CYBER SECURITY newsletter

INSIDER THREATS

Problem

The most important thing to our organization is our data. Data drives our mission and is targeted by numerous adversaries or competitors. The easiest 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 they have trusted access to our information, assets and resources. Compromising our highly confidential data can be as simple as copying critical data to a portable drive or just emailing it out of the organization. Anyone in our organization could be a potential insider, as such you should always be on the lookout for suspicious behavior.

If you see the following behavior, you should report it immediately to your supervisor or our security team:

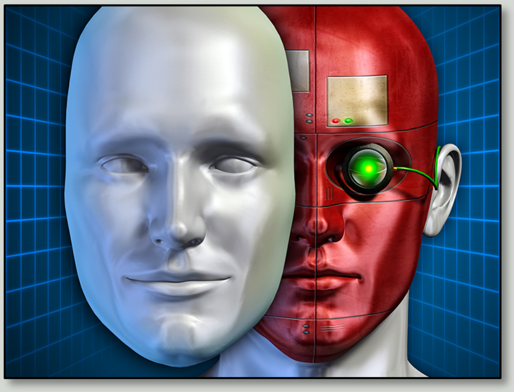
1. Someone asking for access to information they do not need access to in order to perform their job.

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 someone else's accounts or asking someone to give them access to a secure area such as a data center.

5. Sending a large number of emails out of the company with attachments or carrying portable USB drives out of the organization.



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.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

Robert Hanssen

One of the most famous insiders of all time was an individual named Robert Hanssen. Mr. Hanssen joined the FBI in January 1976, where he worked for over 25 years as a trusted FBI agent. During that time one of his primary roles was that of Soviet/Russian counter-intelligence. His job at the FBI was to identify trusted Americans that were really working for the Soviet Union, people spying on their own country. The problem was, during a large part of this time Robert Hansen was one of the top Soviet spies. Only three years after joining the FBI, he had reached out to the Soviet GRU, asking if he could spy for them.

Since he was so trusted by the FBI he was able to provide to the Soviet Union information critical to the United States, including latest tools and technology used by American intelligence. He also identified a variety of Russian people that were actually working for the American government, resulting in the deaths of numerous people. Many consider this single individual the greatest intelligence disaster in America's history.

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

1. For any data that 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 require it. If not, then do not provide the information, or if you are not sure ask a supervisor. In addition, this access should be reviewed on a regular basis. Overtime people that need access to certain data may no longer need it and 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. In addition, be sure you do not copy any work related information to public or cloud based services. Examples include do not forward work data to to your personal email account, sharing data with cloud services such as Dropbox, or copy data to your smartphone

3. Always lock your computer and your desk when you are going to be away for a long period of time. This ensures that unauthorized individuals cannot access any sensitive information you may have in your desk or access your computer.

4. Never give anyone access to your account or share your password with anyone, including a supervisor. By giving someone access to either your account or your password, not only do you jeopardize our organization by giving unauthorized access, but you will be responsible for all of their 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.