Insider Threat Attack steps

Project: Corporate Insider Threat Detection (CITD)
http://www.cs.ox.ac.uk/projects/CITD/index.html
Authors: I. Agrafiotis, J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese

This document outlines an attempt at an exhaustive listing of steps seen in insider threat attacks. We build on research in our previous work in Understanding Insider Threat: A Framework for Characterising Attacks[1], where we present Attacks and Attack Steps. While Attacks aim to be generic, *Attack Steps* define, in detail, the specific activities undertaken to conduct an attack. As such, an Attack can be composed of several chained Steps. An excerpt from the framework of insider attacks diagram is shown in Figure 1.

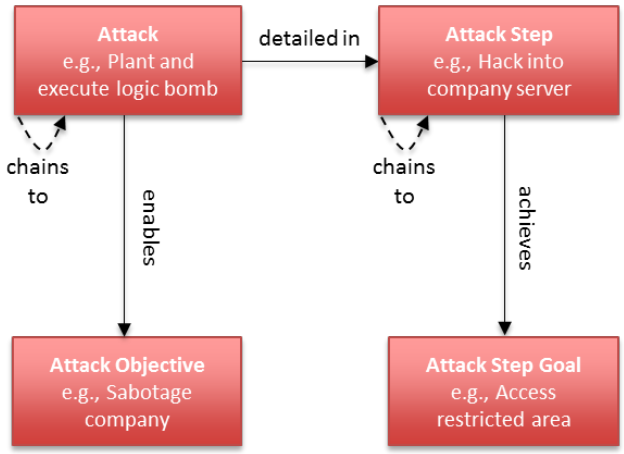

Figure 1: The relationship between Attacks, Attack Objectives, Attack Steps and Attack Step Goals

Below, we enumerate the attack steps.

AS	Attack step (description)
1	Accessing (co-)worker's desks or workstations
2	Accessing restricted company locations (buildings, offices, desks) to which the actor has authorisation – Abnormal / unusual access (e.g., entering outside of working hours)
3	Accessing restricted company locations (buildings, offices, desks) to which the actor has authorisation – Normal access
4	Accessing restricted company locations (buildings, offices, desks) to which the actor has NO authorisation
5	Accessing sensitive company files or information (i.e., proprietary data, processes, system specs, code, software, client data / files) to which the actor has authorisation – Abnormal / unusual access, e.g., large amounts of data accessed
6	Accessing sensitive company files or information (i.e., proprietary data, processes, system specs, code, software, client data / files) to which the actor has authorisation – Normal access

[1] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *Workshop on Research for Insider Threat (WRIT) held as part of the IEEE Computer Society Security and Privacy Workshops (SPW14), in conjunction with the IEEE Symposium on Security and Privacy (SP).* IEEE, 2014. [Online]. Available: http://www.cs.ox.ac.uk/files/6576/writ2014_nurse_et_al.PDF

7	Accessing sensitive company files or information (i.e., proprietary data, processes, system specs, code, software, client data / files) to which the actor has NO authorisation
8	Building a close relationship with (co-)workers with access to company files / systems
9	Building a close relationship with the company's clients / customers
10	Coercing (co)worker to provide their access credentials (electronic or physical) to company files / systems
11	Coercing (co)workers with access to company files / systems to (un-)knowingly assist in an attack
12	Coercing the company's clients / customers to share their access credentials
13	Coercing the company's clients to (un-)knowingly assist in an attack
14	Connecting portable devices (USB drives, CDs, laptops, tablets, portable hard drives) to company workstations, servers or networks
15	Creating backdoors (e.g., secret accounts or system functionality) in company systems to facilitate later attacks
16	Creating fake access credentials (e.g., to allow unauthorised access or transactions)
17	Creating fake documentation – General
18	Creating fake logs (e.g., to cover the attack's tracks)
19	Creating fake receipts (e.g., for demonstrating expenses, actions or sales)
20	Cyber theft (e.g., using key-loggers or sniffing tools) of (co)worker's access credentials
21	Deleting / editing system log files (particularly to cover the attack's tracks)
22	Deleting company files or information (proprietary data, system specs, code, software, client data / files)
23	Denying legitimate / authorised access to company files or information (proprietary data, system specs, code, software, client data / files),
24	Denying legitimate / authorised access to company systems or property (e.g., holding system credentials, software code, client data; typically for ransom)
25	Denying legitimate / authorised access to the company's network (e.g., using DoS attack or programmed code)
26	Disrupting the company's clients from accessing or using files or services (typically a step leading up to or covering for an attack)
27	Downloading sensitive company files or information (proprietary data, system specs, code, software, client data / files) to portable devices (USB drives, CDs, laptops, tablets, portable hard drives)
28	Emailing sensitive company files or information (proprietary data, processes, system specs, code, software, client data / files) to other unauthorised parties (e.g., media, friends, hackers)
29	Emailing sensitive company files or information (proprietary data, system specs, code, software, client data / files) from work accounts to private / personal email accounts
30	Emailing sensitive company files or information (proprietary data, system specs, code, software, client data / files) to competitors' email domains
31	Enabling unauthorised parties to access restricted company locations
32	Filing illegitimate claims (e.g., for expenses, actions or sales)
33	Hacking into company files (e.g., using password crackers) – CAPEC or VERIS community for detailed enumerations of hacking activities
34	Hacking into company systems / networks (and thus gaining unauthorised access) – CAPEC or VERIS community for detailed enumerations of hacking activities
35	Hacking into the files of the company's clients (e.g., using password crackers) – CAPEC or VERIS community for detailed enumerations of hacking activities
36	Hacking into the systems / networks of the company's clients (and thus gaining unauthorised access) – CAPEC or VERIS community for detailed enumerations of hacking activities
37	Inserting malicious functionality / code into company software
38	Inserting malicious functionality / code into software made for the company's clients
39	Installing / placing malicious programs (e.g., logic bombs, password-cracking programs, malware) on to company systems / networks
40	Launching attacks on the company's clients using sensitive company data on clients

41	Launching attacks targeting external parties from company networks (typically to frame the organisation and damage reputation)
42	Masquerading as a (co)worker as a platform for other attacks (likely using previously obtained credentials or hijacked workstations)
43	Masquerading as the company's clients (e.g., using previously obtained credentials or forgery)
44	Misappropriating company finances / monies via electronic means (e.g., illegitimate transfers or withdrawals typically to the actor's accounts or accounts owned by their friends or family)
45	Misappropriating the finances / monies of the company's clients via electronic means (e.g., illegitimate transfers or withdrawals typically to the actor's accounts or accounts owned by their friends or family)
46	Opening illegitimate or unauthorised accounts (e.g., at a bank or institution) using files or information from the company's clients (e.g., to allow access to a line of credit)
47	Physical destruction of company files / computer systems / property / hardware
48	Physical destruction of files / computer systems / property / hardware belonging to the company's clients
49	Physical theft (e.g., by removal or spying) of (co)worker's access credentials
50	Physical theft of company files / computer systems / property / hardware
51	Physical theft of company funds / monies
52	Physical theft of co-worker's property
53	Physical theft of files / computer systems / property / hardware belonging to the company's clients
54	Physical theft of funds / monies belonging to the company's clients
55	Printing sensitive company files or information (i.e., proprietary data, processes, system specs, code, software, client data / files)
56	Processing (intentional) illegitimate or inappropriate transactions or requests that are unauthorised or against company policy
57	Publishing / sharing (leaking) company access credentials to unauthorised parties or Web sites (e.g., in person / online forums or networks - NOT email)
58	Publishing / sharing (leaking) sensitive company files or information to unauthorised parties or Web sites (e.g., in person / online forums or networks - NOT email)
59	Removing security tags from company property or files (typically to a precursor to property theft or removal)
60	Searching for and identifying vulnerable company clients (e.g., the elderly, very wealthy, largely inactive, or those with mental health issues or that are deceased)
61	Selling the company's computer systems / property / hardware – unauthorised sales
62	Sending a (spear-)phishing email with malicious attachments or links to malicious Web sites, targeting company employees
63	Taking a computer screenshot / picture of sensitive company files or information (proprietary data, processes, system specs, code, software, client data / files)
64	Taking a picture of proprietary company property / hardware
65	Tampering with / corrupting / maliciously modifying company files or information (proprietary data, system specs, code, software, client data / files)
66	Tampering with / corrupting / maliciously modifying company processes
67	Tampering with / corrupting / maliciously modifying company property or systems
68	Uploading sensitive company files or information (proprietary data, system specs, code, software, client data / files) to unauthorised Web sites / hosts (e.g., online FTP server, Web server)
69	Using (co)worker's credentials (typically to gain access to company systems / data; may also result in an elevation of privileges)
70	Using / execution of malicious code for an attack or as a platform for another attack
71	Using credentials belonging to the company's clients
72	Using credentials from formerly held roles (typically to gain unauthorised access to systems / data)
73	Using credentials from shared user accounts
74	Using credentials which are fake or forged

75	Using own credentials
76	Using remote access or a VPN to access company systems / data from outside the company
77	Using the company's computer systems / property / hardware without authorisation or contrary to company policy