at the individual and team level.

They can see the facts, exactly where the vulnerabilities lie, and the kinds of behaviour that we need to stop. While management effort is distracted, the IT team can interact with all areas of the business and so can act as proxies to monitor the health of the organisation and identify any hotspots for early, preventive, management interventions.

The IT team will need to be vigilant for signs of reconnaissance and attacks on their system. They also need to work with facilities and physical security to ensure that buildings that are supposedly closed remain so. The IT team needs to ensure that basic cyber hygiene is maintained and that users continue to update their devices with the latest patches to maintain system integrity.

Working at home is work

Home working for those who can relocate their jobs to a home environment can be a boon, and in the case of Covid-19, may be a life saver. This does not mean that IT security rules go out of the window. Basic security principles still must apply: lock your screen when you leave your desk; do not leave your passwords lying around for your children to use; ensure your memory drives are protected by both encryption and password. You know the rest.

Spoofing to misdirect payments has long been a favourite of cyber criminals. Proper control over payments via at least a 2 factor authentication system often relies on wet signatures, where it is practiced. Multi-factor authentication needs to be mandatory, and needs to be structured to work with people in different locations.

More importantly perhaps, people need to work harder to maintain the sense of community when they are separated from colleagues. Good communication is vital. It is easy when alone to believe that the organisation has forgotten you. This can build to feelings of resentment, and it would not be long before an insider event had been triggered.

Given their centrality to ensure effective working on a company on enforced remote working, IT teams can act as the comms hub for an organisation that has dispersed its staff back to their homes. They must be the source of correct information relating to the systems that staff can access.

If staff are taking organisation IT assets to their property to work effectively on office systems, the risk and IT people need to understand that this activity has broadened the attack surface. This does not mean we will automatically lose against motivated enemies. If asset owners, whether official or personal, are more aware of the risks to those assets now and into the future due to this remote working the company can be more resilient.

My enemy's enemy is my friend.

The coronavirus infection will keep us away from our offices for a substantial time. We will be getting used to using either our own computers connected to office systems or office computers using our infrastructure to communicate back to base. We must not forget that if we are using office systems in the home, the acceptable use rules still apply.

Likewise, unsuspecting users of our systems at home may regard our inability to visit certain websites to be problematic. Our internal network people keep us safe from ourselves. They and their IT security counterparts are a thin line of defence indeed. A work system is a work system, not a family one. Your children should not have access, so lock them out!

ARTICLE

Covid-19 and the Maritime industry

Covid-19 impacts the maritime industry like no other. We all expect that the high standards to which the shipping industry operates to be maintained to preserve the integrity of our supply chains and for regulations to be adhered to.

However, under Covid-19 restrictions, surveyors can no longer attend pre-loading surveys; P&I and Hull condition surveys; towage approval surveys; warranty survey on project cargo – the list is long. It is made more complicated that the roving superintendents who are well versed in remote working are now the team member confined.

How does a ship owner or operator manage to maintain the evidence required to support safety on board? How should safety audits be conducted if attendance is prevented by ill health or access suspended. How long can a ship trade without crew changes in the light of quarantine restrictions impacting crew rotations.

The answers stem from truly embracing digitisation. Digitisation can improve the resilience of your digitised assets and the whole shipping enterprise; it should also improve flexibility of operations in respect of ship sourced performance, maintenance, health reporting and increased communications between ship and shore.

Now more than ever the advantages of digitisation should be capable of being realised but only if the corresponding management resilience and recovery plans are in place and practised to ensure those data flows are uninterrupted and uncorrupted.

So whilst the economic pressures will hit the maritime industry along with all other areas of the economy the new approach to remote working needs to be invested in: processes need to reviewed and updated as necessary, training provided, new approaches to monitoring assessed and adopted.

Astaara's View

The world is in for a rough time.

Criminals will be keen to exploit this. We cannot let them win. Black Marketers and profiteers were shot during wartime: this struggle against Covid-19 is a war in a different domain. Life is difficult enough without malicious hackers trying to steal our futures as well as our pasts. Bringing the criminals to justice in this time of global crisis must remain a priority of government enforcement– but this does not help shipping companies operate.

We realise that working at home is not always easy. Digitisation has never been more important. They key is making sure mobile/remote working is done safely and robustly, and there are clear communications of new expectations on employees who are suddenly been asked to change the way they work to ensure that the less robust members of the team do not get left behind

These times of heightened emotions require high levels of engagement between and among colleagues and clients can key our vital supply chains open. Astaara stands ready to help colleagues and clients manage this difficult phase.

Robert Dorey
William Egerton
18th March 2020

Contact

Robert Dorey: robert.dorey@astaara.co.uk +44 (0)7775 515 878
Bill Egerton: william.egerton@astaara.co.uk +44 (0)7747 051 806

#AstaaraCyber #ResilienceandRecovery #marinecyber