
Assessing and understanding insider threats to data security

BY FRANK RUELAS

Here's an interesting exercise to try. Ask someone in your organization's IT or Data Management department to identify the safeguards that are in place to help protect the organization's data. Very often the response you receive will consist of an impressive listing of safeguards that protect the organization's data from external threats. What you may find missing in the response is the identification of safeguards to protect the organization's data from threats that may originate from within the organization, commonly referred to as insider threats. When one considers the significant risks associated with insider threats that may compromise the security of data, it is important to realize that insider threats must also be adequately assessed to minimize or mitigate them to an acceptable level.



Basic concepts

To understand why insider threats may be overlooked or minimally assessed, we need to first understand some basic concepts related to data security, threats, and how threats are identified and managed.

Data security essentially deals with three important objectives aimed at safeguarding or protecting data—confidentiality, integrity, and availability.¹ Although these objectives may be associated with very technical or detailed definitions and attributes, let's look at them from a practical and non-technical perspective, along with examples that help illustrate the concepts associated with each of these objectives.

Confidentiality refers to the protection of data from intentional or unintentional access by an unauthorized individual. Simply put, this means making sure that data is accessible by those who have a need to access it. At the same time, these same processes prevent access to data by those who do not have a need to access it. This is frequently referred to as role-based access, where a person's role is used to determine what data he/she may access. For example, if a person has a role where accessing patient data is an integral part of the job duties or function, this person may have access to an organization's Electronic Health Record (EHR), while those without such a job-related duty or function do not.

Integrity refers to ensuring that data is not altered in an unauthorized manner. An example of this is where computer users are able to access a file in a shared location within a network in a read-only capacity. This allows computer users to view the information within the shared location, but also prevents users from changing the file's contents.

Availability is that data security objective aimed at protecting data against intentional or unintentional deletion. Availability also is aimed at ensuring that users are able to access data when it is needed. An example of this is data backup procedures that allow for the restoration of data if the data is deleted by a user or replaced by another file with the same name, thus making the original data unavailable. This objective also includes efforts to maintain the computer system's operability. Downtime, either as a result of failure of computer equipment (hardware) or by failure of its operating system (software) is another point of emphasis within the availability objective.

So with these three objectives in mind, those responsible for implementing safeguards to protect and promote data security conduct a risk assessment to identify those circumstances or events (referred to as threats) which may compromise any of these

objectives, either individually or in combination.² By analyzing the results of a risk assessment, organizations can then decide what types of safeguards may be used to offset the identified threats. However, threats originating from outside of the organization are often the prime points of focus of a risk assessment, and insider threats may get overlooked or minimally assessed. When this occurs, data security may be significantly at risk.


Insider threats

The significance of insider threats to data security cannot be understated and should not be underestimated. Research shows that the greatest risk to data security comes from insider threats.³ This may sound alarming, given that we would expect insiders (e.g., employees, contractors, and others with access to the data) to conduct themselves in the best interests of the organization, including safeguarding its data. This same research also points out something that people may find quite surprising as well as encouraging.

Although there are instances when data security is breached by insiders with malicious intent, this group does not pose the most commonly encountered threat to data security. The group of insiders that does pose the most significant threat to data security consists of insiders who are committing unintentional acts that negatively impact data security. What is encouraging is that there are root causes that, if addressed, can significantly decrease the threats associated with this group of insiders.

Raising awareness on data security and relating it to a user's access to data may be one of the most effective ways to promote work practices that safeguard, rather than threaten, data security. By taking this approach, and combining it with a hands-on training strategy, users are placed in a position where their increased awareness is associated with their job-related functions, which then constantly

reinforces work habits that safeguard data security.⁴ Too often users are left to their own devices to figure out what they can and can't do in terms of accessing or using data. By *showing* users, rather than leaving them to figure things out for themselves, extemporaneous activity (which may include activity that users are unaware may jeopardize data security) may be reduced or eliminated.



TOO OFTEN USERS ARE LEFT TO THEIR OWN DEVICES TO FIGURE OUT WHAT THEY CAN AND CAN'T DO IN TERMS OF ACCESSING OR USING DATA.

It is not uncommon for problems to occur right from the start when a new employee comes to his/her department. In the rush that precedes getting someone set up on the computer system, the new employee does not have credentials to access data. In turn, this new employee may be provided a generic user login or even provided the login and password for someone assigned to the department who may be out on leave until the new employee's log in credentials and access is defined. Now you have a situation where someone's role-based access may not be in alignment with his/her needs and allows this new employee to access data he/she has no need to view.

In addition, there may be options to monitor the data use and data access patterns of employees to determine if they are exhibiting behavior that may contribute to an unintentional risk to data security. Are employees going to certain locations on the network in attempts to locate needed files and while doing so, venturing into folders that they have no reason to view? Are employees monitored to determine if there may be activity that may warrant additional attention? For example, is

there a department where the employees are calling the IT or Data Management department to reset passwords much more frequently than other departments? If so, what insider activity is contributing to this type of activity?

All of these questions can be asked without users feeling they are being interrogated or investigated for any potential wrongdoing. Falling back on data that justifies the need to ask these questions is a very nice and neat way to stay objective while helping to keep the emotions of anyone involved in check. When doing these types of inquiries, I have found people to be much more willing to share their comments and ideas when I can show them the data that prompted me to ask. This puts people at ease and also makes them feel that their input is necessary to help find much needed answers. In short, it helps prevent an adversarial approach while fostering collaboration, including the identification of opportunities to make both short-term and long-term improvements.

Disgruntled employees

I would be shortchanging the information about internal threats if I didn't bring up what is, hopefully, a very small group of individuals within your workforce. I am referring to are those who may be described as "disgruntled" employees.

The mere idea that disgruntled employees, particularly those who may believe they are about to be fired, would access and take data is troubling enough.⁵ References to disgruntled employees and their impact on data security have even been mentioned in Presidential speeches.⁶ Combine this with the likelihood that some disgruntled employees may know how to operate within a mode that specifically attempts to avoid detection of their data use and data access, and you have the proverbial recipe for disaster for compromising an organization's data security.



Additionally, the threat associated with a disgruntled employee doesn't necessarily mean that the threat goes away once a disgruntled employee is let go. A disgruntled employee may also be able to exploit known gaps in data security. For example, if federal or state rules and regulations require that an organization take certain precautions to protect data security, and the newly released, disgruntled employee is aware that the organization has not fulfilled these requirements, what is there to prevent the disgruntled employee from reporting this fact to the federal or state entity responsible for enforcement of the rule or regulation which has not been satisfied? Although there is certainly something to be said about organizations that do not fulfill their requirements to be held accountable, my point is that for this to be addressed due to the actions of a disgruntled employee is likely not the best way for everyone involved to deal with unfulfilled requirements.

Conclusion

So, although insiders can pose a significant threat, organizations can do well to position themselves to effectively counteract the insider threat through

detection, monitoring, effective training, and the use of effective countermeasures. By maintaining a watchful eye on insiders, an organization is better able to minimize the risks associated with insider threats and thereby do a better job in promoting and strengthening its efforts in maintaining data security. ■

Frank Ruelas (frank@hipacollege.com) is a Compliance Officer with Gila River Health Care in Sacaton, AZ.

[in bit.ly/in-frank-ruelas](https://www.linkedin.com/in/frank-ruelas) [@Frank_Ruelas](https://twitter.com/Frank_Ruelas)

ENDNOTES

- 1 Gary Stoneburner: "Underlying Technical Models for Information Technology Security." National Institute of Standards Technology (NIST), Special Publication 800-33, page 2. December 2001. Available at: <http://1.usa.gov/1EHhBjF>
- 2 Joint Task Force Transformation Initiative Interagency Working Group: "Guide for Conducting Risk Assessments." National Institute of Standards Technology (NIST), Special Publication 800-30, page 30. September 2012. Available at <http://1.usa.gov/1uha4oy>
- 3 Heidi Shey: "Understand The State Of Data Security And Privacy: 2013 To 2014." Forrester Research Inc., page 2. Available at <http://bit.ly/1GTsKjw>
- 4 Fred Beisse: *A Guide to Computer User Support for Help Desk and Support Specialists*. Course Technology Cengage Learning; 5th edition, page 500. March 26, 2012.
- 5 Jeff Goldman: "Disgruntled Employees Present Significant Data Breach Threat." *eSecurity Planet*, July 16, 2013. Available at: <http://bit.ly/1tNIIYE>
- 6 Barack Obama, "Remarks by the President On Security Our Nation's Cyber Infrastructure," May 29, 2009. Available at: <http://1.usa.gov/1tNlnj>