EasyChair Preprint

№ 1544

Implication of employees in security policies definition

Myriam Djerouni

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

September 22, 2019

Implication of employees in security policies definition

Myriam Djerouni

Chief Information Security Officer at Luxith G.I.E.
5, rue des Mérovingiens - Z.A. Bourmicht L-8070 BERTRANGE, Luxembourg
myriam.djerouni@luxith.lu

Abstract. A way of awareness is to involve employees in part of the definition of security policies. The purpose of this approach is not to reduce the level of security required and defined by the policies but to consider when it is possible and applicable their comments. In this case, employees accept more easily the application of policies as they have "participated". Then, the policies should be present to employees during interactive sessions with real cases of security breach, figures, and statistics to illustrate the risks. The benefits of these presentations are to show to employees that risks are not only theoretical and it can really happen.

The purpose of this document is to provide guidance on how to create more cybersecurity awareness, topic handled by the CyberEDU in February 2019. This paper presents the implication of employees across the life cycle of the security policies based on the PDCA (Plan-Do-Check-Act) model. The document will addresses the definition of Information Security Policy (ISP) as well as topic-specific policies and the involvement of the Top Management and employees.

Keywords: Policy maker, Implication of employees, Security Awareness, Interactive Awareness

1 Introduction

1.1 Definition of policies

First, a quick look at the official definitions of "Information security policies" presents in International Standards:

According to the ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary [1], Policy is defined as follow: *"intentions and direction of an organization, as formally expressed by its top management."*

To complete this definition, IOS/IEC 27002:2013[2] - Information technology — Security techniques — Code of practice for information security controls, the control of Information security policies is described as follow: "*A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.*" To respond to the following objective: "*to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.*"

According to the NIST - Glossary of Key Information Security Terms published in 2013, Information Security Policy is "*Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.*"

Policies are the foundation of your security controls design, implementation and review. They are the first step to manage the Information Security in a company. However, the importance of their definitions could be minimized.

1.2 The problematic of policies

Security Policies are defined in many companies, but sometimes this task is underestimated.

For them, policies are the result of a patchwork of copy-paste from documents found on Internet and/or policies defined within other companies, defined by the CISO on his own and simply published on the company's Intranet. The policies are too generic to know what to do with it and sometimes employee do not know their existence. Why they act like that? Because it is mandatory to have security policies in place and probably the Top Management is not acting like a sponsor to support and promote the security policies.

But they forgot the main purpose: a security policy must be applied. To do so, a policy must be clear, understandable, communicated, challenged and reviewed. Then, policies will be declined in operational procedures, which lead the day-to-day of employees.

These characteristics are not explicitly described in the official definition but can be added when a company decide to define it.

2 Definition of policies – "Plan" stage

2.1 Scope of policies

The document addresses the definition of the Information Security Policy (ISP) as well as topic-specific policies. The first one is more high-level and defines the main security objectives in a company by the Top Management, the second ones are more target and respond to specific controls and could be defined in collaboration with target employees.

2.2 Implication of the top management

The first people that you have to be implied and convinced are the Top Managers as they will act as a sponsor for the implementation of security policies. Their implication is essential to define the Information Security Policy, as it provides the management direction and support and it will lead the topic-specific policies.

Sometimes it can be easy, sometime not. It depend of different factor: the domain where you work, the awareness regarding security of your management.

If you prepare an ISO 27001 certification, things could be easier as the management commitment is a requirement of the standard. However, mandatory or not they have to be convinced!

How to motivate the top management?

Their goal is to run a business. Regarding the security, their main concern is how much it will cost. But the real question is how much it can bring to them. You can provide positive arguments in this way: bring sustainability of the business (with the security goal Availability), customer retention, acquire new ones (the security goals Confidentiality and Integrity will increase the trust of your customers), respond positively in Request for Proposal as security can be a requirement, avoid important penalties due to the lack of security.

In fact, you can also show them companies, which failed due to the lack of security, huge penalties they have to pay, the bad reputation they had and so on. The fear of fine, bad reputation, loss of credibility is also a good motivation for the Top Management to be implicated in the security in general. Moreover in parallel, companies are subject to regulations, certification and/or annual audit during which security and general IT controls can be assessed and requested obligations for the company to have a certain security maturity level. You can use these obligations as leverage to involve the Top Management.

Who of the top management should be involved?

The list below is not exhaustive and depend on your organization. But you need at least:

- The Chief Executive Officer (CEO) to commit, support the approach and ensure that adequate resources are in place for the implementation,
- The CIO to ensure that IT in place support properly the business,
- The Head of Business to define the business needs,
- The Head of Legal and Compliance to list the laws and regulations that the company must comply with and respect.

In collaboration with the Top Management, you will define the right balanced between security and service delivered to customers. In fact, if IT is here to support the business, security information is a way to do business: you have to make business securely. It is your goal.

How to define security objectives?

It depends on your business. You have to ensure the three main security objectives: Confidentiality, Integrity and Availability, the respects of laws and regulations, ensure that you deliver a service with goods quality, ensure that you mitigate risks related to your company. This is "common sense" basically.

According to your domain, the focus on security objectives and risks will be different. For example, in healthcare, the confidentiality and integrity will be essential for the patient data in parallel availability primordial for the medical care and treatment. In automotive industry, the confidentiality is important to protect the intellectual property rights to avoid industrial espionage and the availability essential for the supply chain to avoid a stop of the production and important financial loss.

How to involve the Top Management?
First, go straight to the point, they do not have time to make workshop. You have to prepare an ISP to submit to them for comment and validation. The ISP should have at least these topics:

- The security objectives – based on your knowledge of organization, make a proposition of security objectives as described above. For the list of laws and regulation, you have to request to the Head of Legal and Compliance who will assist you as it is also in its interest.
- Define the management commitment (like for example: participate to security committee, support the approach of CISO and decision made, provide resources to support security policies)
- Define clearly the roles and responsibility
- Make a proposition of Topic-specific policies – this input will interest the CIO as the majority is related to his teams
- Entry into force and validity
- The impact on Business for no respect of security policies and the potential disciplinary sanction
- Continuous improvement – to comfort the Top Management as well as employees that security is an ongoing process and the improvement will be step by step

Secondly, create a Security Committee during which the Top Management is a main actor. This committee will be used to validate all security policies, to follow their respect in the organization and to discuss about all security matters.

Once you involve the Top Management, you have the main directives and support to discuss with employees for the specific policies.

2.3 Implication of employees

The implication of employees is helpful to define the topic-specific policies.

Why is it important?
Information security is seen as constraint and source of workload. Therefore, employees can be reluctant to apply policies or security in general.

What are the benefits?

They are multiple. From the CISO side: policies are more concrete and comprehensive as specific aspects of the company are provided by teams, it ensure that policy are technically feasible.

From the employee's point of view, by being involved, they will not have the feeling that the policies are imposed to them. They provide inputs based on their knowledge of the profession and of the sector in order to construct policies understandable and applicable. It is also rewarding as their expertise is taking into account.

The result of this collaboration is to have concrete and pragmatic policies to apply.

Who involved and How?
A CISO cannot be expert in all domain: development, system administration, database, physical security, procurement, human resources and so one. He/she needs to request inputs from relevant collaborators to define topic-specific policies. The target collaborators depends on the policy subject. For example:

- For operational policies like access control, backup, hardening, asset management : IT representative
- For policies related to physical security: Responsible of the facility and premises
- To define rules regarding security in development: Head of development and developers themselves as they code and are the direct person to apply the policy. They can highlight problematic they encounter on the day-to-day basis.

Some policies can required different departments implication like:

- For patching policy: IT Operation to apply patch, Head of service to coordinate time schedule, customers information and validation tests.

You have to do what your policies requires. In this case, through workshop, start with relevant employees to describe the existent and enhance it with security principles. Thanks to the principles of continuous improvement, no need to perform a complete revolution for each policies and procedure during the first iteration. Relevant employees can also be source of proposals because policies can help them to enhance their own process. For example, during the workshop to define physical security, alarm system in place could be obsolete and it can be a good argument to ask for an up-to-date system from the Top Management.

How ensure that minimum of security?

Do not be too strict otherwise, it could lead to shadow IT and then security could be bypassed. Keep in mind that a policy must be applied, respected and followed. It is important to keep it realistic!

But in meanwhile, you have to ensure a minimal baseline of security. To do so, policies must include the Best Practices (it is non-negotiable) and must be flexible. Policies exception can be approved under condition that it is well identified properly justified and validated by the Security Committee for a specific period.

How deals with comment contractor?

In any case, the Security Committee will have the last word. But in order to not offend employees if you do not include his/her comment, take time to explain why. Otherwise, employees will not be motivated anymore to participate if they have the feeling that their arguments are not taken into account.

What about big structure?

Security policies coming from the Head Quarter and distributed to affiliates for application are seen like "imposed". In order to be more acceptable by target employees, it is recommended to add in the first page of the policy the name and position of employees participating to the elaboration of policy. Then, target employees will be comforted that job constraint have been taking into account.

2.4 Validation of policies

Polices are validated by the Security Committee and entry into force. Policies exceptions are also validated and followed during this meeting.

Once it is validated, policies can be communicated to employees and must be applied.

3 Implementation of policies – "Do" stage

3.1 Publication

First, security policies must be communicated and accessible to employees. The easiest way is to publish it on the company Intranet following these recommendations:

- CISO must informed employees when a policy is available and/or has been updated
- A summary may accompanied the policy with the main points.
- The intranet page containing policies should offer the possibility to employees to put comments or ask questions. These employees' inputs can be very helpful for the awareness preparation and updates

3.2 Presentation

The security awareness frequencies are:

- During the entrance of new employee
- During regular awareness sessions, at least once a year, to constitute a great reminder of rules and responsibility of all employees.

The session should be interactive:

- The session should also present security figures and facts, presentation of real security breaches to demonstrate to employees that risks are not theoretical. A relevant material is the yearly Verizon Data Breach Investigation Report [4], which present per industry the security breach and the hacker motivation. One conclusion can be that simples vulnerabilities are still more exploited (unpatched server, SQL Injection, weak passwords …)
- Propose a mini quiz – people are more concentrated if they are evaluated. But to avoid the scholar method, this evaluation form should be fun, like a game.

4 Control of policies – "Check" stage

4.1 Frequency and purpose

Once a year, policy should be controlled in different ways to know if it is applied or not:

- Audits
- Controls

If a policy is not respected it means two thinks:

- It is not applicable, too restrictive to be applied and respected
- Not enough communicated and/or aware

4.2 Measuring tool to validate if security increases or not.

Several controls/methods could help for the review:

- Key Performance Indicators specific like percentage of servers patched, number of access review …
- Controls in place like clean desk policy control. Regularly at the end of the day, enter in every office and check if confidential document are on desk or in the trash, harvest them and make a confidentially note to the person who let these information and in parallel, present the result (anonymized) of the controls on Intranet in order also to aware and remind the rules.
- Exercise like phishing campaign.

The latest controls have both purpose: control the correct application and aware the employee as they learn by their mistakes.

5 Update of policies – "Act" stage

Policy must be regularly at least once a year or after main change in organization reviewed to ensure that it is still applicable, not obsolete and still fit with company's goals and organization.

At the end of a cycle, make an assessment about the application. Main inputs to perform this update:

- Comments of employee left on Intranet or during presentation session
- Internal / external audits result and recommendation to know if the policy is applicable
- Number of policies' exceptions
- Number of incidents related to the no respect of the policy
- KPI trends
- Result of Controls

The policy should be readapted in function and validated by the Security Committee.

6 Conclusion

Information security is not only a matters of the CISO and he/she cannot ensure security alone. He/she need to be supported and assisted by all employees as everybody should be concerned. In order to involve employees, efficient security awareness may be conduct. A solution is to imply employees in every stage of a policy: definition, communication, controls and update. Therefore, securities policies are concrete and pragmatic to be applied.
This approach requires several soft skills that a CISO should have. He/She must promote the security, and be able to adapt his/her speech to target public, to explain the risk to technical and non-technical people and to convince them. He/She must also have leadership skill and patience.

References

1. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
   https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
2. IOS/IEC 27002:2013[2], Information technology — Security techniques — Code of practice for information security controls
3. NIST (National Institute of Standards and Technology)- Glossary of Key Information Security Terms published in 2013
   https://www.nist.gov/publications/glossary-key-information-security-terms-1
4. Verizon Data Breach Investigation Report
   https://enterprise.verizon.com/resources/reports/dbir/