Insider Threats

An insider is a trusted individual whose goal is to steal our confidential information or cause harm to our organization. We discuss how you can identify insiders in our organization and how to help protect against them.
Our organization’s most important asset is our data. It is what drives our mission. Because of this, numerous adversaries and competitors target it. The most effective way for someone to compromise our organization or our data is through an insider. An insider is a trusted individual who has ulterior motives. Their goal is to steal our information or cause harm to our organization. An insider can be anyone who works in our organization, including employees and contractors.

What makes an insider so dangerous is that they have trusted access to our information, assets and resources. Compromising our highly confidential information can be as simple as copying critical data to a portable drive or emailing it out of the organization. Anyone in our organization could be a potential insider. If you see the following behavior, you should report it to your supervisor or our security team immediately:

1. Someone asking for access to information they do not need in order to perform their job.

2. Copying large amounts of information at a copier, carrying a large number of documents out of the organization or transferring extremely large or unusual files.

3. Working strange hours and coming into the office when no one else is around.

4. Someone trying to log into others’ accounts or asking for access to a secure area, such as a data center.

5. Someone you work with suddenly changes his or her behavior. For example, they used to be very friendly, show up to work on time and be well-dressed, but now they avoid any interaction, consistently show up to work late and appear to be very disorganized.

In order to minimize the impact of an insider threat, please take the following steps to help protect yourself and our organization:

1. For any data you are responsible for, only give people access that is required for their job function. Even if someone has the required clearances, ask yourself if their job requires it. If not, then do not provide the information. If you are not sure, ask a supervisor. In addition, this access should be reviewed on a regular basis. Over time, people who need access to certain data may no longer need it, and their clearance should be removed.
2. Do not copy work-related information to personal drives or take sensitive information home with you unless you have prior authorization. Also, be sure you do not copy any work-related information to public or cloud-based services. Do not forward work data to your personal email account or smartphone or share it with cloud services, such as Dropbox.

3. Always lock your computer and desk when you are gone for long periods of time. This ensures unauthorized individuals cannot access any sensitive information you may have on your computer or in your desk.

4. Never share your password with anyone, including your supervisor, and never give anyone access to your account. By giving someone access to either your account or your password, not only do you jeopardize our organization, but you also become responsible for all of that person’s actions.

The insider threat is a real and ever-growing problem. You never know who could be causing harm to our organization, so always be on the lookout for suspicious behavior. If you ever have any concerns or questions, please contact the security team.

Motivations

One of the reasons the insider threat can be so difficult to detect is they often have very different motivations for causing harm. Some people might be unhappy with our organization for reasons such as not getting the raise they felt they deserved or feeling they are not being properly recognized for their work. This causes them to strike back in retaliation. Other people may be motivated by political or ideological reasons and expose information because of their beliefs. Still others may be motivated by greed and steal our information to sell to the highest bidder.

This is why detecting an insider threat can be so difficult and why we need your help. There are often different indicators based on different motivations. If you see something that makes you concerned, please report it so we can have people that specialize in insider threats look into it.