THE NATIONAL CYBERSECURITY SOCIETY

Insider Threat

What is Insider Threat and how will it affect my business?

An insider threat is defined as **a security threat that originates from within the organization** being attacked or targeted. Insiders are often employees or officers of the organization or enterprise. An insider threat does not have to be a present employee or stakeholder – it can be a former employee, volunteer, board member, or anyone who at one time had access to your organization's proprietary or confidential information. Additionally insider threats may be contractors, business associates, or other third-party entities who have knowledge or your organization's security practices, confidential information, or who have access to your organization's protected networks or databases.

FACT 1: MOTIVATION

Insider threats occur for a variety of reasons. In some cases, individuals use their access to retrieve sensitive information for personal or financial gain or to cause harm. The damage that occurs could affect the business's reputation, their intellectual property or financial position. In some cases, insiders align themselves with third parties, such as other organizations or hacking groups, and operate on their behalf to gain access from within the network of trust and share proprietary or sensitive information. One of the most famous insider threat actors was Edward Snowden.

Insider threats can be intentional or unintentional such as when an employee inadvertently shares protected company information because they have not been trained in procedures to protect sensitive data.

FACT 2: PROTECTION MEASURES

1. **Enforce strict data policies.** Securing your company's intellectual property should be a priority. The moment someone is hired, policies that regulate how data is transferred and handled should be made clear.

Did you know?

- √ Insider threat can be both intentional and unintentional
- √ One of the most famous insider threat actors was Edward Snowden who stole NSA classified information
- √ It is estimated that Snowden released has made it easier for terrorists to evade detection
- √ It is important to monitor employee activities and have policies in place to protect sensitive information

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Insider Threat continued....

2. **Immediately change the password access to computers after an employee leaves the organization.** This prevents them from accessing any sensitive data after their termination. Make sure you do the same for any shared company accounts the employee might have access to.

3. **Make sure vendors and third parties know about the employee's termination** so that they can also de-authorize the account and prevent access to any sensitive data in the future.

4. **Ensure departing employees do not have company data on personal devices.** Before a high-risk employee leaves the organization, check whether they have company data on their personal computers, mobile phones, tablets, etc.

5. **Regularly review employee access controls.** If there's no need for an employee to access a particular account, revoke their permission. Additionally, consider restricting the use of remote login applications or cloud storage applications (e.g., Dropbox, Google Drive) on corporate accounts.

6. **Educate employees on password best practices.** This includes creating and maintaining strong passwords. Avoid using shared logins and passwords for desktops, servers, or networks. As tedious as it might be, every password should be long and varied with numbers and text. Make it mandatory for employees to change their passwords on a quarterly basis.

7. **Take advantage of using monitoring technology.** If an employee knows that they'll be monitored, they will be less likely to copy files they should not have access to, email out exactly what happened and who is responsible for security violations.

FACT 3: INCIDENT RECOVERY

1. **Incident Investigation.** If you suspect that an insider has either stolen or compromised sensitive data or done some type of reputational harm, it's important to conduct a confidential investigation documenting what happened, how you were notified, what was stolen, compromised or damaged. Depending on what happened, you may need to involve legal counsel.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Insider Threat continued....

2. **Containment.** Containment involves restricting the spread of the event and the activities recommended depend on the type of incident. If an employee clicked on a phishing email by accident, then the containment can be fairly easily remediated. (Contact your IT security team to conduct an analysis of the computer and infrastructure to determine if malware or another type of intrusion is underway). Disconnecting the affected device and clean up would be warranted.

   If the event involves damage to either your data, systems or applications or involves theft, it will require restricting access to your facility, IT systems or data. Containment in this instance will involve removing the employee's rights to your company assets as well as restricting remote login.

   If the event involves negative commentary on corporate social media sites, immediately contact the provider and shut down the account or use it to report to your followers what has occurred. If the employee is using their own account to spread malicious or damaging information about your business, contact the provider. The SBA has a great site that provides a number of recommendations with respect to social media cyber vandalism. See link below:

   https://www.sba.gov/managing-business/cybersecurity/social-media-cyber-vandalism-toolkit

3. **Recovery/Removal.** Once the investigation is complete, the next set of activities involve removal of the employee, and recovery from the event. However, if the event involved unintentional damage - such as a phishing event - the actions may include: training the employee as well as the entire staff; resetting passwords company-wide; and revalidating who has what access to company assets.

   If the event was intentional, then your HR lead and legal counsel will advise you on next steps to removal of the employee. If the investigation is not complete, or there might be a legal proceeding, your counsel may advise you to keep the employee's computer and account accesses open until the investigation and legal proceeding is complete.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.