

CORPORATION NEWS

August 2016 Issue



Tradeshows

IMPA's Second Year in Singapore



BH GLOBAL
CORPORATION LTD

Thank You for Visiting us at 

Please Visit Us At The Following Tradeshows

 <p>Hamburg Messe and Congress Centre, Germany 06 to 9th September 2016 Singapore Pavilion Booth: B7.205</p>	 <p>Malina Bay Sands Expo & Convention Booth: B1-201 Singapore 29 November - 2 December 2016 2016</p>	 <p>Malina Bay Sands Expo & Convention Booth: B2-009 Singapore 25 - 27 April 2017 2017</p>
---	---	---

Website: www.bhglobal.com.sg • Online Store: www.bh-estore.com • Tel: +65 6291 4444 • Email: sales@bhglobal.com.sg

IMPA Singapore 2016 was held on 17th and 18th May at the Grand Copthorne Waterfront Hotel.

Being one of the event sponsor and exhibitor of IMPA's second event in Asia-Pacific, we are quite impressed with what the organisers have put up.

BH Global had the opportunity to speak in two of the strategy session on Day 1. Sharing on 'Green Lighting Solutions' that provides energy efficient and low-maintenance LED lighting solutions as well as 'Maritime Cyber Security' with insights of cyber security and enterprise IT operation management.

Allowing us to re-connect with ship chandlers and other purchasing professionals on which the association has built its reputation on.

BH Global will be showcasing at SMM 2016 on 6th to 9th September at the Hamburg Messe and Congress Centre, Germany. Looking forward to seeing you at Singapore Pavilion, booth B2-205.

Athena Dynamics's Second Year in RSA Conference Asia Pacific Japan



The world's largest info security event which appeals to nearly 30,000 attendees every year. Held on 20th to 22nd July 2016 this year at Marina Bay Sands, Singapore. RSA provides a unique platform to connect, gain insights and stay ahead of cyber threats. It was an engaging 3 days event and had inspired many professionals through exchanging of ideas and learning about the latest trends in this digital world of globalized society.

Always relevant. Always fresh. Always on.



RSA Conference Asia Pacific & Japan 2016 officially kicks off with an opening address from Singapore's Minister for Home Affairs & Minister for Law, Mr. K. Shanmugam. "Cybercrime is seen, and rightly identified, as a growing threat. It doesn't recognise national boundaries. They hide behind, they are in the shadows, and they strike. And the scale and the speed with which they can strike is such that it can cause tremendous damage," he also added that the plan

signifies a fundamental relook at the way cybercrime is tackled, and Singapore will do more in the battle against online crime through a [National Cybercrime Action Plan \(NCAP\)](#).

athena dynamics
A Member of BH GLOBAL CORPORATION LTD

Experience the Paradigm Shift in Cyber Security

Athena Cyber Security Series

- Sasa Software** Smart Made Simple. **prevent**
- ICONZ-Webvisions** **preventing data leakage**
Your Data. Our Business
- gha** **good hackers alliance**
Be checked by the good hackers or be hacked by the bad ones
- SANITIZING**
Protecting without Compromise
Ultra-Deep Content De-construction, Neutralisation and Re-construction (CDNR)
- CONTAINMENT**
Contain the Threats
Secure Web Browsing, Email and Removable Media
- RESPONSE**
Resilience without Disruption
Award-Winning Incident Response Platform

Athena Dynamics foster strong partnerships with ICONZ-Webvisions, Sasa Software, Resilient Systems and Bufferzone Security to showcased a range of solutions that have already helped numerous large enterprises protect their critical enterprise networks and infra-structures via a unique and unprecedented approach. Together with our dynamic team of practitioners to ensure the highest quality of our deliverables.

Mr. Ken Soh, CEO of Athena Dynamics commented on the overall show response, “RSA continues to be a good platform for Athena Dynamics to introduce strongly differentiated cyber protection products and services to the markets. Having awarded classified and highly sensitive projects in both public and private sectors in just two years of market entry speaks volume of what the markets actually need. Athena

will continue to be innovative in its product sourcing effort, and to bring forth more unique propositions and value-adds. See you in Govware 2016!”

On behalf of Athena Dynamics, we would like to express our sincere gratitude to all our valued partners, customers and other security professionals in supporting us in this event. We hope you have benefited as much we do, looking forward in building more contacts in the upcoming GovernmentWare 2016 on 10th to 12th October 2016, held at the Suntec Singapore International Convention & Exhibition Centre. See you there!

We Look Forward to Seeing You at



Suntec Convention Centre, Singapore
10th to 12th October 2016



Website: www.athenadynamics.com

Tel: +65 6210 2354

Email: contact@athenadynamics.com

Journey Against the Digital Dark Side

Featured on Marine Trader, 2016 Issue 5

"Are My Ships and Offices Safe from Cyber Attacks?"



An Account from Ken Soh, CIO of BH Global Corporation Ltd

If you do not even know what is APT, or VAPT, you are probably already under attack.

Ken has been through an unexpected journey of anguish and surprises when he experienced first-hand the pervasiveness and sophistication of cyber-attacks a couple of years back. Fortunately, with the support and open-mindedness of the management, he managed not just to understand the intricacies of cyber security, he has also managed to turn an unpleasant experience into a new business under the group. He has emerged stronger from the experience and decided to share extensively and educate the community at large on cyber risks with first-person experiences in many related industry conferences and seminars in which he was invited to speak.

This paper serves to summarize with a first-person account the author's own experience the "power of the dark side" in a bid to educate the industry at large the weightage and magnitude of cyber threats today, not just in the context of Enterprise Information Technology (IT, e.g. offices), but also Critical Infra-structures, or Operation Technology (OT, e.g. ships, vessels, ports and rigs).



Doomsday's Prophets

For the longest time, I had been truly put off by many of the cyber security conferences that vendors are trying their hearts out to pitch the seriousness of cyber-attacks and also the vulnerability of our IT systems simply to induce sales. All the doomsday's prophets would deliver similar points, none other than citing other people's well-known examples. How Sony was hacked, how Target was compromised, how such attacks became high profile board room's issues, how the CISO (Chief Information Security Officer) is the first to experience Career Is Suddenly Over, how the CEO (Chief Executive Officer) would be the next to have his Career Ended Overnight when their enterprise systems were compromised.

I was getting a little weary and wary of such industry pitches because, after all the attempts to scare (and of course to sell), there is usually no concrete or radically differentiated fundamentals to share that

could help to effectively mitigate cyber risks. Almost every provider is doing the same fundamental, i.e. to "detect and to remove". The issue today is, we can't even detect many of the advanced threats, or industry would term it "Advanced Persistent Threats" (APT). So is detection still the way to go? Nobody seems to question.

Companies invested a fortune, yet still continue to be compromised. Why?

Similar to many, BH Global invested a bundle in security products, and yet from time to time, compromised incidents would happen. As cyber threats hot up and becoming more sophisticated, cases are becoming more prevalent too. There is an urgent and imminent need to source for a truly effective strategy and practices. However, this is not possible without first trying to understand the fundamentals.

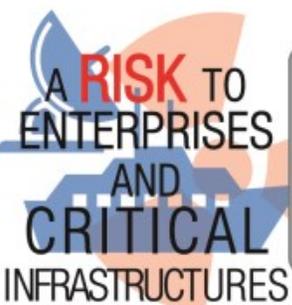
As mentioned earlier, detection-centric practices are no longer working. I started to research, and I started to recall back my past decades of IT operation management, what has been changed, what has evolved.

People + Process + Technology

This is a classic framework. Yes, security cannot be accomplished solely with tech-

nologies. After all, it is still people that operates the technologies. Also, enterprises would naturally need to have strong and effective processes/governance to get the daily operations in good order.

What prompted me deeply is, there seems to be a shift of weightage over the last couple of years. While in the past, people (security awareness) played a relatively important part of the enterprise security framework, technology is becoming on par with it lately. Malware that crashes hard-disks and slows down desktop operations are highly stealthful today. Once infiltrated, it stays silent in the user's PC, typically with remote "command and control" centre from anywhere in the world to take over the infected machine quietly in the background. To make matters worse, millions of new malware emerges daily, rendered even the most advanced detection technology ineffective. In the past, you probably need to download something to have the bad guys in. Today, the simple act of just visiting a site may get one infected quietly in the background. So education may not be as straightforward today. We need good technologies to counter such advanced threats.



We are in urgent need for a radically differentiated paradigm shift!

Having understand the fundamental that detection-centric method is no longer effective, I started to research on technologies that could possibly augment it. What that was discovered then proved to be well worth the effort.

Specifically, the research started with experimentation of non-detection-centric technologies that includes methods such as white-listing (instead of detection which is generally termed as black-listing), and also end point containments. This is not the platform for big technical discussion. Not to touch on geeky pursuits, I would simply put it that some collection of non-detection-centric tool were picked, and some of which are surprising and unknowingly powerful, achieving zero infection in its deployed sites for the last 7 plus years!

Hello world, what have we been doing?

Seeing new lights in cyber protection

I would not say that at the time

of this writing, we have started with the new approach described. The research is still ongoing but yes, definitely a new frontier of protection strategy has been found. It may not be a panacea for cyber threats but at least it completes the loop and it fills the gap where traditional detection-centric cyber technologies cannot fulfil.

The beauty of a non-detection-centric approach is that the technology not just takes care of known viruses and zero-day (new, just born) viruses, it even takes care of the threats of almost all of the future “unborn” viruses. What surprises me is that such technologies were already around for some time, waiting to be discovered for wide-scale adoption. No one seems to care. Is there an industry conspiracy going on somewhere just because the current, traditional cyber protection tools is a multi-billion dollar industry?

Transforming the discovery into a business

The discovery was not only useful to protect the group companies within, it does not take long for business savvy people in the company to realize that it would be a viable and meaningful business to market and apply what that is learnt and discovered to protect the industry at large.

For that, a new cyber arm subsidiary Athena Dynamics (ADPL) was born. The principle proved truly useful and within just two years of operation, ADPL was awarded classified projects in the public sector, security projects in aid of protection of energy plants and more. Such quick adoption by the industry speaks volume of the fact that the protection fundamental of the technology is not only sound, but practical.



A useful business alliance that brought on more surprises

As the cyber business develops, we started to realize that sound product provision alone is insufficient. As cyber incidents become more frequent, there are unsolicited calls from the industry for help from time to time when their enterprises are compromised and needing help in either forensic, vulnerability assessment and penetration testing (VAPT), or post-compromise assessment. We decide that a service arm is necessary and for that, we were fortunate to forge an alliance with a highly accredited ethical hacker group from a country that faces millions of digital attacks daily from its hostile neighbour. The group won world-class hacking competitions such as Defcon and Codeblue year after year since 2010, with its latest credential of opening a water dam door just after 7 hours of consented hacking from internet.

The partnership was named

Good Hackers Alliance (GHA), and with that, we have decided to first do a VAPT on our own corporate website and systems. The VAPT brought on surprises such as the discovery of implanted call-backs from some enterprise PCs, and also unauthorized accounts being created in-house by hackers infiltrated from Russia and Poland. Fortu-



nately, these hacking activities were discovered early and they were still “work in progress”, and no major leakage of data actually happened. The planted call-backs and ‘evil traces’ were removed, and the gaps that were exploited were filled and fixed in no time.

Hacking ships, planes, cars, energy plants and more

Our journey of cyber awareness

reaches new height when we realized GHA’s expertise in consented hacking is beyond just Enterprise IT Systems, for the simple reasons that hackers today have already successfully infiltrated into critical infrastructures. Offshore rigs were hacked and dangerously tilted, vessels systems were found infested fully with viruses.

These hacks could happen directly or indirectly. The server of a shipping company was compromised and the pirates knew exactly which ship, when, where and even down to the fine detail of which crate actually contains the

most valuable goods.

For ships, cyber awareness is rising but more need to be done urgently

It was truly disappointing to observe the negative public outcry when Singapore government decided to segregate sensitive government network from the internet.

From the observation it is apparent that public at large still do not see or understand the magnitude and seriousness of cyber threats today, especially what that were in the dark web, state-funded cyber threats and what an attack to our government network could impact everybody at national level. More education seems imminently needed.

Conversely, it has been comforting to observe that the awareness is rising quickly especially with the support of the authority. Specifically, Maritime Port Authority (MPA) has recently ran a full day Maritime Cyber Security Seminar with overwhelming turn-out. It is healthy to observe that business owners are starting to question what could be done going forward. We are truly humbled to be invited to speak and share in this inaugural event on maritime cyber security, and a very useful panellist exchange in the seminar.

What could potentially be hacked on-board ships and vessels?

Unlike IT systems onshore in shipping offices, they are close to the governing IT department and protection practices and policies

could be enforced effectively. The IT systems on-board ships and vessels are remote. Governance may not be enforced easily. Unless effective cyber tools are in place, its exposure to cyber risk is high.

Separately, more and more OT systems on board ships and vessels today are transiting to PC based and TCP/IP based devices. Devices that are well interconnected, or devices that accept external devices (such as external USB, storage devices) are vulnerable to cyber risks. Just to name same, the following

could be systems that require various extend of VAPT and certifications:

1. Bridge Systems: GPS, ECDIS, AIS, GMDSS, VDR, SSAS, etc
2. Communication Systems: VSAT, FBB, VOIP, WiFi, etc
3. Maintenance Systems: AMOS, DANAOS, etc



It is not just about classification rules, but actionable rules

ADPL is working closely with classification bodies in the fulfilment of new framework in cyber protection. While some high level classification rules have been published in the past, new chapters with actionable items would be necessary. This could be jumped started with series of focused workshop were feedback from the ship owners could be gathered. This, coupled with cyber specialists and practitioners, a reference implementation model could be jointly developed with trial VAPT on shipping devices. Alongside that, specific cyber tools in the IT arena could be identified, enhanced, ruggedized and adopted for marine and offshore purposes.

The assurance framework

Prior to the full fledge availability of the global classification rules, ADPL has derived a simple assurance framework which enterprises and critical infra-structure owners could reference:

VAPT Risk Landscape Assessment

Every IT and OT setup is unique and different. It is important to perform a health-check on the IT and OT setup to sieve out the vulnerability, prior to looking at the following steps.

Non-conventional Protection Instruments

Once the vulnerability is known, specific cyber tools could be considered. As discussed earlier, it is important to consider tools that do beyond just “Detection and Removal”.

Incident Response “Emergency Button”

Corporates today typically have IT operation competency but not incident response (IR). It is important to incorporate IR into the corporate BCM and ERM framework.

OT and IT Security Awareness

Specialized SCADA security awareness training is key.

Cyber Insurance

While cyber insurance is relatively immature today, it is still an important post-event protection instrument that organization could consider and deploy.

How to make the buyer-supplier process win-win

Featuring in IMPA Singapore on 18th May



Tell us about your Total Inventory Management Programme. How does this benefit your customers?

Beng Hui run a Total Inventory Management Programme, which comprises of the provision of interim inventory storage coupled with progressive just-in-time delivery and billing. Be it drums of cables or light fittings, customers can place their orders without having to worry about space for the ordered inventory and hefty financials and be assured that the products are delivered according to schedule.

This is a practical alternative to taking up space in your warehouse, which can be better utilised to store higher value equipment. This also equates to lower inventory holding cost in terms of equipment and labour utilisation.

Companies which partake in our Inventory Management Programme get more competitively priced inventory, price consistency throughout their projects and the assurance of sufficient stocks at all times. We support on-going projects with just-in-time deliveries according to projects schedules accompanied with Project Inventory reports. This in turn will enhance the support our customers can provide to their customers.

In the marine and offshore industry, technical support is vital. What are some key factors that contributed to the success of your team in this area?

We specialise and focus a lot on quality component integration. By understanding requirements comprising of detailed analysis, conceptual design and regulatory impacts, we can then propose adequate components to enhance a product's efficiency and effectiveness - products designed to be superior in meeting various stringent environmental and safety standards. By leveraging on our technical know-how and wide portfolio of premium technically certified marine grade electrical products, selecting the right components was easier and our customers can enjoy the benefits of total solutions.

Working with our brand partners, we are able to provide not only custom-built products but continuous support in the supply of components, after-sales service and product training. This is also made possible with sales support from our dedicated team that follow up closely from project initiation stage to delivery. Our sales are also equipped with global MRO sourcing capabilities and are familiar with international product standards and specifications.

We've heard of your LED initiatives for vessel owners. What is your outlook on green lightings for vessels and what plans do you have for development over the next two years for your SOP brand of marine and offshore LED lightings?

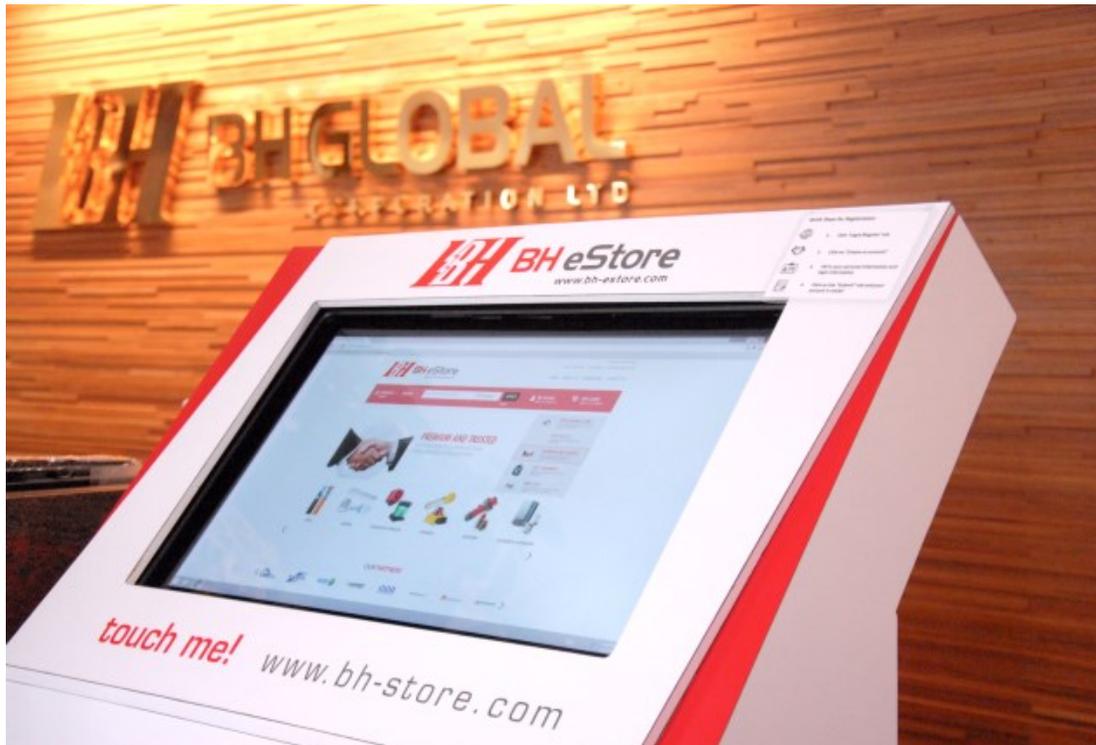
There is a growing trend of owners opting for green lightings on ships. They see the importance and benefit of having almost zero maintenance of lights during their lifetime. What makes us stand out is that we are working closely in a joint venture with a specialist in LED Lighting Industry that has over 16 years of experience in niche LED Integrating Solutions. We are a well-known partner for both LED engines and ODM luminaire projects to many world renowned lighting brands with more than 500 projects till date.

We are open to working in a tripartite relationship with ship chandlers and owners for LED retrofits and new-build projects. In this way, all three parties will benefit. Ship owners will benefit from high quality marine and offshore LED lighting - allowing them to maximise their investment in operations and reduce maintenance needed and ship chandlers will be able to provide support in terms of spares or new lightings from their various offices worldwide. We will be able to provide design support component integration, lux and ROI calculation, product demonstration and even mock ups.

The rise of LED technology will transform the maritime lighting industry. The huge potential for future LED improvements will arise from new levels of quality and efficacy of the lights. We are focused and committed in the development of a wider range of marine and offshore lightings that provides green and innovative energy-efficient technologies and meeting demands of the harsh marine environment at the same time.

e-Commerce in the maritime industry is gaining traction. How is Beng Hui contributing to the transition of her customers' procurement in support of vessel operations?

We are currently exploring initiatives on adaptors that will allow secured and seamless STP (Straight-Through-Process) between 2 ERPs - contain real-time stocks availability information, direct issuance of PO, DO and invoices with improved efficiency.



We have also an online platform BH eStore (www.bh-estore.com) an electrical guide book for marine and offshore industries, which serves as an excellent guide for the technical stores for the electrical superintendents. As part of our e-commerce strategy, BHM e-store is poised to better serve our channel partners and customers, providing them with a one-stop customer engagement portal in which product information is categorically presented with easy-to-use search and compare functions. This improves efficiency, productivity and transparency. We are also exploring direct issuance of PO and payment on this platform. We are very positive of the customers we can reach and assist through our online platform and the huge potential it will bring.

Dinner & Dance 2016—Shanghai Fusion

BH Global held its annual Dinner and Dance at The Chevrans on 28th May 2016 with a Shanghai Fusion theme to spice up the evening programmes.





Chairman, Mr. Alvin Lim giving his opening speech.



Long Service Award

5 Years



(Left to right): Liew Hsiao Voo, Roger Ung, Xiao Xiu Yun Kerry, Thein Hlaing Lukie.

10 Years



(Left to right): Hing Kah Wen Ken, Kong Kim Chwee, Lam Kok Wing



(Left to right): Loo Chee Kian, Tan Soo Hong, Tan Wee Kiah Simon and Wong Yau Yuen Randy who was absent at the time of photo.

20 Years



Award recipient: Boo Hong Hwee



Lucky Draw and Special Draw



(Left to right): Karen Ng, Bryan Hoe and Lim Eng Eng.



Special draw recipient: Jeffrey Tay

Best Dressed Winners



Bryan Hoe and Phoebe Chai



Event Committee Chairman, Jasmin Lim, remarked “It was an honour to be able to partake in the organising of this year’s DND together with my great team. Though the preparation was rushed and that there were very few meetups with the event company, emcee and the event committee from Beng Hui prior to the event, I am glad we managed to pull through with minor hiccups. The highlight of the event for me was the starting of the night when our management marched in ‘Tao Kay’ style to loud Chinese music and towards the end of the night when we formed a long human train and circled around the ballroom. I look forward to showcasing more of the event committee’s camaraderie through such company-wide events. A big thank you to my team! To even more successful years of DNDs ahead!”.

“It was great to be able to work with the team to organise the annual company event. There may be some hiccups during the planning and execution, but the trust and faith from everyone made the event run smoothly and everyone enjoyed the show. Kudos to all who helped and contributed to the success of this event. We shall see you again next year!” - Jenny Yeo, Event Committee Leader.



Happy Hour 2 — The Running Man Relay



Second quarter's Happy Hour, put together by our event committee members, sales and marketing colleagues.

Station 1: Queen Dodgeball

All teams gathered in a cordoned area, games ICs stood at the edge and threw balls at players once



music had stopped. Team with the highest hit faces penalty to pause.

Station 2: The Flying Coin

Teams are to stand behind a taped line and they are to throw coin in a water-filled bowl that is 3 metres away. One member to throw at a time and all members had to have their coin in the bowl before proceeding to next station

Station 3: Water Passage

First player will carry the bowl of water from the previous station while another player will push him/her using a trolley. Every player take turns to fill the water to the brim and only one cup is allowed at every turn.



Station 4: The Speed Quiz

All teams will be given 5 similar mathematical questions, they are to use mental calculation to come out with the accurate answer.





Station 5: Food Bingo

Mini Bingo board of 3 x 3 and team had to randomly place 9 types of food/drinks into the 9 squares. Game ICs will then announce five unique numbers to each team. The number represent the type of food that was place in the squares that players needs to finished up before proceeding to next station.



Station 6: Smiling Photo-zone

Teams are to stand within a rectangle box on the ground and follow the 4 different poses according to game ICs instructions. A player will need have good photography skills to capture it. Once game ICs checked the accuracy of photos, they may search for Jenny who will provide them a popper that represent the end of relay.

