Today's solutions are smart enough to detect the possibility of a recorded voice and request additional information. Indeed, random questioning built into the script could ask callers to repeat a word or phrase to guarantee a 'live' person is on the line. Recruiting the services of Rory Bremner or Jon Culshaw won't help either. The unique characteristics of each person's voice are sufficient for the speaker verification software to detect impostors, however much we think these entertainers sound like other people.

Recent events have shown how important biometrics has become in face to face security situations. However, any business that needs to offer convenient, high-value electronic services where the person isn't present needs to look at a solution that will minimise the risk of fraud. The individual characteristics in our voices make speech verification systems one possible solution. The flexibility included in today's systems offers organizations the ability to balance security against usability.

Where there is low security risk, dealing with non-sensitive or non-private information, configure the system to be more lenient towards unknown prompts or voice prints. However, where sensitive or confidential information is involved, ensure that the system is configured to block any attempt to access from an unknown source. Configuring the system to suit the level of security required will help organisations adapt speaker verification for their own specific applications.

About the author

Steve Kinge has worked at Nortel for eight years and has recently moved into the role of product marketing manager in EMEA for Nortel's contact centre solutions. Highly experienced, Steve has spent almost thirty years in the communications industry in both sales and marketing roles having previously worked at Telephone Rentals, Mercury Communications and Siemens Communication Systems Limited.

Reference

[1] Large Scale Evaluation of Automatic Speaker Verification Technology, Dialogues Spotlight Technology Report, CCIR, May 2000.

Security standardization in incident management: the ITIL approach

Dario Forte, CEO, DFLabs Italy

You can't throw a stone these days without hitting a standards document claiming to offer the state of the art in IT incident management. Many of them focus on organizational aspects rather than on incident response in the strict sense. In this article we will examine the ITIL approach to incident management.

One milestone of the Information Technology Infrastructure Library (ITIL) standard is the development of an effective model of incident management. It ensures IT service continuity in relation to the four elements of Information Technology Service Management (ITSM): organization, personnel, technologies, and processes.

According to the most recent ITIL definitions, the main purpose of incident management is to minimise interruptions in business activities and ensure availability of service. We find little here of what we might read in the RFCs on incident management (specifically RFC 2350), or in the ISO 17799 standard.

The divergence between the ITIL approach and the principles laid out in the literature is further evidenced in the respective definitions of IT incidents. While the RFCs speak of any violation of company security policies, in ITIL an incident is "any event that is not part of the standard operation of a service and which causes, or may cause, an interruption or reduction in the quality of that service".

ITIL and security incidents

Can these definitions be made to coincide? To answer that question, let us look in some detail at the ITIL incident management model. The figure below provides an overview of the process components.

Investigation, diagnosis, resolution, and recovery fall strictly within the purview of the computer security incident response team (CIRT), which will handle the digital investigation and the restoration of function process. Nevertheless, the above scheme implies a great deal of responsibility on the part of the service desk, and yet in the organizations I have visited, the service desk function is detached from security, especially within the enterprise context.

The role of the service desk

According to the ITIL approach, regardless of who actually manages the various tasks, the service desk owns the entire process. It appears unlikely that the service desk's role in incident management will extend beyond an interface for internal users and external customers. With the exception of a few specific cases, it will be difficult to apply this attribution of ownership in an effective way in real world situations.

The service desk can deal with tracking and communication by handling the closure phase and transmitting messages to the figure or function that started the

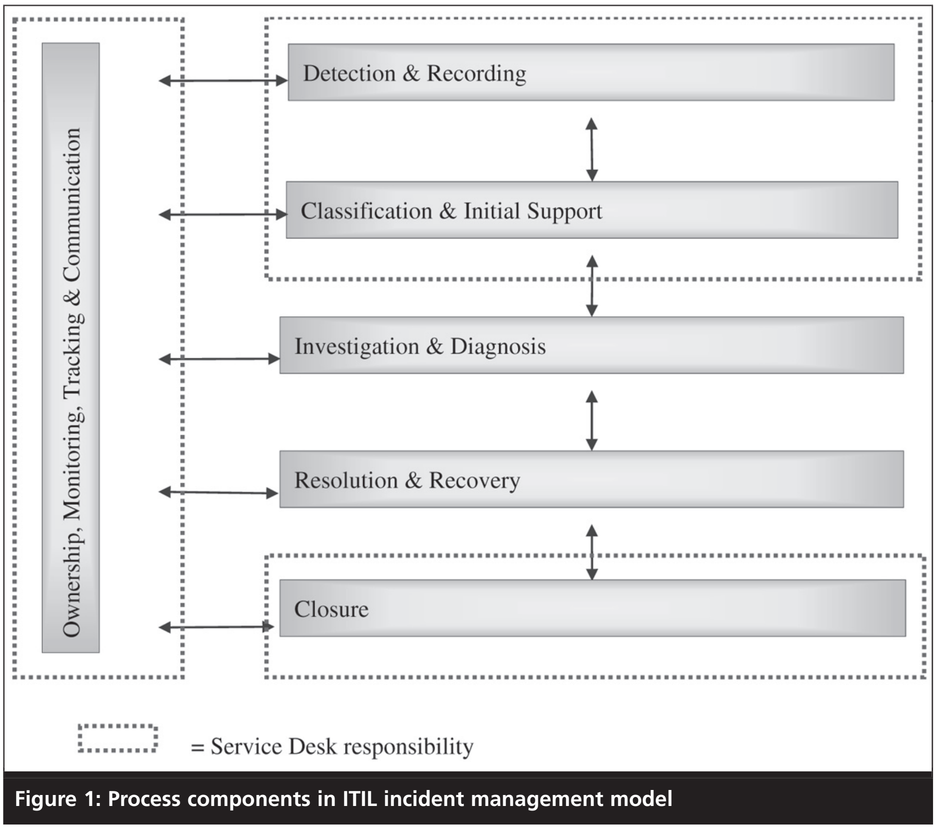
Ownership, Monitoring, Tracking & Communication
Detection & Recording
Classification & Initial Support
Investigation & Diagnosis
Resolution & Recovery
Closure
= Service Desk responsibility

Figure 1: Process components in ITIL incident management model

process. But the comprehensive oversight of other peoples' tasks will be hindered by issues associated with the handling of confidential information. In any case, communication should also be monitored by the company functions assigned to internal and external relations.

In addition to handling closure, the service desk might be the company function best suited for managing preliminary incident response tasks and contacts such as detection and recording. Also known in other literature as the notification or recognition phase, detection and recording seeks to gather the following information:

- Incident type
- Incident source
- What information is available
- Additional details
- Responsibility for the response

Classification and initial support

In theory, the service desk could also handle classification and initial support, provided its staff is effectively trained in such things as responsibility and priority matrices. The ITIL approach does make some suggestions regarding the creation of priority matrices on the basis of impact, urgency, and the type of incident based on the affected target.

Under ITIL, the impact depends on the degree to which business is affected by the incident. Urgency relates to the timeframe imposed for resolving the problem. These factors are also assessed in terms of the resources required to resolve the problem.

These factors may combine in various ways, such as high impact/low urgency. In this example, a server in an important department is hit, but because the entire staff is on vacation the department is not currently operating and the response can wait.

Conversely, in a high urgency/low impact scenario, an employee may not have a modem for her laptop, but needs one quickly because she is about to leave on a trip.

The second example clearly falls within the purview of the service desk, and illustrates how something that really has nothing to do with security, but rather with the provision of a service, is treated as an incident in the ITIL approach. Given the demands of managing a serious incident response action, the service desk might end up finding itself spread a little thin.

ITIL provides an interesting definition of the relationship between the functional and hierarchical aspects of incident response. The functional aspect determines who is responsible for resolving the incident, while the hierarchical aspect defines who must be informed if the incident escalates.

The resolution and recovery process highlights the gap between ITIL's treatment of incident management and that found in other literature. I was directly involved in an ITIL-based incident management project in Eastern Europe. The resolution and recovery task was assigned to a British colleague who, while applying the ITIL directions to the letter, was puzzled by the characteristics of the resolution and recovery phase. The characteristics recommended only marginal interest in the root cause, focus on the mere elimination of symptoms, and the immediate resumption of services.

The role of the incident manager

The incident process manager ultimately takes ownership of the incident management processes, and is responsible for determining what they are, supervising them, and monitoring them. His or her first task is to determine the process itself and to develop it where necessary. This emphasizes the incident manager's role in the 'lessons learned' phase, which is a classic component of the security incident management process.

'Lessons learned' is an extremely important component, as explicitly stated both in the RFC 2350 and in the ISO 17799 standard. However, with this approach, the improvements process is more strongly related to the incident manager's relationship with the service desk than to his or her general oversight of the various players and functions having a role in the overall incident response process.

In any case, these players and functions fall within the responsibility of the incident manager. Within ITIL, incident managers can review the roles of those who do not report directly to them. This might create internal conflicts that must addressed by figures who are higher up than the incident manager. It is hard to imagine how the incident manager can carry out a direct review of the people responsible for the system or network without at least having obtained authorization. In addition to technical skills, the incident manager must clearly have some political dexterity.

Incident management vs review

ITIL provides well-defined guidelines for incident review processes, which are again owned by the incident manager. The aspects that must be addressed and the priorities regarding timeframes and tasks to be carried out are outlined in a clear schematic process. ITIL provides a series of indications regarding the method of review.

Firstly, the review process should be coordinated between internal and independent third parties to gain an objective understanding of the current situation. The incident manager should be able to coordinate the improvement process directly with these third parties, who should in turn be able to implement the improvements.

The reviews must be carried out on an item-by-item basis to verify that all the tasks specified in the procedure are performed. From a pure security standpoint, this part of the review process is identical to the monitoring activities demanded of and carried out by the service desk relating to an incident.

Planning the review cycle

I am sceptical about ITIL's definition of the service desk's role in handling critical incidents. Based on my experience, I do not see how such a central role can be assigned to the service desk in such delicate situations. In my opinion it can only act as a simple communication interface between the incident management function and the internal users or external customers who initiated the incident response procedure.

The frequently of the review cycle has to be planned ahead of time. ITIL states that the activity must be carried out by the incident manager with the operational support of the service desk. The review must be performed on a daily basis (in the event of priority 1 incidents), a weekly basis (priority 2 or 3), or a monthly basis (everything else). The other players involved could be components of the IT department and, perhaps indirectly, those who are sometimes called key customers. The reviews will obviously produce multi-level reports.

Regarding the purpose of the review, the incident manager must be capable of monitoring and reviewing actions related to ongoing incidents (where we are and where we are going). Two other factors must also be considered that might not be included within the sphere of security in the strict sense: service performance targets and the objectives of each incident management process.

The above-mentioned activities are just a part of the tasks that the incident manager has to manage. But who is this figure, and where do we place them within the company structure? If we look at the issue from the ITIL point of view, it is clear that we might opt to include the incident manager directly in the IT department. But if we look at the thing from a pure security standpoint, this is not always possible, especially in companies where the security functions are off in their own department, separate from the IT function.

Can ITIL really handle security incidents?

Five years ago, if someone had dared use the acronym RFC for something other than Request for Comments, it would have created an uproar. Nowadays, when a diesel motor can compete (and win) at Le Mans, we should not be surprised to see the same sacred acronym rendered as Request for Change. Purist leanings aside, experience in the field suggests that the ITIL approach to incident management is exactly what it purports to be: a support to service provision. But if we look at it strictly from a security standpoint we are forced to deem it inadequate in terms of coherence and effectiveness.

It is nevertheless possible to take components from the ITIL process and use them to improve security incident management. But this is not our main concern. What causes a bit of worry is the wide use that ITIL is (quite rightly) enjoying in the IT world. Treating incidents in a merely tactical way might represent a strategic error, leading us to underestimate the importance and requirements of security and its legal repercussions. We may relegate security breaches to the category of simple puzzles akin to a networked printer that doesn't work and has to be restored to service by whatever technician happens to be available.

About the author

Dario Forte, CISM, CFE, is adjunct professor at Milano University at Crema and founder of DFLabs, an Italian company specializing in incident response and digital forensics.