Insider Threat Examples by Sector

Agriculture and Food	A bookkeeper at a restaurant wrote 75 checks from the organization's account over a 25-month period to pay for personal expenses, and opened a credit card in the organization's name. She altered the organization's accounting records, and stole $175,000 before being caught. Six years prior to this incident, she was convicted of a similar fraud. She used the stolen money to purchase expensive collectible dolls.
Banking and Finance	A branch manager for a banking institution, after running into gambling issues, family health issues, and unforeseen expenses, stole more than $225,000 from business accounts.
Chemical	A senior research and development associate at a chemical manufacturer conspired with multiple outsiders to steal proprietary product information and chemical formulas using a USB drive for the benefit of a foreign organization. He received $170,000 over a period of 7 years from the foreign organization.
Commercial Facilities	A consultant in the commercial facilities industry downloaded the organization's proprietary software and, upon termination, tried to sell it to another organization for nearly $7M. She also used another organization's bank account to pay for a personal credit card bill, costing the second organization more than $425,000. It is believed that access to this account came from the consulting work from the first organization.
Communications	A group of insiders at a wireless telecommunications firm created clones of more than 16,000 customer cell phones; for at least six months they made approximately $15M worth of unauthorized calls, many of which were international.
Critical Manufacturing	A contractor for an automobile manufacturer set up a wireless network for their part distribution facility. Upon termination, the contractor deleted files and passwords on wireless devices in the distribution facilities, shutting down the manufacturer for nearly 8 hours.
Dams	N/A
Defense Industrial Base	A system administrator served as a subcontractor for a defense contractor. After being terminated, the system administrator accessed the system and important system files. The actions of the insider caused the system to crash and subsequently denied access to more than 700 employees.
Education	Over a 5-year period, a secretary who had worked at a youth organization for more than 20 years used a point-of-sale system to issue at least 500 fraudulent refunds totaling more than $300,000 to the insider's own bank account.
Emergency Services	An IT worker in a telecommunications company responsible for running an emergency 9-1-1 system deleted data on three servers that handled emergency calls, which brought down the system. He then stole more than 50 back-up tapes to further amplify the attack.

Insider Threat Examples by Sector

Energy	An oil-exploration company hired a temporary consultant to assist in setting up a Supervisory Control And Data Acquisition (SCADA) system that enables communication with offshore platforms and detection of pipeline leaks. His contract was about to expire and he requested permanent employment; the request was rejected and his contract ended. For 2 months following termination, he planted malicious programs on the organization's systems that temporarily disabled the SCADA system.
Healthcare and Public Health	After termination, a system administrator for a public health organization remotely accessed the organization's systems and deleted files, modified employee information, and changed passwords to the systems. She then locked the company's firewall with a new password until she was caught and pled guilty nearly 3 months later.
Information Technology	A network administrator for an organization in the IT industry was simultaneously employed by another organization, and resigned after being confronted about the matter. He then installed a script that created a backdoor on the server and deleted file systems on two servers, costing the organization more than $200,000.
National Monuments and Icons	N/A
Nuclear Reactors, Materials and Waste	A software developer worked at a high technology firm that developed supercomputers that were often used in nuclear weapons safety systems. After transferring out of the supercomputing division, he sought revenge on his former colleagues by demonstrating the inadequacy of their security. He logged in remotely to one of their supercomputers, downloaded the password file, and then ran a password cracking program on the file before being discovered by the organization's personnel.
Postal and Shipping	Following termination, a programmer at a logistics company used several backdoors he had installed prior to termination and a shared account to remotely access the network, and removed critical programs he had developed, causing a server and multiple programs to fail.
Transportation Systems	Two employees at an organization that was in the middle of a labor dispute sabotaged the system controlling the traffic lights of a major city. The sabotage took 4 days to fix, during which time traffic was greatly affected.
Water	An electrical supervisor developed applications for a SCADA system used by the water industry. After termination, he installed a malicious program on one of the organization's critical systems, damaging the SCADA system.

Source: CERT Insider Threat Center, CERT Program, Software Engineering Institute, Carnegie Mellon University, 2012.