IPCSA
International Port Community Systems Association

15 July 2015

Cybersecurity

In the Maritime and Logistics Supply Chain

Workshop summary, conclusions and recommendations

"Cybersecurity is:

- A 'top ten' risk, according to a survey of 28 industry sectors and 1,500 companies (Aon Global Risk Management Survey 2015).
- Vital for business continuity and reliability; vital for protection of the public; and vital for businesses seeking to be 'trusted third parties', as any breach can have a massive impact on a company's reputation."

Thanks go to Bureau Veritas for hosting the workshop in their London Office

CONTENTS

About IPCSA

IPCSA and its members play a vital role in global trade facilitation; the electronic communications platforms provided by Port Community Systems ensure smooth transport and logistics operations at hundreds of sea ports, airports and inland ports.

IPCSA was originally formed as EPCSA in June 2011 by SOGET, Le Havre, France; MCP, Felixstowe, UK; Portic, Barcelona, Spain; Portbase, Rotterdam and Amsterdam, Netherlands, dbh, Bremen, Germany and DAKOSY, Germany. The reason for forming EPCSA was that Port Community System Operators (PCSOs) did not had a common position at the European Union. Thus the leading PCSOs agreed that they needed work together in areas of common interest.

On 1st September 2014 the association changed from a European to an International association to better reflect our growing membership which now includes organisations from all parts of the world.

For more information on IPCSA go to www.ipcsa.international

IPCSA Cybersecurity Workshop, London, July 2015

A number of organisations – including the European Commission, International Maritime Organization, World Customs Organization, tax officials and governments – are focusing strongly on the issues and risks around cybersecurity. But until now there has been little focus on cybersecurity in the context of data sharing across the ***whole supply chain***.

Members of the International Port Community Systems Association (IPCSA) invited key supply chain partners and stakeholders to join them for a day-long workshop to consider the challenges, risks and possible solutions in the field of cybersecurity in the Maritime and Logistics Supply Chain.

The workshop had two perspectives: firstly, what should Port Community Systems (PCSs) do individually and jointly, and secondly, what should the wider supply chain do.

Cybersecurity is:

- A 'top ten' risk, according to a survey of 28 industry sectors and 1,500 companies (Aon Global Risk Management Survey 2015).
- Vital for business continuity and reliability; vital for protection of the public; and vital for businesses seeking to be 'trusted third parties', as any breach can have a massive impact on a company's reputation.

Millions of lives and livelihoods depend on many highly complex, constantly adapting supply chains. One weak link could threaten the entire supply chain.

Considering this from a PCS perspective:

- The electronic communication platforms that Port Community Systems provide ensure the swift, efficient exchange of information and are vital for trade facilitation. However, in the wide variety of stakeholders sharing data within a PCS, each presents a unique risk.

- A PCS must balance its 'networking' role, which is critical for trade facilitation, with the need to keep data secure, because any cybersecurity breach could affect the whole supply chain. How can PCSs ensure the data is available, while also ensuring the integrity and confidentiality of that information?

- Thousands of companies within the logistics chain use PCSs as an added value to their business process. The effect of a PCS being influenced by a cyberaction could delay the port process. The delivery time of the goods could be influenced negatively by this.

The workshop was facilitated and led by Will Sambrook, from the Ideas Centre, and took the form of breakout discussions followed by the sharing of ideas and conclusions. It also included a presentation by Kevin Calder, of Mills & Reeve, on the legal aspects of cybersecurity.

The challenges and risks

If one weak part within the supply chain is compromised, the entire chain is threatened. The discussions highlighted:

- The logistics chain includes large corporate groups and also small agencies employing only one or two people. They operate at different levels with different priorities and resources.
- The supply chain business is a very dynamic one with contracts, contacts and employees constantly changing, making control difficult.
- Securing data transmission must be a priority – but there are still instances where information and data is exchanged by fax or in open emails, so that it can be easily read on the way into the system.
- Even if data is secure, knowledge remains a real risk. A disgruntled employee could be a weak link. But so could a former member of staff who once had knowledge. So could a poorly trained member of staff with access to vulnerable parts of the system.
- The relevant national legislation varies from one country to another.

- In some regions, Cloud solutions are more secure than conventional data centres – but in some cases, the opposite is true.
- It is also quite conceivable that a rogue organisation could 'plant' a temporary or permanent member of staff into a company in order to infiltrate the system.
- Additional risks highlighted by Kevin Calder of Mills & Reeve included: identity theft – often made easy by the 'post-it note on the screen'; loss of unencrypted data – sometimes on a memory stick or laptop mislaid away from the office; criminals setting up domain names similar to your organisation's in order to harvest data; liability for third-party loss; and business interruption.

From a PCS perspective:

- Some of the data held by PCSs is public data, but some is very private and sensitive in terms of business and/or security risk. As well as the issue of who is the individual owner of the data, another potential risk is the combination of data sources – i.e. the sharing of data.
- A key question to ask is: who has access to the data and who shares the data? In a PCS environment, data is shared by many different kinds of stakeholders and customers, whose individual security/access policies are beyond the reach of the PCS.
- Users of a PCS may not necessarily understand, though it will have been agreed with their organisation, who else will have access to the data that they submit or share in the system.
- A major risk could be manipulation of the data in the database, potentially causing chaos in the port and logistics environment, which is extremely dependent on accurate, timely, accessible information.
- Some PCSs are vulnerable to other organisations' weaknesses, including those using infrastructure provided and controlled by government or other public bodies, as well as the data that is being supplied. Is the system strong enough and secure enough to cope with that weakness?

What steps are needed in the Maritime and Logistics Supply Chain?

Who should be involved in the fight against cybersecurity risk? The answer is: All of those involved in the logistics chain, i.e. software developers, including PCS providers; network providers, including network infrastructure; government; importers and exporters; trucking companies; anyone involved in moving, buying, selling, trading; international organisations such as the IMO, EC and IPCSA.

Key elements to come out of the workshop discussions:

- AUTHORISATION: The right people should have the right access to the right data: people are often the weakest link and there should be strong policies on who is authorised and at what level for data access and exchange. This should be decided and controlled on a 'need to know' basis. Access must be restricted – not everyone needs to know or access everything.
- IDENTIFICATION: Strong ID processes are vital and can have the biggest impact in terms of limiting the chances of people breaching security. All stakeholders should have strong systems for monitoring current staff, regularly changing passwords, deleting ex-employees from the system, etc. User names and passwords must be tightly controlled and not accessible, and multilayered ID processes such as biometrics and secondary ID could be considered.
- EDUCATION and AWARENESS: Employees, customers and stakeholders need to be made aware of data security issues. Focus on behaviour, education, enforcement and control.
- PROCESSES: A strong focus on physical access, technical protocols, firewalls, general rules/standards, improvements, encryption and virus protection. The use of secure data exchange must ensure that PCSs can guarantee as high a security level as possible.
- VIGILIANCE and PREPAREDNESS: There are individuals and organisations focusing entirely on trying to break into security systems or data – for financial gain or fraud purposes, as part of a terrorist threat, or simply to outwit the system. A PCS's resources, and those of the wider logistics chain, should at least limit their chance of success.

- CONTRACTS: Contracts with IT system and software suppliers can specify security levels and require them to comply with your own policies. Procurement strategies should be examined – do you have one supplier or a multi-sourcing approach? What due diligence is carried out with regard to suppliers or third parties you are dealing with?
- INTENTIONAL vs UNINTENTIONAL: Not all cyber attacks are external, intentional attacks. More attention needs to be paid to internal and/or unintentional risk, such as untrained staff making errors.
- MONITORING and TRACEABILITY: Stakeholders in the supply chain must constantly monitor their systems to eliminate any weaknesses or vulnerabilities. Processes should be in place to identify any breaches and pick up on any unusual ways of working or strange behaviour, such as large amounts of data being removed.
- TESTING, REVIEW and AUDIT: Systems should be regularly tested, preferably by third party organisations, for their robustness against hackers, with advice on how to follow up the findings of such tests. Interfaces between systems should also be tested. No system should stand still. It should continually evolve and develop to ensure that it has the latest security and techniques.
- ENFORCEMENT: Cybersecurity policies or guidelines within organisations are critically important in today's world. However, such policies fail if they are not monitored or enforced. There are many standards available that can help organisations develop such policies.
- SHARING IDEAS: An example given was the Belgian Cybersecurity Guide, available online: http://iccbelgium.be/becybersecure/
- BALANCE: Between security and usability.
- MITIGATION AND BUSINESS CONTINUITY: PCSs must be seen as Trusted Third Parties (TTP). Reliability of service, security backup and contingency plans are critical

From a PCS perspective, all of the above elements should be considered. However, four elements seemed to be the most important, namely:

- AUTHORISATION: The right people should have the right access to the right data: people are often the weakest link and there should be strong policies on who is authorised to use the PCS and at what level. This should be decided and controlled on a 'need to know' basis. Access must be restricted – not everyone needs to know or access everything.
- VIGILIANCE and PREPAREDNESS: There are individuals and organisations focusing entirely on trying to break into security systems or data – for financial gain or fraud purposes, as part of a terrorist threat, or simply to outwit the system. A PCS's resources, and those of the wider logistics chain, must match this or at least limit their chance of success.
- MONITORING and TRACEABILITY: PCSs must constantly monitor their systems to eliminate any weaknesses or vulnerabilities. Processes should be in place to identify any breaches and pick up on any unusual ways of working or strange behaviour, such as large amounts of data being removed.
- MITIGATION AND BUSINESS CONTINUITY: PCSs must be seen as Trusted Third Parties (TTP). Reliability of service, security backup and contingency plans are critical

General business risks

Though the workshop highlighted cybersecurity, other, more general, business risks were identified, including:

- KNOWLEDGE: If an employee leaves a company, they can take knowledge with them. How can this knowledge be secured and the risk eliminated of that employee accessing or exploiting the system later and creating significant problems in terms of commercial or safety threats?
- CONTINUOUS IMPROVEMENT and INVESTMENT: In people, systems and technology. Undoubtedly this will become increasingly important.

Standards

Whilst the key elements highlighted are critical parts of cybersecurity and defence, an underlying feature related to standards. There are numerous standards already available and it was considered that, rather than 'reinvent the wheel', there should be firmer commitment by the industry stakeholders to existing standards such as:

- SANS20 – https://www.sans.org/critical-security-controls/
- ISO27001/2 - http://www.27000.org/iso-27001.htm
- NIST800-53 - http://csrc.nist.gov/publications/PubsSPs.html#800-53
- ISF - https://www.securityforum.org/
- Belgium Cybersecurity Guide - http://iccbelgium.be/becybersecure/

These standards are not exclusive and there are others that cover different trades within the Maritime and Logistics Supply Chain; however, they provide an example of some of those that are available and that are currently used.

General conclusions

Delegates concluded that, given the nature of cybersecurity and the broader logistics chain, total cybersecurity and the avoidance of all risk is not achievable. Rather, the focus should be on constant improvements and on ***limiting*** the impact if a breach does occur within an individual organisation or within a chain of organisations.

- How can we be more secure than we were before? Focus on business processes and on people.
- Whatever security level should or could be achieved, hackers or others intent on compromising or accessing data will always find a new way. So the process is continuous.
- Organisations must recognise that it is not a case of 'if' we are going to get security breaches, but 'when'. Stakeholders must not only minimise the chances of a security breach – but be ready to limit the damage at every step

as well. They should also consider how any breach may affect their clients and suppliers.

Conclusions specific to Port Community Systems

A Port Community System needs to be secure, because cybersecurity weaknesses affect the whole supply chain. Delegates concluded that, given the nature of a PCS and the broader logistics chain, the focus should be on constant improvements and on ***limiting*** the impact if a breach does occur.

- The position of a Port Community System as a Trusted Third Party is vital for business confidence. There must be a strong focus on reliability, continuity, contingency.
- Mitigation and Business Continuity: PCSs must be seen as Trusted Third Parties (TTP). Reliability of service, security backup and contingency plans are critical
- PCSs need to focus on being at the forefront of cybersecurity and need to continually think about how they can be more secure than they have been before. There will always be the chance that hackers or others intent on compromising or accessing data will find new ways. So the process is continuous.
- PCSs need to focus on processes, particularly those of user access and control and monitoring of usage to identify and report abnormal use or unusual data flows.
- PCSs have reported that cybersecurity risks are increasing and all ports and Port Community Systems must recognise that, as with all organisations, it is not a case of 'if' we are going to get security breaches, but 'when'. PCSs must not only minimise the chances of a security breach – but be ready to limit the damage at every step as well, for all users in the within the affect data flows.

Recommendations

These recommendations outline local, national and international that may have the potential to mitigate cybersecurity threats and risk. Maritime and logistics actors and PCS operators should consider, with the support of their trade associations and international and regional bodies working together to address the current threats to the supply chain.

- Each PCS should, at a local/national level, bring together key stakeholders in the supply chain and create an Information Sharing and Analysis Centre (ISAC) to discuss cybersecurity threats, risks and experiences. Strict guidelines and protocols should be in place to ensure such an environment is confidential between participants, who ideally would be information security experts.
- At a regional level, appropriate organisations – for example, the EC for the European region – should support the industry by the creation of higher level Cybersecurity Forums, bringing together stakeholders from regional and international organisations. It would be recommended to use the UN Regional Commission regions, i.e. Europe & North America, West Asia, Asia & Pacific, Latin America & Caribbean, and Africa as a base for this and this would also help create an international perspective.
- IPCSA should consider setting up a specific PCS Information Security Group within its membership.
- All organisations should, at a minimum, organise penetration tests – usually carried out by outside security consultants – to ensure their systems are secure. This should be done at least once a year.

Next steps

IPCSA will circulate this paper amongst its members and other stakeholders in the Maritime and Logistics Supply Chain for their considerations. In addition, IPCSA will also work with international and regional organisations to consider how their support could help reduce cybersecurity risks for the trade.

Workshop Participants

Organisation	Name	Organisation	Name
APCS	John Kerkhof	IMO	Alper Keceli
Bureau Veritas	David Lappage	IMO	Helio Vincente
Bureau Veritas	Olivier Moreau	IPCSA	Richard Morton
CLECAT	Nicollete van der Jagt	MCP	Alan Long
DAKOSY	Evelyn Eggers	MCP	Russels Knowles
Dbh	Uwe Liebschner	Mills & Reeve	Kevin Calder
ESPO	Laurens Schautett	Portbase	Linda van Moorst
FONASBA	John Foord	Portbase	Hans Rook
Freelance Journalist	Felicity Landon	PROTECT	Jerome Besancenot
Freeport of Riga	Daniels Atkacuns	Port de Tarragona	Anna Navarro
Ideas Centre	Will Sambrook	Port de Tarragona	David Gonzalez

Further information

For further information on these workshop outcomes and to work with IPCSA on cybersecurity issues, please contact:

Richard Morton, Secretary General, IPCSA

Tel: +44 7796334960

Email: Richard.morton@ipcsa.international

Web: www.ipcsa.international