#25
DEC: 2018

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

EPSCO-RA
Maritime Cyber Security Solutions

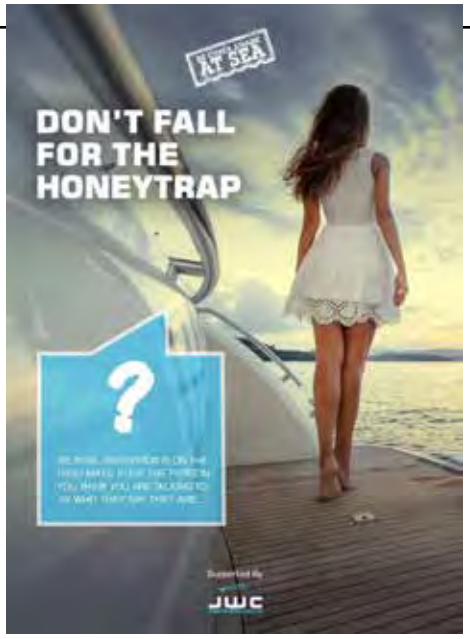
SMART4SEA TRAINING AND EDUCATION AWARD 2018
UNSUNG HERO OF INDUSTRY: HIGHLY COMMENDED, SAFETY AT SEA AWARDS 2017
BEST CYBER AWARENESS CAMPAIGN, INTERNATIONAL CYBER SECURITY AWARDS 2017

2018 Training Award SMART4SEA

Welcome to "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the shipping and offshore industry initiative, "Be Cyber Aware At Sea".

Issue 25 is generously sponsored by Epsco-Ra, a global leading maritime cybersecurity company, providing a comprehensive delivery of cybersecurity consulting and managed services to the international shipping community. Visit www.epsco-ra.com to find out more. You can also read their thoughts on why cybersecurity is not merely an IT issue, and feedback from recent seminars.

Inside you can also read more of the efforts to boost maritime cyber security, more particularly the human element. You can also find out more about the campaign at https://www.becyberawareatsea.com/ Stay safe, stay secure, be cyber aware at sea.



EPSCO - RA
Maritime Cyber Security Solutions

BE CYBER AWARE AT SEA

PEOPLE ARE KEY TO SECURITY

One of the unifying themes for all cybersecurity experts is the fact that the human factor has a huge part to play - both as problem and solution. This is as true ashore in ports, as it is on the ships which visit them.

It is people who are key to preventing a catastrophic and potentially reputation-destroying cybersecurity attack on the ports and terminals of the world.

Port operators are being encouraged to take stock of their workforce, as they look at the basic human vulnerabilities which remain the largest threat to any organisation.

The cyber vulnerabilities which exist need to be acknowledged, understood and mitigated against, and it is an imperative to protecting individuals and organisations alike from the latest cyber security risks.

Speaking to Port Strategy, Protection Group International (PGI) senior cyber threat analyst Olly Jones recently emphasised the fact that while there is undoubtedly an important role for technology to play, the biggest weakness in the defensive chain is "still the individual on the end of a keyboard".

"Even some of the most sophisticated nation state attacks primarily target end users, as it is often far easier to entice an individual to click on a malicious link, rather than to develop and exploit a technical vulnerability in a system," he told the media.

He advises that individuals be more responsible with their online behaviour to help mitigate the cyber risk, both to themselves and the businesses they work for — if an email even seems slightly suspicious or if a link or attachment from a distant or unknown contact seems too good to be true, do not click on it.

Holman Fenwick Willan (HFW) partner Toby Stephens agrees that human behaviour makes ports vulnerable: "Whichever way you look at it, people are known to be your biggest risk in terms of cyber security.

"This can cover a multitude of interpretations and we will leave you to reach your own conclusions, but it extends from those inadvertently introducing risks to systems, right through IT professionals to CIO/CTO level, and whether they are getting senior management onboard and supporting the plans and strategies they have to combat cyber risks," he says.

He concedes that it will take time for the industry to develop and implement strategies to counter growing cyber threats. Indeed, lawyers have seen a general move with some players in the container supply chain revisiting their template contracts to ensure they have general provisions to deal with cyberattacks and tightening up their force majeure provisions.

THE CYBER ELEPHANT IN THE ROOM....

OSM Maritime Group chief technology officer Chakib Abi-Saab believes there is an "elephant in the room" when it comes to digitalisation. Speaking at the Maritime Digital Innovation event in Singapore he said "One of the biggest challenges we face is that many technology leaders fail to understand the business side of their organisation.

"We go to the board of directors and the chief executive and we talk about technology: we talk about speed, we talk about backups.

"We do not talk about the bottom line, we do not talk about competitive advantages, and until we change that and start addressing technology in business terms that make sense for the business, we will not move forward.

"The maritime industry is a business, this is not an area where we allow technology because it's cool," he said.

SINGAPORE EYES NEW TECH ROLE

The inaugural Maritime Digital Innovation Summit took place in Singapore on 14 and 15 November with speakers and delegates from across southeast Asia and further afield coming together to discuss pressing issues related to digitalisation in the maritime sector.

A range of topics were covered but strong trends throughout the two-day conference were cyber risk, additive manufacturing, autonomous shipping and how to increase the uptake of digital solutions.

The first day kicked off with Association of Singapore Marine Industries (ASMI) president Abu Bakar Mohd Nor delivering the opening address. Noting the length of the downturn in the industry, Mr Bakar said "While we see positive signs, we cannot just rely on business as usual.

"Industry must seize more opportunities, especially in the area of innovation and capability improvement."

He gave details of the Industry Transformation Programme being implemented by Singapore's Ministry of Trade and Industry, which seeks to strengthen 23 key sectors of the country's economy through setting out roadmaps known as ITMs for innovation and transformation and deepening partnerships between the public sector, government and industry.

The maritime ITM is led by the Maritime and Port Authority of Singapore, while there is also a marine and offshore engineering ITM being led by ASMI. "The whole idea is to achieve global leadership in smart marine and offshore engineering solutions," Mr Bakar explained.

CLASS WORKS WITH PARTNERS

ClassNK, the Japanese Classification Society which ensures the safety of vessels, has signed a partnership agreement with TÜV Rheinland, a specialist in testing, inspection and certification services.

According to a statement, the two companies will collaborate to provide digital services for safety, cybersecurity and privacy for the maritime sector.

As part of the partnership agreement, both parties will jointly develop and deliver a cybersecurity certification scheme, utilizing expertise gained from each company's range of available services.

In addition to this, ClassNK will work with TÜV Rheinland to establish cybersecurity guidelines that target onboard software currently in development. The partnership is expected to offer the shipping industry efficient and pragmatic certification services that meet current standards of cybersecurity.

Koichi Fujiwara, ClassNK President and CEO, said: "I am pleased to be able to further strengthen our collaborative relationship with TÜV Rheinland.

"Digital transformation is changing the way that business is conducted and offering more opportunities, while cybersecurity is an essential factor to its promotion and adoption in the maritime industry.

"Through the new partnership, we will do everything possible to overcome the cybersecurity challenges of the industry by combining TÜV Rheinland's abundant expertise and our society's accumulated knowledge and experience on management systems for ship operations as well as the structure, machinery and other components of ships themselves."

More details at https://www.classnk.or.jp/

SATELLITE COMMS GIANT EMBRACES NEW CYBER ROLE

Inmarsat has introduced two new components to its maritime cybersecurity service, Fleet Secure, as it continues to develop solutions that combat ever-increasing cyber threats faced by shipowners and ship managers.

Vessel operators will benefit from a powerful, multi-layered endpoint security solution, Fleet Secure Endpoint, which is based on industry leading technology from ESET, a world leader in digital security, and powered by Port-IT and protects desktop computers and other systems connected to a vessel's network.

Fleet Secure Endpoint has been developed to remove infections and thwart hackers before damage occurs to onboard endpoints and connected systems. The solution will be available for commercial use from January 2019 and is compatible across Inmarsat's maritime portfolio of services, including Fleet Xpress, FleetBroadband and Fleet One. It also complements the resilience of Inmarsat's own satellite and ground network enabling consistent cybersecurity standards to be maintained.

Peter Broadhurst, SVP of Safety and Security for Inmarsat Maritime said: "It is a priority for every fleet operator and ship manager - shore-side and at sea - to ensure their systems are properly protected. As this enhancement to Fleet Secure demonstrates, Inmarsat is constantly monitoring the ever changing cybersecurity landscape and devising new tools and approaches for addressing potential problems; ensuring that ships and their crew remain safe –physically and virtually."

Inmarsat has also launched a training app for mobile devices, Fleet Secure Cyber Awareness. This enables seafarers to educate themselves on the tactics that cyber criminals might employ in attempting to infiltrate a company's IT infrastructure.

Addressing the human element is essential to maintaining a strong security posture, says Broadhurst: "Many attempts to gain unauthorised access to IT infrastructure require some sort of activation by an end-user in order to infect a system and cause further damage. These attacks are often heavily disguised so as to trick and manipulate end-users into unwittingly granting permission.

"However, there are nearly always tell-tale signs that, if spotted in time, would prevent escalation. Crew education is therefore an indispensable component in realising a well-rounded security strategy and the reason behind teaming up with Stapleton International and Marine Learning Alliance to launch our Fleet Secure Cyber Awareness module."

THE BIG ONE IS STILL YET TO COME... SO BRACE YOURSELVES

It has not happened yet, but the experts warn that it is coming. The Big One — the worst-case cyber-attack on the shipping industry.

Mark Sutcliffe, director of CSO Alliance, an online community of shipping company security officers, explained the thinking behind the warning. "A worst-case scenario might involve intrusion that invokes a cascade failure of a vessel carrying hazardous or polluting material, or possibly sustained disruption to networked navigational systems that could have an industry-wide impact".

Sutcliffe says most maritime cyber-threats have been confined to distributed-denial-of-service attacks, website defacement and ransomware, but that a cascading intrusion affecting ports worldwide could certainly happen.

"Network intrusion that creates a cascade effect, disrupting systems in a globally important mega-port such as Rotterdam or Singapore, would have [a] significant operational and consequently financial impact on the entire European Union logistics and transport chain," he says. "There is evidence of attacks developing in maturity of approach and impact, for example shipbroker fraud."

Despite the risks, there are no specific laws to prevent cyber-attacks in shipping. But Sutcliffe says organisations such as the IMO, US Coast Guard and the EU are drafting guidelines that might become laws.

"I think it will be a learning curve," he says. "You learn how to address it the best way and then you set laws."

The IMO will need to get more involved in the cyber security issue, says Natasa Pilides, Cyprus' deputy shipping minister

In January, a section dedicated to security, including cyber-risk, was introduced in the third edition of the Oil Companies International Marine Forum's Tanker Management and Self Assessment (TMSA) programme.

The language was also included in the seventh edition of the vessel inspection questionnaire from the forum's Ship Inspection Report Programme (SIRE), made effective in September.

"Because TMSA and SIRE are imperative to gaining charters, tanker operators now have a commercial incentive to demonstrate they have given systematic consideration to potential vulnerabilities and implemented appropriate mitigations and safeguards to address them," DNV GL says in a report on digital defence.

BIMCO NEW CYBER CLAUSE

BIMCO has announced a cybersecurity clause that will require its members to put procedures in place to protect their data systems.

The clause is due to come into effect in May 2019 and is being drafted by a team led by Inga Froysa, the General Counsel at Norwegian shipping company Torvald Klaveness.

Other parties involved in drafting the clause include shipping management service provider Navig8 and maritime insurance firm UK P&I.

It will fulfil two important functions – to raise awareness of the risks of cyber-attacks and to provide a mechanism for ensuring that procedures are strong enough to prevent them from happening.

BIMCO has said the drafting team has discussed if the clause should also address payment fraud, but the conclusion was that this was best dealt with at a procedural level by companies tightening up their internal payment procedures.

In a statement, BIMCO said: "Mitigating the effect of a cyber security breach is of paramount importance and the clause requires the affected party to notify the other party quickly so that they can take any necessary counter-measures.

"The clause is also designed for use in a broad range of contracts. This way, the clause can cover arrangements with third-party service providers, such as brokers and agents."

See www.bimco.org for more details.

COMPANY SUFFERS CYBER ATTACK

Australian ferry and defence shipbuilder Austal recently reported that it has been hit by a cyberattack. An unknown offender managed to steal internal data, including some staff contact information and unspecified data affecting a "small number of stakeholders." The firm emphasised that its ship design drawings for vendors and customers are neither sensitive nor classified, without specifying whether any drawings may have been taken.

Austal said that the attacker attempted to engage in extortion using the stolen information and tried to sell it online. In line with its company policy, Austal did not respond to extortion offers, the firm said.

Austal said there were no indications that the data breach had national security implications. "Austal's business in the United States is unaffected by this issue as the computer systems are not linked," the company said.

The Australian Cyber Security Centre and the Australian Federal Police are investigating the attack, and the Australian Department of Defence is providing technical assistance. "This incident reinforces the serious nature of the cyber security threat faced by defence industry, and the need for industry partners to put in place, and maintain, strong cyber defences," said the Department of Defence in a statement. Austal said that the attack had no effect on its day-to-day operations, and that its data systems have been secured and brought fully back

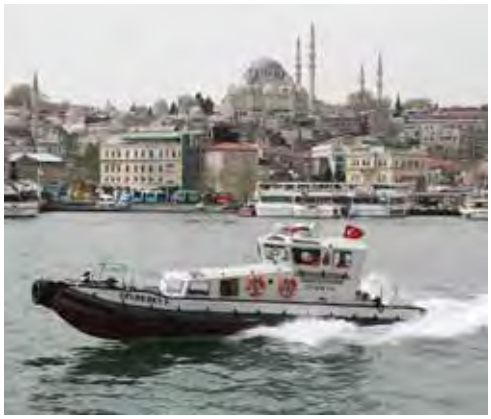
TURKEY FACES THREATS

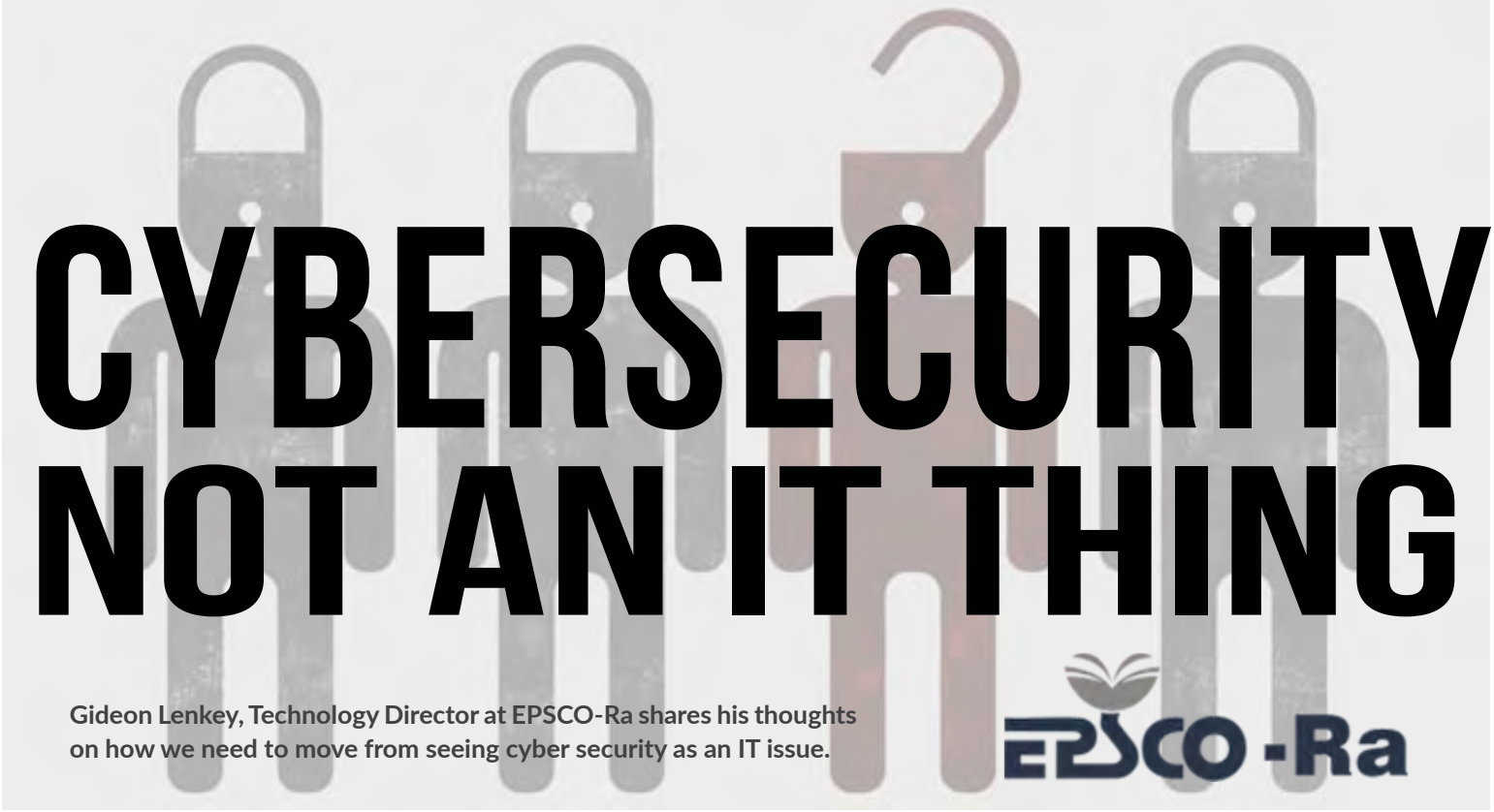
According to Duygu Doğan, Senior Associate at Kılınç Law & Consulting, an Istanbul-based corporate and commercial law firm, Turkey's maritime sector is particularly vulnerable to future attacks.

Turkey has a thriving shipping sector that is continuously growing each year. The shipbuilding, ship breaking and recycling industry is one of the fastest growing sectors in the economy employing more than 300,000 people. However, unlike the US and the EU, there is no dedicated law that governs cybersecurity in Turkey, making shipping companies even more potentially vulnerable to cyber attacks.

Instead, there is the Data Protection Law No. 6698 (DPL), which was introduced in 2016. This serves as an umbrella law for the protection of all personal data by any means, including cyberspace. It contains relevant provisions of international instruments while sectorial regulations form a legal patchwork for cybersecurity. However, Duygu argues, there needs to be more specific domestic legislation that directly regulates illegal cyber activity.

Accordingly, Turkey needs to implement regulations that protect every company in the shipping industry from such pernicious attacks.





CYBERSECURITY NOT AN IT THING

Gideon Lenkey, Technology Director at EPSCO-Ra shares his thoughts on how we need to move from seeing cyber security as an IT issue.

Although for the most part maritime companies are starting to embrace the notion that cyber-enabled systems bring with them an element of risk, real operational risk of expensive downtime, there is still the tendency to approach it as an IT problem. That is to say a technological problem with a technological solution.

This of course is a mistake, an arguably understandable mistake, but a mistake that many companies across many industries have made in the past. Just because using a piece of technology brings risk with it does not mean managing that risk is automatically another piece of technology.

Managing risk is a business process and should include the risk posed by cyber-enabled systems. Ship owners and managers understand risk and deal with it every day, weather, fire, pirates, bunkering to name a few.

Each risk is quantified, some are even regulated, and each owner or manager develops processes to manage them. Take engine room fires as an example, an engine room fire poses a serious risk to a vessel. It can lead to serious damage, expensive down time, loss of life or even loss of the vessel.

Managing a risk like this begins with understanding or at least an awareness of what happens when you don't. This primarily happens when disaster strikes someone else and owners or managers decide they don't want this to happen to them. It can also happen with regulations imposed on behalf of the welfare of others when risk is not properly managed.

With the risk defined then policies, procedures, education and technology are brought to bear on the problem. The policy is to have in place a system to quickly extinguish an engine room fire. In this example let's say the technology is a CO2 system designed to quickly extinguish the fire and the process is a written procedure the crew are trained to follow to extinguish the fire using the CO2 technology. The system must be tested regularly to confirm it works. All of these steps together comprise a risk management process.

So what does a fire suppression system have to do with cybersecurity? Well, let's take a look at a common cybersecurity risk everyone can relate to, the communications PC on the bridge. If this system becomes unavailable or infected with malware it can impact operations in an expensive way. Vessel downtime measured in days is not uncommon. But unlike the mature risk management process for engine room fires, the approach most often seen in the field is one of only deploying the technology component.

In other words, IT is left to deal with it on their own without much real support from management. That would be like just giving the engineer the CO2 system and expecting it to just work without policy, procedures, training or testing. This approach to cybersecurity is indicative of the maturity of cyber risk management in the maritime industry in general.

Ideally, risks posed by cyber-enabled systems are identified though a risk assessment process as part of a regular and ongoing internal risk management practice. With risks properly understood management can decide how much risk they're willing to take and how much they're willing to spend to manage it. That's a pretty solid foundation to build an approach on and more mature than simply reacting to what comes your way.

The next steps are specifying the controls, setting the polices, designing the procedures and then selecting the technology. Did you notice that the technology comes absolutely last? That's because it's a tool to help implement a policy and satisfy a control requirement.

It's not the solution itself and never will be! Finally, the process itself must be tested to document it actually does what it's supposed to and further identify potential gaps. In cybersecurity that means a penetration test, attack simulation or table top exercise. If you're simply specifying technology at the operational level without a process and support from executive management then failure is likely in your future.

If you want to mature your company's cybersecurity practices then look to industries like critical infrastructure or finance and adapt an existing framework like NIST. There is no need to reinvent the wheel but there is a lot of hard work ahead of you. Smart people doing hard work is the secret to a mature and effective cybersecurity management practice and probably always will be.

BV WANTS SMARTER SHIPS

Bureau Veritas' global technology leader for smart ships, Najmeh Masoudi recently spoke on the view from Classification Societies on cyber security and smart shipping.

Ms Masoudi gave updates on smart shipping projects BV is currently involved in and cyber services it provides as well as opining on trends within the sector and offering advice on cyber security. She highlighted that cyber can be broken down into three interacting areas: cyber security, aimed at preventing intentional malicious actions; cyber safety, aimed at preventing accidents and mistakes; and cyber performance, which is aimed at measuring and improving health and performance through data use.

While digitalisation may be here to stay it must be balanced with the human factor, and that innovation is dependent on being able to change established mindsets. The conservative nature of the shipping sector was contrasted with the more relaxed approach to risk taken in the tech sector. A factor that may increase demands was client requirements – charterers may impose requirements for certain technologies to be installed on vessels before they will consider chartering them.

WHY WE ARE LOSING THE CYBER WAR

Epsco-Ra recently held a series of hugely successful Maritime Cyber Security Seminars entitled, "Why We're Losing the Cyber Security War & What You Should be Doing About It"

The progressive seminars were brought to the international shipping community in Hamburg, Germany and Limassol, Cyprus, to great acclaim.

The seminars looked at how shipping companies' operations fail, despite investing money and effort behind cyber security initiatives. They also explained how cyber threats are actually threatening the security of the global maritime industry. However, they stressed that by protecting against such cyber risks, organisations can defend against all types of cyber attacks which impact daily operations on land and at sea.

With offices in USA, Cyprus, Singapore and Germany, offering over twenty years' experience in maritime and security industries, Epsco-Ra is a global leading maritime cybersecurity company, providing a comprehensive delivery of cybersecurity consulting and managed services to the international shipping community.

To find out more about any upcoming seminars for the year ahead, see www.epsco-ra.com

PORTS EMBRACE THE HUMAN ELEMENT

Emphasising that the "human element is huge", American Association of Port Authorities (AAPA) freight and surface transportation policy director John Young has been stressing the positive developments in regard to awareness, education and counter measures.

"Los Angeles, for example ... they have a mobile cyber security operation centre that prevents 15–20 cyber threats each month on their network," he says.

"Certainly, there is more awareness ... great communication with the Coast Guard, the Department of Homeland Security has put out a lot of indicators as to what a clean bill of cyber health should be in this country, not just in maritime, but in general."

Mr Young observes that 85% of AAPA ports anticipate an increase in direct cyber or physical threats to their port over the next ten years. "Cyber is not something that is an annual appropriation — it is something that you work on every day. If you have ever been hacked, then you know the vulnerability that you have.

"As more and more time goes on, and more people are hacked or come to the realisation that they are vulnerable, then that translates into greater security all round."

EPSCO - Ra

Maritime Cyber Security Solutions

Borders...
Defended

Incidents...
Handled

Cyber Security...
Managed

Phone: +357 25 733091 • Email info@epsco-ra.com • www.epsco-ra.com