Edvard Tijan, univ. mag. ing.
Serđo Kos, Ph. D.
Dario Ogrizović, univ. bacc. ing.
University of Rijeka
Faculty of Maritime Studies
Studentska 2
51000 Rijeka
Croatia

Review article
UDC: 004.056.5
656.615
Received: 24th March 2009
Prihvaćeno: 6th May 2009

DISASTER RECOVERY AND BUSINESS CONTINUITY IN PORT COMMUNITY SYSTEMS

This paper presents the structural analysis of a port community system (PCS) and its main stakeholders, both internal and external, who are involved in the execution of port business activities. Typical information and telecommunications infrastructure of a PCS is outlined, along with the main challenges in its introduction. Furthermore, a significant emphasis is put on information security within the PCS, presenting a firm base for the introduction of both the concept and the model of integral security. Finally, often very overlooked business functions – disaster recovery and top-level function of PCS business continuity, are defined in detail, along with the requirements for the creation of a robust business continuity plan, whose goal is to ensure the functioning of a PCS in case of disastrous event or a foreseen disruption in line with the PC ICT system risk analysis.

Key words: *port community systems, information security, business continuity, disaster recovery*

1. INTRODUCTION TO PORT COMMUNITY SYSTEMS

Port community systems (PCS) are holistic, geographically bound information hubs in global supply chains that primarily serve the interests of a heterogeneous collective of port related companies [4]. Necessarily, they are complex in their nature due to diverse base of involved stakeholders that operate in the same environment – the port community [9].

Usually, the economic activity that is being executed is spanned geographically over a certain enclosed area – sometimes with dislocated adjacent sites serving specific purposes - under the supervision of the centralized governing

entity. Separate business functions are usually entrusted to concession holders, who are separate registered entities (limited liability companies or corporations) [15]. Furthermore, the activity in nature is quite diverse with specific demands for the ICT support, so the expected forms are general cargo handling, liquid cargo handling, container cargo handling, cargo forwarding, towing/tugging, quality and quantity control, ship supplying, ecology and general services.

One can imagine that the overall business activity within port community systems in fact involves a heterogeneous portfolio of used ICT technologies, goods and services supply technologies, used processes, involved stakeholders and applied specific branch standards.

Figure 1: Port community system

Source: created by the authors

The goal of the port community systems is to provide a common framework to all players who use maritime transport in a local supply chain scene that will enable them to supply the requested goods exactly when purchasing

parties need them, to supply exactly those goods requested, and to do so while minimizing the cost. Of course, only a fully optimized system can achieve the above stated goals.

From the operational standpoint, the port community systems are supposed to manage and promote general, private and public objectives that are often divergent, if not opposite. Generally, the parties involved in the functioning of port community systems can be divided into three groups:

1. Customers (be it in-house or outside)
2. Public bodies
3. Non-customers and others

A successful implementation of a port community system is able to incorporate business processes of all involved parties, but also to further promote their autonomy. These two seemingly oposing principles need to be reflected in the creation of an operational framework of the PCS and in forms for business to business (B2B) interfaces.

2. CHALLENGES IN SETTING UP PORT COMMUNITY SYSTEMS

The most common framework that sets up port community IT systems is the multi-tier architecture in which the presentation, application processing and data management are logically separate processes. In case of port community systems, it is usually a 3-tier system [5] with the following elements.

Figure 2: Port community ICT system components

Source: created by the authors

Hardware and system layer is comprised of the users' workstations and servers with installed operating systems that are connected to internal office networks (LAN – local area networks) and further, towards extranet of the open Internet (WAN – wide area networks). Additionally, supporting and peripheral equipment like printers, scanners, fax machines, mass-copy stations, subnotebooks and palmtop computing devices can be considered a part of the

hardware infrastructure too, mainly due to their complexity, variety and prevalent usage nowadays.

Applications and business services servers are the core parts of this layer, used to support predefined mission-critical services within port communities. However, the often overlooked element of this system is the organization of help desk and user services, change management and creation of common framework to manage the system as a whole. Both are best achieved by using one of the industry-standard certification systems.

A help desk is an information and "hands on" assistance ICT function that resolves issues that the users' encounter [2] while using ICT resources in their daily work within the port community system. The support is provided via telephone, email personally, or by using remote logon. Considering that all the involved parties within port community systems have their own help desk systems, it is a challenge to organize a functional integral port community ICT system helpdesk. A help desk can be a central service of a wider Service desk system. One of the most widespread organizational blueprints for a service desk and help desk rollout is ITIL – Information Technology Infrastructure Library that implements IT service management best practices.

Help desk systems that should serve a large number of customers, like those present in a typical PCS scenario, would have to be organized in such a way that they will be able to manage different types of incidents, with the first level that usually answers the most common questions that are readily solvable by using the knowledge base of the resident PCS FAQ (Frequently Asked Questions) repository. If the issue is more complex, it gets escalated upwards to a second level. Considering the complexity of PCS ICT systems, it is to be anticipated that even the third level of support, dealing with difficult and even critical issues and bug fixes should be present, or adequate support contracts should be put in place.

Considering the three-tier architecture, the organization of a help desk should reflect this specific request, so within the PCS ICT systems it is necessary to establish several teams that may dedicate themselves to specific aspects of the ICT infrastructure. Common prudency would call for three separate teams to manage the incoming PCS help desk calls: desk side time (or desktop deployment team), network and infrastructure team and core applications team.

The critical part of every PCS ICT system is the creation of a consistent repository of Service Level Agreements, main elements of every ITIL model [6]. Presuming that all stakeholders in the PCS systems are simultaneously users and internal customers of the PCS ICT system, a Service Level Agreement, in form of negotiated agreement between customers and service providers, enables clear-cut description of the providers' obligations towards its customers, providing transparency and independence from adopted models of the in-house service desk management.

The software infrastructure superimposed over this layer can be divided into **general software** that is usually comprised of an operating system and kernel software, antiviral/anti spam protection, frontend Internet portal and applications server, **database software** (document management system) and **business application software** that includes information routing services and a certificate server used for the unique user authentication.

The applications being run in the PCS are typically large database and transaction systems that require high availability, scalability and load balancing. Modern concepts that support such paradigm that are readily adopted in PCS ICT systems are **virtualization, mirroring and clustering**. The virtualization concept separates the hardware layer from the real physical hardware, creating a complete simulation, resulting in a system capable of running applications in an environment called **virtual machine**. In large systems like the PCS, this concept can decrease costs and provide flexibility, by routing specific tasks to the physical resources that are currently abundant, as opposed to the traditional physical server resource dedication to a certain task. The clustering concept is based on the network connection between servers, which can be utilized to provide superior processing power, provide load balancing of tasks, enable distributed data management towards various nodes or perform grid computing. Both these concepts use mirroring and in combination, they can provide a basis for the implementation of redundancy and hot-restore in case of a disaster – a solid basis for the execution of disaster recovery and business continuity within the PCS.

The separate subsystem of a great importance is the Public Key Infrastructure (PKI). It is represented by a set of policies, laws, procedures, standards, tactics and software used to regulate the operation of issued certificates and keys used to access the specific parts of the PCS databases and applications. It also includes used keys and procedures to ensure that the involved parties are properly authenticated prior to executing requests or transactions.

The issuing of certificates is entrusted to the certification authorities who are trusted by consensus and empowered to issue digital certificates and virtual (electronic) credentials used to sign, uniquely indentify and encrypt data prior to transport or storage. Every organization using the PKI should have an up-to-date centralized certificate repository with applicable certificate policy defining criteria for their use. It is in fact a storage location where certificates are being stored and published, but also, where revoked certificates no longer in use are being safe kept. Logically, the PKI infrastructure is organized in a top-down manner where all lower certification levels trust those above them, reaching the top level (root) certification authority [8].

However, in a PCS scenario the PKI system is not used only to authorize transactions within databases, but also for system requests such as the user's authentication or simple services like messaging, faxing and emailing.

3. INFORMATION SECURITY IN PORT COMMUNITY SYSTEMS

Implementing the PCS is a complex endeavor that includes all port community stakeholders and central governing authority in achieving common goals while maintaining the existing information processing and telecommunications structures and simultaneously keeping costs at a reasonable level. Looking at blueprints of the largest port communities, it can be noticed that information security is being treated somewhat marginally, in terms of technical security (logon security, antiviral protection) and PKI. However, information security encompasses much wider spectrum of activities, executed not only within the governing body, but also spreading toward stakeholders` systems.

The best prescribed way to manage information security is establishing the ISMS – Information Security Management System within the organization that governs the PCS ICT system. It initially calls for a definition of a clear security policy, statement of applicability, risk analysis and risk treatment, followed by audit testing of the efficacy of controls established to remedy possible risks and finally, repeated periodical evaluation. Internationally recognized norm that is able to achieve this goal is the ISO/IEC 27001, standard dealing with the information security management system that should be used together with the ISO/IEC 27002, before known as ISO/IEC 17799 – a practical code defining goals of security controls that represents a practical model for establishing, implementing, using, following, maintaining and constantly improving the information security management system [1].

The strong point of this way of managing information security is that it can be tailored to suit the needs of the organization that is implementing it, to support all processes and to be adjusted to the size and type of internal organization. This can also be achieved by selecting a suitable scope to which the norm applies – in case of the PCS it can be a PKI subsystem, management of the data contained within the database system or management of the information exchanged with customers (by customers meaning stakeholders present outside of the central PCS system).

The main focus should be the involvement of the PCS governing body and top management of all stakeholders to achieve the goals of the ISMS setting up and possible consequential certification. Its involvement should ensure that in the case of setting up the PCS ICT from scratch, it will be aligned with real business needs and will also be adequately financially followed. If the ISMS is set up after the PCS is in use, it will ensure that the scope of the ISMS is properly set up and a proper implementation and certification timing is achieved. Also, the segregation of the operative ICT and ICT security functions from the ICT security supervision and internal audit should be endorsed by the PCS ICT project directors.

Information security is closely connected to the basic principles of integral security that involves other activities dealing with physical security, human resources, security of service contracts, creation of appropriate Service Level Agreements, public relations, litigation and health and safety, to name but a few. The PCS's are exposed to internal and external customers in execution of their activities. The goals of the information security functions are inherently in line with the goals of the integral PCS security, best served via a centralized function of a CSO – Chief Security Officer, governing its various aspects and achieving the integral security either through managerial process or by influence.

4. INTEGRAL SECURITY OF PORT COMMUNITY SYSTEMS

In complex environments like the PCS ICT systems, it is inadequate to treat business functions separately and try to ensure their continuity and general security without a general coordination. A need arises to create an integrated model of the port community security that will integrate the best practices of the ICT and general security, align port communities with legislative requirements, provide a solid basis for certification and review on a continuous basis, allow for seamless integration of new stakeholders, provide cost optimization and finally promote internal innovation goals.

It is reasonable to expect that implementation of all these functions, that are at least partially existent within the PCS scene participants' systems, will be almost impossible if they do not let a portion of their governing sovereignty to the PCS maintaining authority. Therefore, it would be prudent to create a separate function within the PCS – an integrated security function (ISF), present at the very top of the PCS managing entity, entrusted with creation, influence and management of the integral security, keeping in mind both the particular interests of the involved PCS participants/stakeholders and the overall goals of the PCS. Such function can be similar to the CSO (Chief Security Officer) function, present in many corporations today, and it should be functionally tied to the highest management levels. It can execute its function through the hierarchy of management or managing by influence, depending on the overall PCS organization. The dedication of the top management to the integral security goals will enable the integral security of the PCS to become not only an operative duty but also the strategic responsibility.

This globally encompassing model (see Figure 3.) enables focusing into one top level function, whose main purpose is the coordination of all security efforts within the PCS, regardless of their nature or primary source. There is no doubt that the position of the manager of the integral security function (ISF) or the CSO within the PCS should be a function of the senior management, so the recruitment requirements should adequately reflect business

needs. High educational levels of the CSO candidates are highly valued across industries, so a diploma in legal sciences, business administration, accounting and finance, security management or crime investigation is expected, and so is the certification in security and related disciplines. However, in case of the PCS integral security, the liaison between business needs and organizational structure has to be further strengthened in order to reflect true business needs, so the candidate`s quality, type of experience and other achievements in maritime organization security should be thoroughly evaluated prior to establishing the function.

For the PCS CSO, it is very important to consider the overall picture and to avoid being focused in the area with the candidate's previous experience where executives usually feel most comfortable. Sometimes, in the execution of the integral security, some candidates tend to put an emphasis on the technical security or port access security, those who have a technical, of the ICT, background focus on the security of networks, applications and logical security controls, while the CSO-s with military or criminal investigation background tend to be reactive instead of proactive, and thoroughly react only when a certain threat has already emerged.

It is up to the stakeholders to decide on the adopted model of the ISF execution and whether to seek for candidates at the open labor market, or to recruit them internally. Both methods have their inherent pros and cons, but it is important that in each case the CSO candidates have to promote overall integral security of the PCS, thus raising internal and external customer and stakeholders' perceived levels of satisfaction by using the new integration model.

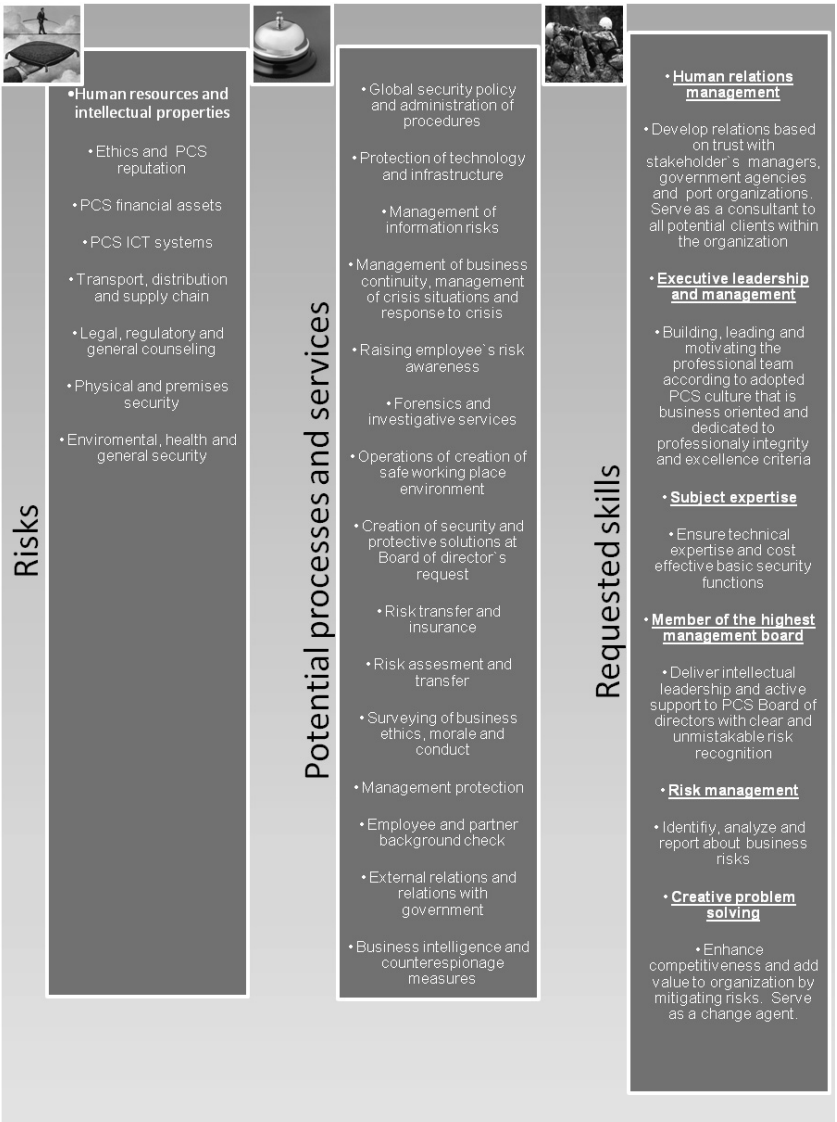

Figure 3: Port Community Integrated Security Function

Source: adapted from S. Aksentijević: "Integrated security function and information system security management – Saipem Mediterranean Services LLc, Rijeka", master thesis, Faculty of Economics, Rijeka, 2008, p. 130. [14]

5. PORT COMMUNITY SYSTEM DISASTER RECOVERY

The creation of disaster recovery procedures and of robust framework within the organization which is able to sustain disasters is a real challenge for every organization – its efficacy can be tracked by using simulations, but its real function san only be seen in case of a true disaster. The disaster recovery consists of processes, policies and procedures related to the creation of recovery scenarios for critical technologies within every organization after a human induced or a natural disastrous event.

The disaster recovery is a subset of the high level process – business continuity planning and includes planning for the resumption of the functioning of hardware, software, contained data within databases and physical communications in Intranet and Extranet environment of the PCS.

The majority of large companies spend between 2% and 4% of their IT budget on disaster recovery planning, with the aim of avoiding larger losses in the event that the business cannot continue to function due to the loss of the IT infrastructure and data. Of those companies that had a major loss of business data, 43% will never reopen, 51% will close within two years, and only 6% will survive in the long-term [7].

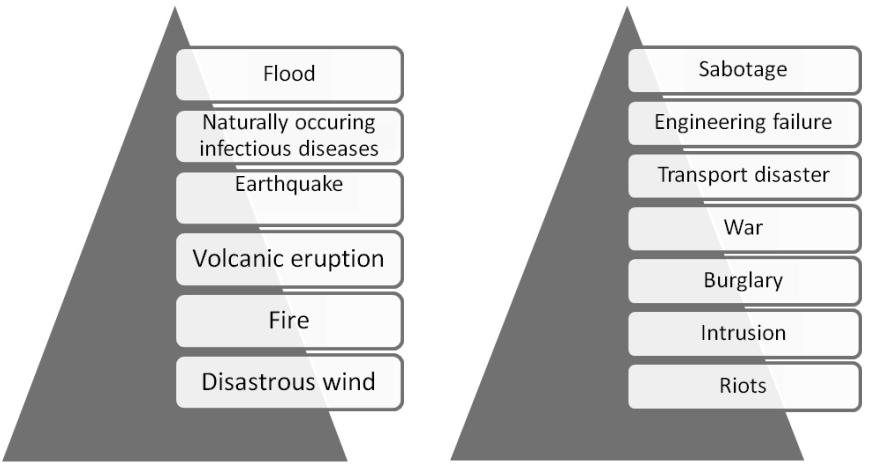

Figure 4: Sources of disasters

Source: created by the authors

The methodology of the creation of the PCS disaster recovery plan requires a disaster classification. The disaster taxonomy calls for classification in two different branches: natural disasters and man caused disasters (see Figure 4).

Colloquially it is stated that "disaster occurs when hazard meets vulnerability" [3]. The majority of commonly occurring disasters in a complex ICT scenario are those that may occur because of the exploitation of security vulnerabilities in the software, hardware or network layers. Luckily, it is the technical aspects of the ICT system that are usually protected even without external enticement, as those who are operationally running them are aware of the best practices used in order to ensure recovery from disastrous events, so they are implemented on-the-go.

The disaster recovery plan should clearly outline measures that should be executed within port security systems in order to eliminate threats, or if threats result in disasters, to remedy them. There are usually three different sets of measures that should be undertaken in order to achieve this (see Figure 5). The measures are implemented in form of controls. They need to be documented and should be tested in a simulated scenario to verify their efficiency.

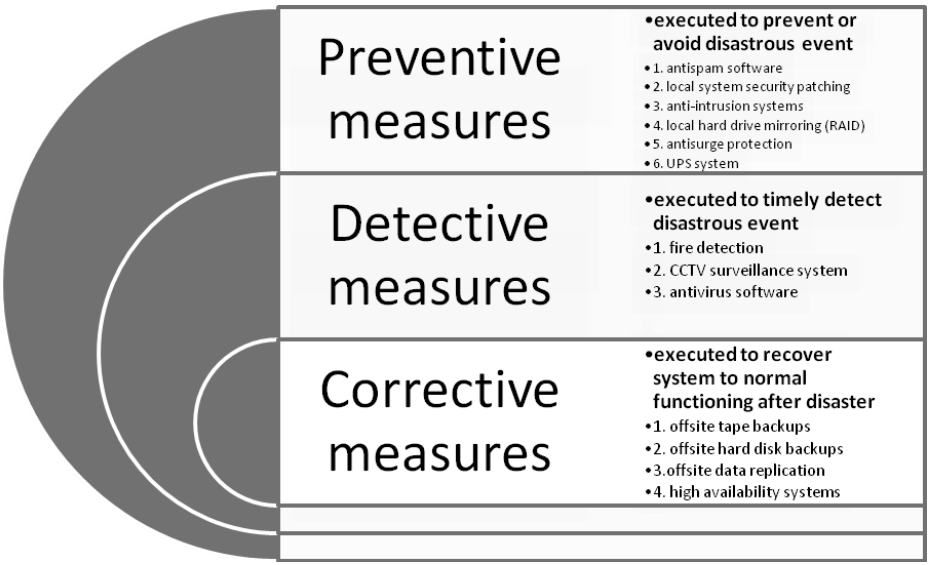

Figure 5: Disaster recovery plan measures

Source: created by the authors

Significant efforts should be undertaken within port community systems to determine those processes and systems that present core business points. Usually, these are: critical portions of the network interconnectivity system, PKI, the internal customer frontend and the database system. Within the business continuity plan, recovery point objective (RPO) and recovery time objective

(RTO) should be defined for these processes and core points, and then they need to be mapped onto a physical layer represented by the PCS ICT system.

Once that task is achieved, the disaster recovery planner determines the strategy most appropriate for each of the PCS core business processes. The real-life execution of the RPO and RTO should be aligned with the budget dedicated to this task from the PCS governing entity. The rule of the reverse reciprocation applies: the more seamless disaster recovery, the higher the cost. Therefore, if all possible disasters are anticipated, the cost of implementation will rise immensely, rendering the solutions non applicable. So, a wise implementation of the disaster recovery within the PCS ICT systems will call for:

Detailed identification of possible risks with disastrous consequences within business continuity scenario

Cooperation between those that are governing the PCS ICT system and the customers, identification of the possible forms of cooperation and decision on disaster recovery plan execution and maintenance cost sharing. This option might prove to be money-saving as existing resources (processing power, physical space, storage space) of internal customers may be used for remote recovery in case of a local system disaster. In this case, clear contractual relationship between the PCS governing body and such internal clients should be set up.

Implementation of feasible and reasonable measures to remedy disasters and disastrous event risk transference, if possible. It is quite clear that no PCS can be entirely protected from disasters, but it is possible to lower the risk and impact significantly, depending on the scope, size of the system, variety of possible disasters and dedicated investments.

6. PORT COMMUNITY SYSTEM BUSINESS CONTINUITY

Sometimes the complex ICT systems with detailed disaster recovery procedures do not have living and understandable business continuity plans (BCP-s). The main reasons usually quoted are lack of funds, complexity of activity and underlying need for cooperation between diverse stakeholders. The goal of the BCP process is the creation of a coherent and robust plan that is available to the nominated crisis management, along with the disaster recovery plan. The business continuity plan should be a part of the overall PCS risk assessment. The creation of the BCP calls for several interlaced steps (see Figure 6).

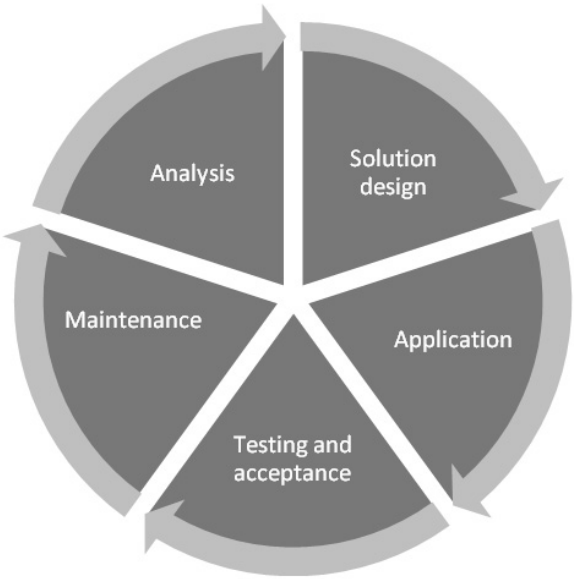

Figure 6: Phases of business continuity plan creation

Source: S. Aksentijević, E. Tijan, B. Hlača, „Importance of organizational information security in port community systems", MIPRO 32nd international convention, Conference on Information Systems Security (ISS), Opatija, Croatia, May 25-29 2009, (under review) [9]

6.1. Analysis

The business continuity planning analysis consists of the business impact analysis, threat analysis and impact scenario analysis [10]. The result of this phase is a clear differentiation between critical and non-critical functions within the PCS. The business function is considered to be critical if the implications of a certain event to the functioning of the PCS are not acceptable. This acceptability perception can be changed if the cost to establish a certain recovery function is clearly presented. Also, a business function can be considered critical if it is defined as such by the governing law. The business impact analysis results with requests to recover critical functions, which are made of the time line of recovery, business requirements and technical demands that need to be fulfilled in order to recover the function.

The threat analysis is the following step, during which the potential threats to the PCS are identified in order to detail specific ways to perform the recovery. This step is essential in order to create a successful and functional disaster recovery plan. Most threats have the potential to damage the PCS infrastruc-

ture - except for some, for example contagious diseases. After the threat definition, business impact analysis needs to be documented. The basic rule is that planning is performed for disasters of large impact and scale, and not for every imaginable small scale event, as they are usually a part of a larger disaster.

After this phase is completed, the outputs are documented business and technical plans of demands which enable the commencement of implementation. A good PCS asset management may come in handy as it enables an easy identification of available resources and also of those resources that can easily be reallocated. This documentation usually details the required number of working places at a secondary (backup) location, people involved in disaster management including contact and technical details, applications and data needed to recover the main PCS processes, temporary workarounds, allowed service interruption times and needs for stationary items. However, if the environment of the PCS is not purely an office environment, those organization units dealing with distribution or warehousing will have to cover this aspect, specific to their business function.

The results of this phase are usually documented as a separate business continuity strategy.

6.2. Design and application

The goal of the design phase is the identification of the most viable disaster recovery and business continuity solution in respect to the cost that meets two most important criteria from the business impact analysis - threat analysis and business impact analysis. The requested recovery goals are in this phase translated into operative measures. The output is the establishment of the PCS Business Recovery Organization [11].

A successful design of the PCS BCP leads to effective procedures used to escalate, inform and activate the business recovery plan, focusing to the critical organization of the business function. Typically, the organization requirements can be translated into minimum requests for the applications and data, and time that can pass until the data and applications are available (maximum "downtime").

The disaster recovery plan can also encompass components outside the PCS infrastructure and applications, for example, it can define ways to retain information stored on paper media or define methods to reestablish technologies used within a port for the physical movement of goods. Therefore, the BCP is usually overlapped with disaster recovery planning. The result of a successful design is a detailed description of the following functions and activities:

- crisis management
- secondary location of workplaces
- telecommunications structure between primary and secondary locations

- ways to replicate data
- applications and software needed for secondary location
- physical requirement of the secondary location

During the implementation, design elements are brought to a real-life execution. It can be viewed as a separate phase, but due to its operative meaning, it represents a significant portion of the PCS BCP, in regard to cost and time. These steps cannot be executed successfully if the PCS BCP Board is not established, and if the procedures for the disaster recovery and activity continuation are not clearly defined. Furthermore, the important parts of the BCP are also maintenance and evaluation of vendor contracts in order to maintain contingency reserves of all critical resources.

It is very important to roll out this activity to all PCS stakeholders and to start with internal campaigns underlying the importance of the following procedures in regard to the PCS creation and training. The PCS clients are also the external parties like local communities, police, customs or firefighters, so it is also important to include them in the BCP process if necessary.

6.2. PCS BCP maintenance

The BCP manual maintenance is separated into three periodic activities. The first one is the confirmation of outlined activities, distribution to all parties and stakeholders who are involved, and a specific training of those involved in the PCS recovery. The second one is testing and confirmation of the technical solutions used to perform the recovery. The third one is testing and confirmation of the documented procedures, usually conducted in regular intervals (once or twice per year) or when the PCS operations have been significantly changed.

The BCP manual needs to be checked in order to maintain its relevance for the organization. Usually, information that needs to be identified and refreshed include changes in the employee schedule, changes in regard to the key clients and their contact data and changes within the PCS that include the opening of new departments or organization units, closing certain sections and other fundamental changes [12].

As part of the ongoing maintenance, every technical solution used within the PCS should be checked. This refers to the checking of:

- the distribution of new virus definitions,
- the application and database security,
- the distribution of security patches,
- the equipment and application functionality and
- the information security according to the predetermined information security audit system.

Organizationally, this phase calls for the checking of working procedures used to operate the PCS ICT system, checking for changes in the ICT systems, documented work lists and recovery procedures and checking whether the infrastructure is able to reach recovery within the predetermined time frame.

6.3. PCS BC testing and acceptance

The main purpose of testing the PCS BCP should be the acceptance by the organization after proving the compliance with all requests imposed by the PCS governing authority. The testing can also be unsuccessful due to an inadequate or wrong recovery time, design errors or application errors [13]. The usual parts of the PCS BCP testing involve:

- test calls to crisis team,
- technical test of switchover from primary to secondary location,
- technical test of reverse switchover,
- application tests and
- business processes tests.

The best practice shows that the BCP should be tested at least once every two years. Apart from the clear technical acceptance of recovery measures, it is important that those recovery measures are compliant to goals, policies and ethical viewpoints of the governing authority.

7. CONCLUSION

The Port Community ICT Systems are complex systems created in order to concentrate, centralize, serve and optimize business processes within port communities. These business processes are mutually interlaced and their owners are main PCS stakeholders. However, stakeholders whose needs should be served are also: people from local communities, the police, customs authorities etc.

The PC ICT systems are usually studied as a conglomerate of hardware and software, with a set of logical rules applied to their functioning. One often overlooked function is the integral and information security, but also the methods and sets of procedures that should be used to ensure port community business continuity and disaster recovery in case of a catastrophic event caused either by human error or “force majeure” (inevitable accident).

The disaster recovery is a subset of business continuity planning procedures that refers to the specific measures that should be executed in order to restore business operations of the port community to the acceptable state in case of a major disaster. The output of business continuity planning within

port communities is a robust set of procedures that are continuously tested and set in place in order to ensure an uninterrupted functioning of the PC ICT systems by using the recognized standard methods in order to ensure business continuity in line with the goals of recovery, acceptable duration of service interruption and management approved risk and impact analysis.

The business continuity and disaster recovery should meet the agreed criteria for the cost efficient expectation goals set by the port community governing body. A reasonable application of those measures should in advance be transferred to the involved stakeholders in form of clear goals and targets, while the application should be entrusted to the business continuity board comprised of relevant instances within the port community with clearly outlined roles in execution of the business continuity and disaster recovery.

REFERENCES

[1] Hlača, B., S. Aksentijević, E. Tijan, Influence of ISO 27001:2005 on the port of Rijeka security, Pomorstvo, 22 (2008), 2, 245-258.
[2] Definition from SearchCRM.com: http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214586,00.html, 28.02.2009.
[3] Disasters and the environment (Department of Humanitarian Affairs/United Nations Disaster Relief Office - United Nations Development Programme, 1995.
[4] Srour, F. J., et al., Port community system implementation, lessons learned from international scan", Transportation Research Board 87th Annual Meeting, Washington DC, 2008.
[5] High-level analysis of the architecture, http://www.infocopter.com/know-how/multi-tier.htm, 09. 03. 2009.
[6] ITIL model definition from TheArtOfService.com, http://theartofservice.com/ITIL/ITIL/ITIL-Model.html, 22.02.2009.
[7] Hoffer, J., Backing up business - industry trend or event, Health Management Technology, Jan 2001.
[1] He, Qi, Katia Sycara, Zhongmin Su, A solution to open standard of PKI", Berlin, Springer, 2006.
[8] Aksentijevic, S., E. Tijan, B. Hlaca, Importance of organizational information security in port community systems, MIPRO 32nd international convention, Conference on Information Systems Security (ISS), Opatija, Croatia, May 25-29 2009.
[9] Aksentijević, S., Plan kontinuiteta poslovanja - faza analize, *Sigurnost.info* - Portal za informacijsku sigurnost, https://www.sigurnost.info/kontinuitet_poslovanja/plan-kontinuiteta-poslovanja---faza-analize.html, 15. 02. 2009.
[10] Aksentijević, S., Plan kontinuiteta poslovanja - faza dizajna rješenja i implementacije, *Sigurnost.info* - Portal za informacijsku sigurnost, https://www.sigurnost.info/kontinuitet_poslovanja/plan-kontinuiteta-poslovanja---faza-dizajna-rjesenja-i-implementacije.html, 15. 02. 2009.
[11] Aksentijević, S., Plan kontinuiteta poslovanja - faza održavanja prihvaćenog plana, *Sigurnost.info* - Portal za informacijsku sigurnost, https://www.sigurnost.info/kontinuitet_poslovanja/plan-kontinuiteta-poslovanja---faza-odrzavanja-prihvacenog-plana.html, 15. 02. 2009.

[12] Aksentijević, S., Plan kontinuiteta poslovanja - faza testiranja i prihvaćanja od strane organizacije, *Sigurnost.info* - Portal za informacijsku sigurnost, https://www.sigurnost.info/kontinuitet_poslovanja/plan-kontinuiteta-poslovanja---faza-testiranja-i-prihvacanja-od-strane-organizacije.html, 15. 02. 2009.
[13] Aksentijević, S., Integrated security function and information system security management – Saipem Mediterranean Services LLc, master thesis, Rijeka, S. Aksentijević, 2008.
[14] Yearbook 2007, Port Authority of Rijeka, Rijeka, 2007.

Sažetak

OPORAVAK OD KATASTROFE I UPRAVLJANJE KONTINUITETOM POSLOVANJA U LUČKIM INFORMACIJSKIM SUSTAVIMA

*Rad predstavlja strukturnu analizu objedinjenog sustava informatičko-telekomunikacijske razmjene poruka i podataka u lučkom okruženju (PCS-*Port Community System*), kao i glavnih sudionika u sustavu, internih i eksternih, koji sudjeluju u lučkim poslovnim aktivnostima. Definirana je tipična informacijska i telekomunikacijska infrastruktura PCS-a, s glavnim izazovima prilikom uvođenja sustava. Značajan naglasak je stavljen na informacijsku sigurnost unutar PCS-a, što predstavlja čvrst temelj za uvođenje koncepta i modela integralne sigurnosti. Zaključno, dvije često zanemarene poslovne funkcije su detaljno definirane: oporavak od katastrofe (*disaster recovery*) i upravljanje kontinuitetom poslovanja (*business continuity management*), kao i zahtjevi za kreiranjem robusnog plana kontinuiteta poslovanja. Cilj takvog plana je osigurati rad PCS-a u slučaju katastrofe ili predviđenog prekida u skladu s analizom sustavnih rizika informacijsko-telekomunikacijskog sustava u lučkom okruženju.*

Ključne riječi: *lučki informacijski sustavi, informacijska sigurnost, upravljanje kontinuitetom poslovanja, oporavak od katastrofe*

Edvard Tijan, dipl. inž.
Dr. sc. Serđo Kos
Dario Ogrizović, dipl. inž.
Sveučilište u Rijeci
Studentska 2
51000 Rijeka
Hrvatska