6 Things You Need to Know About Insider Threats

(and Who to Watch Out For)

In any successful organization or business, there will always be the threat of those who wish to steal, cause harm or destruction. Every day, hackers attempt to exploit vulnerabilities in the protective walls companies raise using rigorous cybersecurity measures. But if that threat is coming from inside the organization, these walls become useless.

1 What is an Insider Threat?

Interior breaches of security, called insider threats, are highly dangerous to both the infrastructure of an organization and the sensitive information it holds. Insider threats come from an entity familiar with the inner workings of an organization- whether a current or former employee, contractor, or other business partner.

2 Criteria to be considered an Insider Threat

These perpetrators usually meet the following criteria to be considered insider threats:

- they have had or currently possess authorized access to an organization's network
- system or data and who, intentionally or not
- causes harm or increases the probability of future harm to the confidentiality or integrity of the organization's information systems.

According to the 2017 U.S. State of Cybersecurity Crime Survey, insider attacks account for 20% of all electronic crime events. In this same survey, 30% of the affected organizations reported that insider attacks were more damaging than outsider threats.

In order to better understand how inside threats work, let's first break them down into their respective categories: ***unintentional and malicious.***

Insider attacks account for **20%** of all electronic crime events.

ID AGENT A Kaseya COMPANY

Sales@IDAgent.com | 888-ID AGENT

3 Unintentional Insider Threat defined

Within unintentional insider threats there are four classes:

1. accidental disclosure 2. phishing scams 3. physical record 4. portable equipment

Accidental disclosure occurs when sensitive information is mishandled, being either posted to a public website or delivered to the wrong fax or email address. Phishing scams, the most common form of email scams, occurs when an entity is infected with malware or hacked using a fraudulent email link or attachment. Both physical records and portable equipment deal with the mishandling of confidential physical materials, which are documents and portable devices such as USBs and CD-ROMs, respectively.

4 Target: A lesson learned the hard way

Mistakes happen to all of us. However, it's crucial to be vigilant when performing business, whether you are directly involved in an organization or a third party. Unfortunately for the retail chain Target, this was a lesson learned the hard way.

In 2013, Target experienced a data breach unlike any other. In order for hackers to obtain sensitive information from the company, they exploited one of Target's third-party vendors who was using sensitive credentials. The hackers infiltrated the supplier and thus gained access to Target's private servers- including their point of sales machines. From this unintentional insider threat, target warned over 110 million credit and debit card users that their information may be compromised. That's over 11 gigabytes of data pilfered by these hackers.

This is a harsh reminder that not only should organizations take care in understanding the behavior of internal employees but also contractors and third-party vendors who may also be provided access to an organization's systems and data...even if they aren't directly tied to sensitive systems.

5 Malicious Insider Threat defined

Though the Target incident involved inadvertent credential exposure, most insider threats are unfortunately on purpose. These intentional attacks, called malicious insider threats, come in three basic forms.

The first of these malicious insider attacks is Information Technology (IT) sabotage, which is an insider's use of IT to direct specific harm at an organization or an individual. As the name would suggest, this form of attack is most commonly prevalent in the IT industry.

Similarly, the second of the attacks involve **using IT to steal IP from the organization**, called Intellectual Property (IP) theft. This type of attack often utilizes industrial espionage for outsiders to steal information from the targeted company.
The third and most common form of malicious attack is **fraud**. Fraud is when an insider uses IT for the unauthorized modification, addition, or deletion of an organization's data for personal gain. This is the most damaging class of insider attack to several industries, including banking and finance, healthcare, and government, both federal and state.

Fraud is the most damaging class of insider attack to several industries, including banking and finance, healthcare, and government.

6 Insider Threats are a serious crime

Every day, government agencies monitor and report those who commit malicious insider threats. Not only do commercial companies fall prey to them, but these same government agencies do as well. Over the past few decades, several cases have been brought to light in which supposed trusted government employees sold or otherwise stole information from government agencies to foreign entities. Insider threats are a serious crime and are punishable by over a decade in prison and several thousand-dollar fines.

By educating employees on these and other types of threats, companies can better strengthen their defense against exposure to harm and loss. A robust suite of tools including employee security awareness training and anti-phishing exercises, dark web monitoring, data leak prevention, and multifactor authentication, to name a few – can help organizations protect their business from insider threats and risk from attackers outside their networks.

ID Agent was the first company in the Channel to market Dark Web Monitoring directly to MSPs. The company's Dark Web ID™ provides real-time monitoring and alerting for exposed credentials associated with a company's domain, so that action can be taken before a breach occurs. The company also rolled out a complementary Security Awareness Training and Anti-Phishing platform called BullPhish ID™, so the MSP can help its customers to make their employees the frontline of defense, rather than the weakest link in security. For more educational resources and to learn more, visit www.idagent.com.