Christopher Victor Grupe

- Senior Network Design Engineer
- 46 years of age at sentencing
- Former Army Reservist (Resigned after losing clearance)

CDSE

Center for Development of Security Excellence

CASE STUDY

Sabotage

WHAT HAPPENED

In early December 2015, Christopher Victor Grupe, an employee for a transcontinental railroad company named the Canadian Pacific Railway (CPR), was working on a network upgrade at the Nahant Yard, which is a diesel servicing yard in Davenport, Iowa. The transition to the new system was scheduled to take place during a "change window" starting at 8:00 pm on December 3. During the change window, the existing system would have to be taken down. Grupe had requested the change window be moved to December 2, but senior management denied his request. Still, Grupe decided to proceed with the upgrade on December 2, causing an unexpected outage.

Grupe's supervisor, Ernest Seguin, wound up restoring the service. After doing so, Seguin reiterated to Grupe that the two of them would upgrade the system together during the scheduled change window on December 3. Seguin also reminded Grupe that making changes outside of the scheduled change window would be cause for termination. Despite that warning, Grupe disregarded Seguin's instructions and again tried to upgrade the system on his own, which caused more problems.

Grupe ignored Seguin's multiple attempts to contact him; however, this changed when Seguin told the on-site project manager that he was going to have Grupe escorted from the property by CPR police. Grupe finally called Seguin and was verbally abusive on the phone to Seguin. Still, the two continued to work with other employees to complete the upgrade, but Seguin suspended Grupe and later told him to stay off CPR property during his suspension. Seguin also took steps to suspend Grupe's computer accounts and building access. Again, Grupe disregarded Seguin's instructions by showing up on CPR property and communicating with on-site CPR staff.

On December 15, 2015, following a 12-day suspension, Grupe was notified by CPR management that he was going to be fired due to insubordination. However, at Grupe's own request, he was allowed to resign, effective that same day. In his resignation letter, Grupe indicated that he would return all company property—including his laptop, remote access device, and access badges—to the CPR office. Before returning his laptop and remote access device, Grupe accessed the CPR computer network's core "switches," which are high-powered computers through which critical data is channeled in the CPR network. Once inside, Grupe deleted files, removed administrative-level accounts, and changed passwords on the remaining administrative-level accounts, effectively locking CPR out of these network switches. Grupe also attempted to conceal his activity by wiping the laptop's hard drive before returning it to CPR.

Later, when trying to address a networking problem, CPR staff discovered that they were unable to access the main network switches. CPR then investigated whether someone had changed the password. As part of the investigation, another network design engineer called Grupe to ask if he knew of any previous passwords that would get them into the switch. Grupe did not disclose that he had changed the password for the admin account. After CPR IT staff was able to regain access, they discovered evidence in logging data connecting the damage to Grupe. CPR hired an outside computer security company to identify the source and scope of the intrusion and to conduct an incident analysis, which ultimately connected the damage to Grupe. Grupe was convicted of one count of intentional damage to a protected computer. On February 13, 2018, Grupe was sentenced to one year and one day in prison for causing intentional damage to critical portions of CPR's computer network.

INDICATORS

Professional Performance and Lifecycle: 12-day suspension and termination due to insubordination.

Technical Activity: Grupe's actions caused an unexpected power outage. After termination, he deleted files, removed administrative-level accounts, changed passwords on administrative-level accounts, and attempted to conceal his activity by wiping the laptop's hard drive, yet an outside computer security company was able to connect network damage to Grupe's actions.

Security/Compliance Incident: In two instances, Grupe, proceeded with a system upgrade without supervisor authorization, and Grupe violated a suspension order to remain off of company property.

IMPACT

Grupe's disgruntlement and intention to exact revenge on CPR endangered a transcontinental railroad used to provide transportation and supply chain deliverables across North America. CPR incurred a $30, 000 loss as a result of Grupe's actions.

ADDITIONAL INFO

Consider the following question:

Could CPR's mitigation response for Grupe have been decided differently?

Resources for further exploration:
Insider Threat Indicators in User Activity Monitoring:
(https://www.cdse.edu/Portals/124/Documents/jobaids/insider/Insider-Threat-Indicators-in-UAM.pdf)

IF YOU SEE SOMETHING, SAY SOMETHING!

Contact the appropriate POC to report any observed potential risk indicators:

Name: _____ Agency/Department: _____
Title: Supervisor/Security Officer/ITP Senior Official/ITP Manager