Journal of Information Systems Engineering & Management
2019, 4(2), em0098
ISSN: 2468-4376

A Contingency Plan Framework for Cyber-Attacks

Vladimir Sanchez Padilla [1], Franklin F. Freire [2*]

[1] *ESPOL Polytechnic University, Escuela Superior Politécnica del Litoral, ESPOL, Campus Gustavo Galindo Km. 30.5 Via Perimetral*, Guayaquil, ECUADOR
[2] *TECSU Tecnológico Sudamericano, Campus Urdesa Central*, Guayaquil, ECUADOR

*__Corresponding Author:__ franklin.freire@tecsu.edu.ec

Citation: Padilla, V. S. and Freire, F. F. (2019). A Contingency Plan Framework for Cyber-Attacks. *Journal of Information Systems Engineering & Management*, 4(2), em0098. https://doi.org/10.29333/jisem/5898

Published: August 29, 2019

ABSTRACT

Contingency plans administered in computer centers are necessary for business continuity since organizations not only store or process data to offer different service platforms. Organizations could experience different repercussions facing external or internal risks affecting their investments. The fact of having computer support for unwanted events that affect devices is important. Cyber-attacks in data networks lead to a serious problem due to economic damages that an unauthorized intrusion entails. A contingency plan for cyber-attacks can cover just technical issues. However, these are long term projects with continuous execution and improvement, since necessary tasks master for going from production to contingency, and then reversing the changes in the case whether an emergency or an unexpected event occurs. This paper aims to be a framework reference about how to cope with a situation of cyber-attack.

Keywords: computer hacking, data security, information security, security management

INTRODUCTION

Computer systems are for daily use, whether in the workplace, academics, entertainment or information. Dependence of always being online to solve problems or to stay informed (Baron, 2008) has increased if we measure it in timing factor, turning users vulnerable to attacks with the objective of stealing sensitive information, paralyzing systems, or sending alarms. It becomes a necessity to have an emergency plan before attacks occur (Vatis, 2002), since not only these situations lead communication devices to shut down, but also affecting organization credibility, important issue towards investors and general public systems are daily used, whether in the workplace, academics, entertainment or information.

A cyber-attack is an action taken by one person or a group to breach flaws by forcing access to restricted areas or devices for taking control of personal computers by disabling firewalls or stealing information from databases (Sanchez Padilla, 2014; Vatis, 2002).

Once both identification and mitigation protocols fail due to a cyber-attack, a solution is to deploy an alternative site, at least with the necessary items to return to online status, considering the budget and type of contingency. Different contingency plans work with different processes and the requirements to overcome a cyber-attack vary depending on the affected scenario. Fulfilling the objectives proposed previously by an organization attains solutions (Habib et al., 2017). Some of them are:

- Establishing the importance of cyber-security.
- Defining critical equipment that conveys sensitive data from both customers and suppliers.

- Analyzing service priorities provided by the organization to customers.
- Planning and detailing business continuity strategy.

CYBER SECURITY AND CYBER-ATTACKS

A definition for cyber-security is the preservation of confidentiality, integrity, and availability regarding information. This concept covers information security as the state of being protected against unauthorized use of data information as well. How can both concepts be correlated? Cyber-security focuses on virtual environments, while information security applies to traditional ways of managing information. According to computer security specialists, cyber-security aims to the prevention of in-service failures and interruptions, confidentiality violations or stored data inconvenient. Both terms can be interchangeable, representing data protection oriented for end-users, corporations or governments. In other words, cybersecurity is the security of digital information (Dunn et al., 2005).

A cyber-attack is the illegal infiltration into private or public networks to steal information. It generates failures or implanting computer viruses. Depending on the purpose, it could be considered an act of cybercrime or cyber terrorism. When classifying a cyber-attack is necessary to set goals. Cyber-Attack leads for committing a cyber-crime, a term that references to whether logical or physical damages aiming to computers, networks or connectivity devices. It derives to illegal access for stealing information or committing fraud by spoofing methods of electronic payments (Vatis, 2002). Cyber-attacks could lead to cyber-terrorism, which is an attack that is a step above of a simple cyber-crime because it uses informatics technics for developing acts against a population to cause damage for political or ideological purposes (Arcuri et al., 2017).

Another term that appears is ethical hacking. The difference between cyber-attack and ethical hacking regards in the intruder intentions even having the using the same tools and knowledge, but cyber-attacks exploit systems vulnerabilities to perform illegal damage. Ethical hacking finds the same vulnerabilities but follows steps to correct failures and invoice the service provided. Moreover, ethical hacking does not compromise information security, due to confidentiality agreements (Sanchez Padilla, 2014).

Successful or unsuccessful cyber-attacks are not carried out by isolated people. Several groups and companies are responsible for renting their services to crackers. Governments hire hackers for ethical hacking purposes and spend large sums of money for training informatics technicians to defend different systems against cyber-attacks (Arcuri et al., 2017) or to perpetrate a cyber-physical offensive in case of a cyber-war.

Intrusions can come from either outside or inside an organization, by crackers with the knowledge to enter illegally through several parameters. In some cases, the attackers could be systems administrators or related technicians (Dunn et al., 2005).

There are different reasons to encourage an attack, e.g., for boasting technology capacity or just for exploiting certain vulnerabilities in data networks (Fuchs, 2008; Sanchez Padilla, 2014). Regardless of the causes, on behalf of the law, an intrusion without consent is illegal and depending on the country or region, this can result in jail or a fine.

STAGES FOR CONTINGENCY

Contingency plans must be developed according to both general and specific aspects, applying international standards, such as ISO 27001, ISO 22301, among others. Depending on the type of business or service, it is necessary the alignment with local laws for avoiding legal issues and for complying with annual planning (Ashok et al., 2016). The plan must be executed and maintained as a project with agreements for improvements and scheduled maintenance (Ten et al., 2016). Basic stages to follow are:

- Definition
- Planning
- Realization
- Closure

The definition should begin with a clear understanding of the goal to achieve, establishing the objectives to pursue, e.g., not to lose information in case of an event, continue with business operations within a set time, in case of internal or external attacks, operate in an alternative site, whether owned or rented.

Planning establishes what type of contingency meets the defined objectives. The methodology to pursue should recover critical processes, avoid alterations in stored information, render an official version of events and (if needed) socialize it with internal and external staff. Rumors that result in the organization distrust or business continuity in short or long term must be waived, assuming controlled risks with a reduced service unavailability

time. Failure control relates for preventing abrupt power cuts, transmission grids problems, violent social demonstrations or computer attacks. Planning does not focus on the creation of a guiding document (Sanchez Padilla, 2014); it coordinates the assets, requiring a monitoring place and an alternative site based on backup devices with storage capacity to operate from short to large periods until the end of the recovery process (Ten et al., 2016).

Realization addresses the main part of the whole plan as the running of the planning stage. Errors detected and necessary adjustments turns into a contingency efficiency (Dunn et al., 2005), carrying out the following:

- Specifying requirements from different departments to attain priorities.
- Analyzing and evaluating a recovery process through a specific plan.
- Determining a recovery plan.
- Testing recovery procedures.

Closure, as the last stage, contemplates the formal acceptance of the contingency plan proposed, tested and corrected by the administration, responsible for the running in case of eventualities.

BUSINESS CONTINUITY

Planning the continuity allows the business operation experiencing short intermittency or without affecting services provision. In financial institutions, a plan contemplates virus attacks, data links abnormal saturation (Dunn et al., 2005). It is difficult to determine a continuity plan that covers the total needs of a financial institution. Two types of plans have been considered in this framework: one for business continuity and another for cyber incidents response. The combination of them guarantees adequate operations and services offered to ensure business continuity facing cyber incidents, contemplating the unavailability only in small events (McDonald, 2008). Continuity has the following objectives:

- Assuring service availability by 95% of the time in case of events.
- Backing up a site with similar devices or virtualized.
- Establishing an alternative control center to manage the contingency.
- Generating action procedures for the staff in case of a cyber-incident.
- Mitigating cyber-incidents through technological resources.

Objectives will guarantee a little impact operation, such as the unavailability for a few minutes, until the alternative system updates due to a cyber-incident. There are two scenarios for answers: 1) uploading an alternative site in case the main center suffers damage; 2) Isolating the event in a short time before the main data center experiences inconvenient.

Incidents isolation is done through detection and prevention techniques. Physical devices involved and their logical programming could get compromised since attacks are constantly mutating to break systems securities. Therefore, specialized staff in computer security have to analyze behavior regarding network traffic, bandwidth consumption, portal checking. Teams generate and study reports for determining traffic patterns and for performing regular audits about internal activities respect the use of facilities and assets provided by the organization (Sandhu, 2010).

DATA CENTERS COMPARISON

At data centers, technical staff manage configurations of servers and several devices related to operative and administrative options for the start-up and running. The deployment of a physical data center could cost more than half a million US dollars, depending on variables, such as air conditioning, energy sources, electric grids; while a virtual data center could cost approximately USD 10,000 considering several aspects, such as the no presence of rotating shifts staff, insurances, purchases, hardware depreciation, licenses updating, among others.

Large organizations offer information storage services to end-users and small/medium-sized companies without increasing costs in purchasing or configurations. **Table 1** depicts a comparison between a physical data center with a virtual data center.

The difference between them is the confidence that each one provides to the organization. In some scenarios, virtual options may not be convenient because of vulnerability (McDonald, 2008; Sanchez Padilla, 2014). Moreover, moving whether the main operations or contingency to cloud results in continuous fear of the non-technical management positions due to potential information access by crackers. At the moment of contracting corporative level services, agreements regarding confidentiality and conflict resolutions should not affect data center operations, attaining business continuity by redundancy links.

Table 1. Data Center Comparison

PHYSICAL DATA CENTER	VIRTUAL DATA CENTER
Maintenance of devices.	Leasing of devices.
Costs due to management.	Costs by configuration.
Staff with rotating shifts.	No additional staff.
Assurance against incidents/disasters.	Assurance and maintenance managed by the provider.
High investments for Small and Medium Enterprises.	Medium investments for Small and Medium Enterprises.

CONTINGENCY PLAN AND TASK GROUPS

A contingency plan has a series of potential events that could compromise business continuity (McDonald, 2008). However, this paper focuses on events classified as cyber-attacks with consequences of service unavailability. Events that result from a cyber-attack are the denied of service, filtering of confidential information, malicious infection or internal attacks (Sanchez Padilla, 2014), and the contingency plans run actions in case they appear. The official channels are the means to inform about attacks. Schedules for facing these scenarios are:

- Day time : 06:00 to 18:59
- Night time : 19:00 to 00:00
- Morning time : 00:01 to 05:59

The corresponding shifts will be according to the described scenarios. The computer center provides support during non-labor hours, but the computer security department remains responsible all the time. The infrastructure staff comes from the areas of information security, communications, computer centers, servers, and databases. Meanwhile, the development staff is responsible for applications and quality control software for keeping business continuity. The plan includes the participation of every department involved in infrastructure and development, always led by someone designated from the information security department, guiding step by step changes regarding functional tests and starts-up.

Assigning functions is a fundamental part of the plan (Sandhu et al., 2010). The planning starts as soon as an event occurs since a service either intermittent or cut must not last long. The basic premise is the permanent service availability. However, intermittencies whether programmed (e.g., maintenance, revisions, production steps) or not (e.g., logical programming failures, power cuts), affect availability at different managing levels (Ten et al., 2016).

The leader belongs to the information security department. A group of human resources keeps reports about events to external and internal staff, suppliers and customers as the only authorized information source. The leader is the one authorized to generate official reports to human resources (Dunn et al., 2005). Tasks groups involved are (Kallberg et al., 2012):

Information Security Team: Responsible for directing actions during contingency and recovery. This group documents events as a technical report and defines policies and procedures at the security level of infrastructure and development.

Communication Team: Responsible for migrating data links in coordination with the service providers, updating firewalls rules and other configurations in data centers, and after carrying out changes, the leader informs about tests and deployments for authorizing the running of the data center.

Computer Center Team: Responsible for the system monitoring and the first management level of routine and medium impact incidents. They verify services status and operations in production and contingency responding to the head of infrastructure and technology management. However, at the moment of the contingency, they have to be capable to report incidents to the leader.

Servers Team: Responsible for the servers running, whether operating systems, snapshots, and parallel configurations. In case of emergency, priority features are approached to the technical support for the computer security area.

Database Team: Responsible for the management and development of databases, relating the tasks to administration and improvement applications as well as their maintenance. During a contingency, they update tables' information by backups. At this point, they will have the support of the computer center area. The restoration time is important to pursue the contingency production stage.

Application Development Team: Responsible for the data processing, statistics, systems analysis and sales volume information, providing an environment for internal users to work efficiently. During the contingency, this team will upload the latest application updates to the data center for verifying the correct system performance.

Quality Control Team: Responsible for testing new versions and patch applications, both for information processing and applications for internal users. They verify the latest application updates deployed in the data center by the application development team.

Response procedures are the steps to pursue when activating cyber-attacks alerts. A checklist with the content of the proposed plan by the information security leader is necessary. Procedures include the stages mentioned whether before, during or after the attack, and are dependent on the recovery strategy.

Tests are gathered to schedule work programs during timelines, either for simulation, total or partial interruption before a cyber-attack. Parallel tests run without service interruption, emulating load balance mode, but in case of attacks, threats or services loss, the contingency could result affected. Tests development in the maintenance stage helps for subsequent audits to be executed (Sanchez Padilla, 2014). Procedures must follow a chronological sequence throughout an event, classifying in phases of Alert, Transition, and Recovery, described as follow:

Alert phase: Detects attacks from the first moment. They face from a partial affection to total service loss, cataloged as critical. Three parts compose this phase:

- Notification: Several tasks relate this action as defining who should inform in the first instance at the moment of compromising work stations due to a cyber-attack, especially to internal users to stop working or devices that shutdown. The leader informs to different areas the alert in case of contingency.
- Evaluation: The situation initially assesses damages with the information collected. Teams involved in the application of the contingency plan will be expecting an emergency state to be determined, not taking a long time since during a cyber-attack is valuable to avoid irretrievable data damage or deeper intrusions that compromise the organization integrity.
- Execution: When declaring an emergency, the leader starts with the contingency deployment mobilizing technology devices (servers, databases, computer centers, and control quality) to run actions already established to stop production and migrate operations.

Transition phase: It is the previous phase for migration from the main data center to the virtual data center in the shortest time possible, ensuring database information by updating and verifying operating systems performance in virtual machines. This phase includes procedures, information backup, guide manuals, as well as contingency plans and actions run by teams in coordination with the leader.

Recovery phase: Phase classified as a return to normality, considering the following aspects after attack mitigation:

- Meeting with the contingency team: To coordinate the return of the operations in the main data center. A procedure must be decided to revert changes, since new information is only found in the virtual data center, migrated by different teams under the supervision of the leader.
- Damage evaluation: After attack mitigation, there should be an evaluation of damages magnitude (if any) produced in the system immediately with enough time for recovering from errors.
- Prioritize activities: These activities focus on the real applications of the contingency compared to the plan for evaluating real damages. These should accomplish taking into account strategies applied for the organization, addressing the team dedication for temporary tasks supporting the affected systems.
- Results evaluation: To evaluate objectively every activity carried out once the actions of the contingency plan conclude, regarding response time, circumstances, staff behavior, and team performance. This evaluation comes from feedbacks and lists potential scenarios or actions which originated the cyber-attack.
- Feedback: Results valuation optimizes the original action plan, improving team actions that became difficult to accomplish, reinforcing positive actions. Operational and economic costs are elements to evaluate.

The staff involved in the tasks will review the contingency plan approved by management departments, as well as the procedures for business recovery and the resumption of the operations in the main center (Kallberg et al., 2012; McDonald, 2008). Finally, the plan is the final result of the project development start-up, approving in a straight manner to minimize impromptu decisions.

CONCLUSIONS

A contingency plan to face cyber-attacks is a proposal that organizations must consider, whether for mitigating or avoiding theft of information with the necessary assets. Cyber-attacks generate information disclosure, erasure of hard drives and services unavailability. The best contingency plan considers several possible factors due to failures either informatics or human. The organization staff needs the motivation to take care of data through the encouragements of commitments and loyalties. It is recommendable to socialize plans regarding information protection in all the organization levels, encouraging the staff to follow procedures and provide suggestions to departments in charge of information security.

Contingency plans should be applied at least twice a year previous risk analysis evaluation as well. Tests are critical because they not only provide indicators of the knowledge that staff has about the start-up of the plan and about actions where shortcomings are present, but also provide rules to overcome damages done by crackers. The

commitment is to continually achieve processes automation in necessary tasks and increasing knowledge about the information covering done by the staff.

REFERENCES

Arcuri, M., Brogi, M. and Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17)*, Venice, Italy.

Ashok, A., Govindarasu, M. and Ajjarapu, V. (2016). Attack-resilient measurement design methodology for State Estimation to increase robustness against cyber attacks. *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA. https://doi.org/10.1109/PESGM.2016.7741979

Baron, N. (2008). *Always On: Language in an Online and Mobile World.* https://doi.org/10.1093/acprof:oso/9780195313055.001.0001

Dunn, M., Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich), ITU (2005). A comparative analysis of cybersecurity initiatives worldwide. *WSIS Thematic Meeting on Cybersecurity*, Geneva, 28 June – 1 July 2005, Document: CYB/05.

Fuchs, C. (2008). *Internet and Society: Social Theory in the Information Age* (1st Edition). Routledge Research in Information Technology and Society.

Habib, H. F., Lashway, C. R. and Mohammed, O. A. (2017). On the adaptive protection of microgrids: A review on how to mitigate cyber attacks and communication failures. *IEEE Industry Applications Society Annual Meeting.* https://doi.org/10.1109/IAS.2017.8101886

Kallberg, J. and Thuraisingham, B. (2012). Towards cyber operations - The new role of academic cyber security research and education. *2012 IEEE International Conference on Intelligence and Security Informatics*, Arlington, VA. https://doi.org/10.1109/ISI.2012.6284146

McDonald, R. (2008). New considerations for security compliance, reliability and business continuity. *2008 IEEE Rural Electric Power Conference*, Charleston, SC. https://doi.org/10.1109/REPCON.2008.4520132

Sanchez Padilla, V. (2014). Data Network Threats and Penetration Testing. Journal of Telecommunications, 28(2).

Sandhu, R., Krishnan, R. and White, G. B. (2010). Towards Secure Information Sharing models for community Cyber Security. *6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010)*, Chicago, IL. https://doi.org/10.4108/icst.collaboratecom.2010.3

Ten, C., Ginter, A. and Bulbul, R. (2016). Cyber-Based Contingency Analysis. *IEEE Transactions on Power Systems, 31*(4). https://doi.org/10.1109/TPWRS.2015.2482364

Vatis, M., (2002). Cyber Attacks: Protecting America's Security against Digital Threats. *ESDP Discussion Paper ESDP-2002-04*. John F. Kennedy School of Government, Harvard University.