Smashing the Information Security Policy for Fun and Profit

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

日本語版も入手可能
www.isaca.org/currentissue

One of the chief components of an organization's information security strategy is the security policy. This is a compulsory, high-level administrative document that sets out the strategic objectives and principles of information security that must be adhered to in any activity that may affect the organization's environment and defines the responsibilities and roles of all the actors involved. By way of a rhetorical comparison, it could be said that an information security policy is to an organization what a constitution (or the Magna Carta) would be to a country.

However, and just like an organization's physical or logical assets, the documentary and administrative components of an organization have vulnerabilities and can be exploited to impact its security and operation. Sadly, these kinds of vulnerabilities are not taken into account in a "traditional" risk analysis, leaving the organization exposed to potential attacks, such as a "work-to-rule."

David Eduardo Acosta R., CISA, CRISC, CISM, BS 25999 LA, CCNA Security, CEH, CHFI Trainer, CISSP Instructor, PCI QSA, OPST
Is an information security consultant and lieutenant in the Professional Reserve Officers of the National Army of Colombia. He currently works with Internet security auditors in Barcelona, Spain, and is chief editor of *PCI Hispano (www.pcihispano.com)*, a web portal specializing in Payment Card Industry Security Standards Council standards in Spanish. He is an active member of the IEEE. He can be contacted at dacosta@ieee.org.

The "Work-to-Rule" in the Unionized Context

A "work-to-rule," or "rule-book slowdown," is a type of industrial action where workers take advantage of errors in the contextualization and details of a procedure, applying these in the strictest, most meticulous and literal way possible in normal operating conditions, leading to delays and alterations in the organization's productivity. Unlike traditional strikes, which involve explicit temporary cessation of labor, in a work-to-rule, the tasks assigned to the worker are neither interrupted nor lacking compliance with established rules. This tends to make them more effective and more difficult to contain and correct. Often, this type of industrial action is developed in a covert and highly organized fashion, leaving management without any means of handling its impact.

One of the sectors most prone to undertaking this kind of action is the health care sector.[1] In this sphere, procedures for hygiene and handling of patients, samples and medications must be extremely detailed to guarantee their appropriateness and safety, for both the patients and medical staff. However, if these protocols are written in a specific way and then adjusted to the medical environment where they are to be applied without considering possible exceptions, their strict implementation may lead to unjustified delays in care and abusive bureaucracy, even to the point where human lives could be at risk. By taking advantage of this pressure, striking workers can exact compliance with their demands. Additionally, if the administration seeks out the potential causes of the industrial action, it may turn out that the origin lies in its own shortcomings in its phrasing of the regulations. This might render it counterproductive to ask the workers not to comply with the procedures initially established and thus be forced to accept responsibility for their entire impact on the operation, without the tools to apply corrective measures with respect to the personnel who have taken part in the industrial action.

Undermining an Information Security Policy With a Work-to-Rule

Following from the concept previously described, undermining a poorly written information security policy can be fairly easy. Taking into account that the vast majority of these documents are based on generic templates, are rarely reviewed, are not adapted to the actualities of the organization's business or the current state of its information environment, and generally do not include procedures for managing exceptions, the reality of adhering strictly to these types of regulations can lead to delays in operation and/or consequences for the integrity, confidentiality or availability of information. With the addition of the obligation-to-comply factor on the part of those involved, such failures can be amplified by means of a work-to-rule, causing productivity losses to the business, with knock-on effects that are both financial and operational (i.e., affecting service level agreements [SLAs]).

Additionally, an information security policy is supported and complemented by auxiliary documents that focus more on specific areas/topics whose importance is classified according to the degree of obligation they entail. This is the situation for regulations, standards, procedures, technical instructions, guides, recommendations, etc. The implementation of a work-to-rule would be possible via any of these components of an organization's regulatory framework.

Several illustrative examples of work-to-rule on an information security policy or a vulnerable auxiliary document include:

- A company's information security policy makes it obligatory for "all operating systems susceptible to malware to have an updated, working antivirus solution installed." However, this organization has within its computer pool a series of stations with limited hardware used as point-of-sale (POS) terminals. A work-to-rule can be implemented through the obligatory installation of antivirus software on these stations, with the ensuing impact on their performance and availability adversely affecting customer response times and normal operation, as well as their response to daily transactions and sales.
- The information security policy makes it obligatory to install security updates during the month following their release by the manufacturers. The work-to-rule could be applied to the unplanned-for updates to critical components by merely complying with the time frames indicated, which can affect the availability of the company's services.
- With regard to password management, the policy states that "changes to passwords that have been forgotten must be applied with physical validation of the user's identity." If the user is not in the city or the country, the administrator in charge of the change may apply the work-to-rule to the implementation of this check, thereby affecting the user's access.

> **"Undermining a poorly written information security policy can be fairly easy."**

Additional examples can be found in the implementation of policies on change management and user management, where often the stages for request, approval and implementation tend to be very strict and the implicit red tape can be exploited in a process of work-to-rule, impacting the company's normal operation.

Unfortunately, the organization affected by this problem cannot contradict itself by making its workers disobey the security policy's controls, since this would invalidate the regulations; thus, the situation leaves the company at the mercy of the resulting procedural chaos.

Enjoying this article?

- **Learn more about, discuss and collaborate on information security policies and procedures in the Knowledge Center.** *www.isaca.org/information-security-policies-and-procedures*

Protecting a Security Policy From a Work-to-Rule Attack

It is easily concluded from the aforementioned descriptions that the vulnerabilities exploited by a work-to-rule are usually related to errors in phrasing, problems with the management of exceptions, lack of updating, and the design of a security policy or its auxiliary documents that does not reflect the reality of the company and is inappropriate in operational terms. These kinds of mistakes generally have their origin in the belief that security documentation serves only as filler for the purposes of bureaucratic procedures and no one ever reads them—common faults in developers, operators, systems administrators and some misguided heads of security.

> **"The security policy should be designed to adapt to the environment it protects rather than the reverse."**

To prevent this risk, the following series of premises should be borne in mind when drawing up and implementing a security policy:

1. **Carry out periodic testing with hypothetical scenarios to identify failures in the policy that could be exploited by malicious users.** To identify weaknesses in the regulatory framework before they can be exploited by malicious employees, management can make use of exercises involving the application of the information security policy in simulated situations where the participants—personnel from key areas within the company (i.e., legal, human resources, public relations, physical security, business continuity)—can interact in a hypothetical scenario. These types of exercises are very common in plans for incident response and business continuity, whose testing methodology can also be extrapolated to information security policies.

   To detect problems that may be exploited by a work-to-rule, it is necessary to analyze a situation involving the application of a security policy (simulation principle) and go step-by-step through the instructions described in the regulatory framework. If the process detects any tasks or guidelines that could adversely affect normal operation or if cases of possible exceptions are identified, they are reviewed in detail and the following criteria are applied.

2. **Analyze the organization's information security context and try to find a balance between security and operational controls.** The security policy should be designed to adapt to the environment it protects rather than the reverse. This is why it is necessary to have prior, detailed understanding of the need to protect information and the cultural environment in which the organization works so procedures can be written that are:

   - **Logical**—Procedures should be as natural as possible and aligned with the organization's present operation. Likewise, they must comply with cost/benefit criteria based on the potential existing threats. Implementing controls that are out of line with the reality of the company can lead to controls whose focus is either too narrow or too broad and that can needlessly prove wearing to the organization. At this point, the experiences of other organizations are often useful for review purposes (benchmarking).
   - **Precise**—The policy should be written in such a way that it expresses exactly the organization's security needs and focuses on this point in particular. Any deviation can open the door to a potential vulnerability. Modularization can be an important element at this point.
   - **Concise**—The policy should be phrased using only those words strictly essential to express the idea. It should avoid the use of any words that

may be unusual, superfluous or unnecessarily technical, or any filler phrases that might blur the concept and permit ambiguity and misunderstandings. Brevity is essential.

- **Timely**—The policy should be up-to-date at all times and describe the present situation and needs of the environment in which it is being applied. The imbalance between changes and controls can result in a deterioration of security levels, allowing vulnerabilities in the implementation of countermeasures and safeguards.
- **Clear**—The policy should be written with the target audience in mind (i.e., the users). Anyone who reads the document should be able to understand it without needing to resort to external references. This means restricting the use of technical terms to those strictly necessary and utilizing simple language.
- **Complete**—The security policy should adhere to the maxim of the five Ws (and an H):[2]
  – Who?
  – What?
  – Where?
  – When?
  – Why?
  – How?

  The absence of any of these elements in a guideline can indicate that it is an unnecessary control that can be ignored as it has no practical justification.

- **Objective**—The policy should be written in the third person, eliminating any subjective factor that might indicate that a guideline was chosen due to favoritism or preference for a particular individual, technology or area.

  On finishing the task of writing the policy (or during review/reevaluation), its guidelines should be analyzed in terms of these listed filters for the purpose of identifying any unnecessary or vulnerable elements.

3. **Establish compensatory controls and measures for exceptions.** The flexibility to adapt to inevitable changes in technology and new threats should be a key factor in the security policy to ensure its validity and currency. In addition to guidelines (among which the policy itself is to be found) aimed at deterrence, prevention, detection, correction and recovery that make up the basic protective arsenal, there should be compensatory controls. A compensatory control is defined as an alternative control that can be implemented when there is a justified administrative or technical limitation (exception) that does not allow the use of an initially established guideline.[3] These types of controls allow a level of security equal or superior to the original.

> **“The use of incentives can be implemented as a tool for persuading personnel to become involved in these types of initiatives.”**

In addition, it is essential to establish extraordinary measures in case of emergencies. These measures are known as exceptional measures and they enable the policy to be adapted to unforeseen situations, acting as a countermeasure in the event of a control failure or a response to unforeseen activities.

4. **Define communications mechanisms to obtain feedback from the policy's users.** The creation of bidirectional communications channels allows management to garner first-hand information from policy users that can be used to adapt the policy on the basis of experiences of day-to-day operation. Contact forms, suggestion

boxes, online chats or other social network tools can be valid channels for gathering feedback that will enable early detection of errors and their proactive correction.

The use of incentives can be implemented as a tool for persuading personnel to become involved in these types of initiatives.

> **“The use of incentives can be implemented as a tool for persuading personnel to become involved in these types of initiatives.”**

5. **Establish schedules for periodic review of the security policy and updates when significant changes to the environment arise.** Responsibility for reviewing documents, deadlines and scenarios that trigger these reviews should be established in the policy itself, including changes in technology, entry or retirement of third parties, delegation of tasks to external companies (i.e., outsourcing), and acquisitions/mergers, which may be catalogued as significant changes in the environment.

   Additionally, it is essential that the head of security keep the controls in the security policy aligned to the threats in the environment. This guarantees that application of this document is valid and aligned to the reality of the company, avoiding obsolete or unnecessary guidelines.

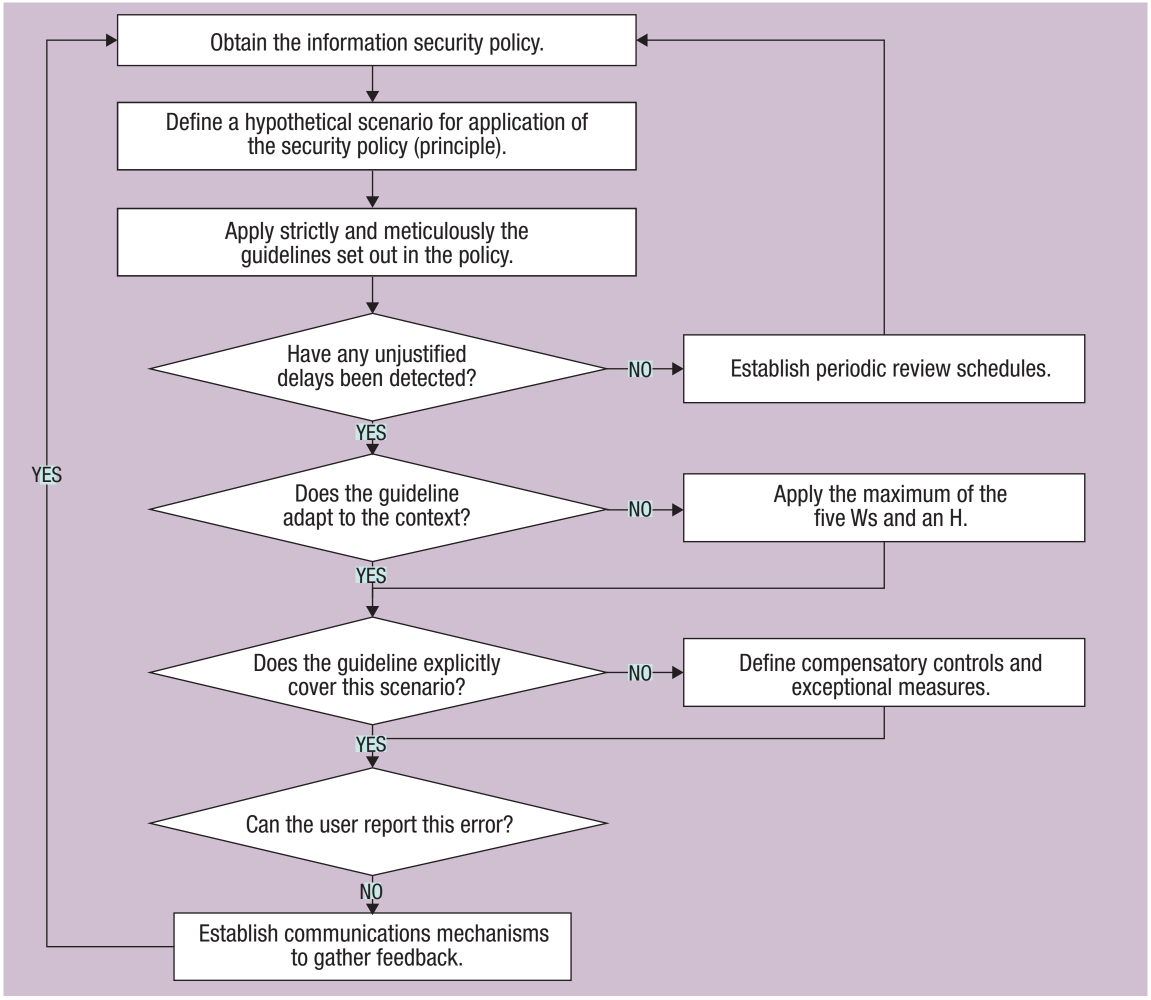
   Broadly speaking, the flow of validation would be as shown in **figure 1**.

Conclusion

Based on the information an organization manages, the security policy should set out the requirements and controls for the protection of the various assets according to their criticality. It is precisely at this point that the phrasing of a policy is a key factor, since, depending on the way in which the aforementioned guidelines are expressed, there can be flaws due to either excessive laxity or restrictiveness. These vulnerabilities can be the objective of abusive bureaucracy on the part of malicious staff using a work-to-rule, where guidelines are followed in their strictest form. If the policy is not up to date or in line with the operational reality of the organization and fails to allow for management of exceptions, the impact of this type of industrial action or sabotage could have grave consequences for the company’s handling of information security.

To prevent and manage this problem, there should be methodological application of bidirectional channels of communication with the personnel involved, administration of periodic tests to search out potential incongruities in the document, recurrent reviews of the regulatory document, use of compensatory controls and exceptional measures, and ongoing analysis of the organizational context and definition of the cost/benefit of the guidelines. These tasks will work together to prevent the policy from ending up as a “dead letter” that will, sooner or later, become a threat to the company itself.

Figure 1—Validation Flow for Updates to Security Policy to Avoid Work-to-Rule


Obtain the information security policy.
Define a hypothetical scenario for application of the security policy (principle).
Apply strictly and meticulously the guidelines set out in the policy.
Have any unjustified delays been detected?
NO
Establish periodic review schedules.
YES
YES
Does the guideline adapt to the context?
NO
Apply the maximum of the five Ws and an H.
YES
Does the guideline explicitly cover this scenario?
NO
Define compensatory controls and exceptional measures.
YES
Can the user report this error?
NO
Establish communications mechanisms to gather feedback.

Source: David Eduardo Acosta R. Reprinted with permission.

Endnotes

[1] ABC España, "Los enfermeros convocan una huelga de celo por el decreto que les impide prescribir medicamentos", 28 October 2015, *www.abc.es/sociedad/abci-enfermeros-convocan-huelga-celo-decreto-impide-prescribir-medicamentos-201510281549_noticia.html*

[2] Spencer-Thomas, O.; "Writing a Press Release," 20 March 2012, *www.owenspencer-thomas.com/journalism/media-tips/writing-a-press-release*

[3] Williams, B.; "The Art of the Compensating Control," March 2009, *https://www.brandenwilliams.com/brwpubs/TheArtoftheCompensatingControl.pdf*