The Crucial Principle of Need to Have Available

亦有中文简体译本
www.isaca.org/currentissueforums

When confidentiality, integrity and availability (CIA) were established as the main information security attributes in the 1990s, employees around the world were not working from home due to a global pandemic. Even though extensions of the CIA triad have been proposed,[1] they have not been thoroughly investigated because cyberprofessionals have been, and, in some cases, still are, busy applying the first three attributes. Fast-forward to today, a time when ransomware is a very common attack method and enterprises are considering offering a permanent remote work option to employees. Even though the CIA triad will always be at the core of what cyberprofessionals do, there is a need for an audit of information security principles to identify where there is room to evolve.

The presence of employees in physical workplaces laid the foundation for the need-to-know principle, which states that one must only have access to the information their role requires. Now that the majority of the workforce is remote, applying this principle has become challenging because employees do not require access to all data all the time. This is seconded by how modern data leakage[2] and insider threat[3,4] algorithms operate. In the same way that a security guard would be suspicious of an employee trying to enter the building late at night, an employee remotely accessing data that are not required for their current set of tasks at odd times or in bulk would also be cause for concern.

To further restrict access to information for processing data, wherein not all data a user or system has access to are required for them to perform their next set of prescribed tasks, the need-to-have-available principle should be followed.

Defining the Principle of Need to Have Available

The term "need to have available" describes the surrendering of a role or permission that grants one or more users or systems access to data after confirming that access to these data is not required to complete the next set of premeditated tasks.

This is a principle of confidentiality and availability on the basis that only certain types of information are required to complete the next set of tasks, provided that these tasks are known ahead of time. As a result, the type of data required to complete the tasks can also be predetermined, concluding that only a subset of the roles or permissions are required. Once the current set of tasks concludes, the roles and permissions need to be reassessed and the principle reapplied for the next set.

The Principle of Need to Know

Unlike the principle of need to have available, the need-to-know principle assumes data are available

YIANNIS PAVLOSOGLOU | PHD, CISSP

Is a cybersecurity executive with 20 years of experience. He is the founder and chief executive officer (CEO) of KIBERNA, an enterprise specializing in data-driven information security, data protection and operational resilience services. He has successfully held the position of chief information security officer (CISO) in two countries, with pioneering work in process catalogs and service definitions to protect organizations. In 2019, he was elected to the board of directors of (ISC)2, overseeing the CEO, where he has been further voted (ISC)2 Secretary for the calendar years 2021 and 2022.

independent of the task at hand. This becomes more granular with the principle of need to have available, which focuses on what data are required for performing specific tasks at any given time (**figure 1**).

The granularity of the principle of need to have available adds in a time factor to data access that requires planning ahead. Roles and permissions become more dynamic. They are assigned and reevaluated based not only on the role and responsibilities of a user or the permissions of a system, but also on the next set of tasks being planned. Assuming most organizations already apply the principle of need to know,[5] practitioners should assess how the planning and application of the principle of need to have available can improve the enterprise's security. For this reason, it is worth examining cyberincidents from 2021 and how their impact would be different had the principle of need to have available been applied.

JOIN THE DISCUSSION

- Learn more about, discuss and collaborate on information and cybersecurity management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Analysis of Significant Cyberincidents in 2021

A data set from the Center for Strategic and International Studies (CSIS) provides a timeline of records for significant cyberincidents since 2006.[6] CSIS focuses mainly on cyberattacks on government agencies, defense and high-tech organizations, and economic crimes with losses of more than US$1 million.

In this assessment of incidents, it is assumed that the principle of need to have available would have been applied correctly, therefore, the victims or systems of each attack would have surrendered any roles or permissions not required to perform their next set of tasks before the incident took place. This would have resulted in each victim or compromised system only having access to a smaller data set relative to what they could request or be granted access.

Analysis focused on a two-stage review of each of the first 101 significant cyberincidents reported by CSIS in 2021. The first stage involved research of each significant incident reported to understand if there is enough information about the incident available in the public domain to form an opinion with regard to the principle. The second stage focused on significant cyberincidents in which enough information was available to opine. Based on the data, an opinion was formed on whether if the principle of need to have available had been applied correctly ahead of time, it would have limited the impact of the attack (**figure 2**).

Results showed that of the 101 incidents reviewed, approximately 15 percent did not provide enough information on which to opine. Twenty-three percent of incidents would not have had any difference in impact had the principle of need to have available been applied before the time of attack. Sixty-two percent of incidents reported in 2021 would have had less of an impact if the principle of need to have available had been applied accurately and proactively.

Use of the principle of need to have available in some of these cases would have led to smaller data sets for ransomware to encrypt, cryptocurrencies stored requiring further access rights and virtual private network (VPN) vulnerabilities yielding limited data access (as further roles would be required). However, it did not make a difference in cases where cybercampaigns were longer than three to four years, wherein it can be assumed that a victim used all their access roles during that time. Still, even for elongated campaigns, despite not being able to limit the impact of attack, the principle of need to have available would have made attackers work harder for the data. Attackers would be required to closely monitor the permissions granted to victims and extract additional data based on those permissions over time. These

FIGURE 1

The Principle of Need to Know Compared to the Principle of Need to Have Available

Principle of Need to Know	Principle of Need to Have Available
A user shall only have access to data their job function requires.	A user shall only have access to data their job function requires for performing specific tasks.
A user is assigned access to data based on their role and responsibilities.	A user is assigned access to data for performing specific tasks.
Permissions are granted and revoked based on what the job function requires.	Permissions are granted and revoked based on the prescribed tasks.
Permissions are reassessed based on the responsibilities of the user.	Permissions are reassessed based on the completion of a set of tasks by a user.

examples illustrate that there is value in limiting access to data based on the tasks to be performed.

Principle Critique and Disadvantages

Despite the advantages of the principle of need to have available, not all tasks in a modern work environment are linear or can be sequenced in time. The principle of need to have available requires steps to be premeditated with regard to the information processed or produced. Consider a chief executive officer (CEO) of an enterprise who wants to look at strategy documents from 10 years ago. Dedicating a role for that task alone would not be practical. The principle cannot be applied to all roles and ranks within a modern workforce. A solution to this could be granting access to a larger data set to employees physically in the building.

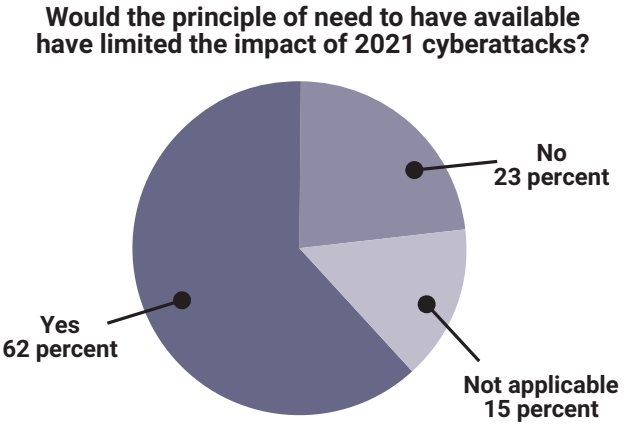
A second critique of this principle is that it can stifle innovation. If a user realizes they can combine the data they are using with another data set to be more effective, they must pause to request an additional role to do so. Human brains are not wired to operate in that way; therefore, the principle needs to be applied with caution and only to protect specific sets of data for good reason. To promote innovation, during phases of brainstorming, data pools could be generated ahead of time and used for limited time periods.

A third critique is that the user in question would need to know the tasks they are performing well enough to be able to describe what data are required to perform them. This, compounded by the fact that if not carefully thought out, surrendering a role can put the completion of the tasks at risk, would require a truly skilled workforce to be a prerequisite to successful implementation of the principle. It is essential to ensure that employees understand the data they use before applying the principle of need to have available.

Unlike other information security principles, the principle of need to have available poses an inherent risk in having to categorize (and perhaps get wrong) what data are needed and who within the organization utilizes those data, compared to the reward of limiting the effects of a significant cyberincident when it occurs. Still, this is something that most organizations have been forced to do almost by osmosis during the phases of the COVID-19 pandemic. Thus, it would make sense to formalize the principle of need to have available for the future workforce.

FIGURE 2

Analysis of 101 Significant Cyberincidents From 2021



Real-World Examples

There are several resource planning systems wherein granular permissions are granted based on policy, only for specific duration and often with prerequisites for integrity and trust. For example, enterprise resource planning (ERP) systems for streamlining business processes and reducing complexity not only have security features to guarantee confidentiality,[7] but they also allow for policies to be created for specific purposes such as:[8]

- **The need to share, wherein organizations must share data to carry out their operations**—This is a more generic instance of the principle of need to have available, wherein access to data is granted based on how they will be further shared. Under the need to share, the task for the access role is known and, therefore, the principle of need to have available also applies. The need to share would fully align with the need to have available, such as when, for example, an administrator of an ERP system revokes access from users when there is no upcoming task to share. If the people responsible for sharing the information further do not have a task to perform such an activity in their next set of activities, it would make sense to review the subjects and remove their access until further required.
- **Trust policies, wherein data are only shared between specific organizations**—An example of how the principle of need to have available is applied at an organization on the peer-to-peer level is the implementation of trust policies. When two organizations need access to data between them, a trust policy is typically implemented for a specific time duration depending on a

contractual agreement. Instead of dedicating time to investigating the more granular tasks of employees, access to data is granted for a duration that is stipulated in the organizations' contracts.

- **Integrity policies, wherein only specific individuals are authorized to modify certain data**—The principle of need to have available can be applied more specifically after determining who can modify the data to guarantee quality and accuracy. Often in cases where users no longer have a need to modify data, access rights are revoked until the need arises again.

With the ability to create policies for specified purposes, various commercial ERP products, including SAP, Oracle and Microsoft, provide functionality for use cases that use to some degree the principle of need to have available. Beyond ERP, parties responsible for designing policies within their organizations can also consider the principle of need to have available, but it is typically not for a strict time-based, task-driven duration. Information security officers, auditors and risk managers often are the roles that point out that if an access permission is not required for long periods of time, it can be revoked and granted again closer to when the prescribed activity is set to occur. This discussion is more common after a malware or ransomware attack.

Minimizing the Impact of Ransomware

The impact of ransomware can be further minimized if the principle of need to have available is applied proactively and with the correct level of rigor. For example, consider that an employee falls victim to a stage 1 ransomware payload, with stage 2 beginning to encrypt files within their filesystem. Had their access been restricted to only the data required for them to perform their next set of tasks, the impact of the ransomware on their files would be smaller in proportion. Furthermore, had access rights been restricted, there would be a set of permissions limiting where the payload could access and search for data to encrypt. Thus, the ransomware's impact would be further reduced because there would be fewer data available to encrypt and the permissions would restrict where the ransom payload could deploy. It could also be argued that given the majority of stage 1 ransomware is transmitted via email, if accessing links and files via email is not part of the prescribed set of tasks at a given time, and, provided that the need to have available is applied correctly, then the employee is further protected from ransomware in that moment.

Conclusion

The physical presence of employees in the office provided the starting point upon which to establish information security principles. In the face of the global COVID-19 pandemic, there has been a need to revisit what data are available and to whom. The principle of need to have available offers a method to limit the impact of significant cyberincidents and, therefore, assists in the management of a remote workforce. For the principle to be effective, one must premeditate which roles or permissions are required based on the data needed to complete a set of tasks. This can lead to risk in revoking remaining employee roles and finding out they are required after revocation. Despite the overhead of needing to think about what roles should be kept while performing tasks, this principle offers an undisputed way to limit the impact of incidents as they happen.

Endnotes

1 Parker, D. B.; *Fighting Computer Crime: A New Framework for Protecting Information*, John Wiley and Sons, USA, 1998
2 Guevara, C.; M. Santos; V. Lopez; "Data Leakage Detection Algorithm Based on Task Sequences and Probabilities," *Knowledge-Based Systems*, vol. 120, 2017
3 Ye, X.; M. M. Han; "An Improved Feature Extraction Algorithm for Insider Threat Using Hidden Markov Model on User Behavior Detection," *Information and Computer Security*, 2020
4 Lv, Q.; Y. Wang; L. Wang; D. Wang; "Towards a User and Role-Based Behavior Analysis Method for Insider Threat Detection," 2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC), Institute of Electrical and Electronics Engineers (IEEE), China, August 2018
5 International Organization for Standardization (ISO) standard ISO 27002:2013 *Code of Practice for Information Security Controls* references the need to know as a principle directing access control policy definition.
6 Center for Strategic and International Studies (CSIS), "Significant Cyber Incidents," *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents*
7 Thuraisingham, B.; Database and Applications Security, *Integrating Information Security and Data Management*, Auerbach Publications, USA, 2005
8 She, W.; B. Thuraisingham; "Security for Enterprise Resource Planning Systems," *Information Systems Security*, 2007