



Shannon Stafford

- Employed in the IT department at a global company
- Sentenced to 12 months and one day in federal prison, followed by three years of supervised release
- Ordered to pay restitution in the amount of \$193,258.10 to his former employer



CDSE

Center for Development
of Security Excellence

CASE STUDY

Illegally Accessing and Damaging a Computer Network

WHAT HAPPENED

- Stafford worked in the IT department of a global company with thousands of employees and offices around the world. As part of his duties, he had access to the system login credentials of other employees and was authorized to use them in the course of his technical support duties. He was also responsible for disabling users' network access credentials at the end of their employment.
- In 2014, Stafford was promoted to manager and technical site lead for the Washington, D.C., office, but in March 2015, he was demoted back to an IT support role due to performance issues. Stafford's performance issues continued, and he was fired on August 6, 2015. Stafford did not return his company laptop.
- On the evening of August 6, 2015, Stafford made 10 unsuccessful attempts to access the company's network using his own credentials and the credentials of a former co-worker.
- In the early morning hours of August 8, 2015, Stafford succeeded in accessing the computer that had been located under his desk without authorization. Leveraging the unauthorized access, he erased all file storage drives used by the Washington, D.C., office, then changed the credentials for the storage management system.
- On August 11, 2015, Stafford unsuccessfully attempted to remotely access the company's computer network from his home approximately 13 times, using credentials that were not his.
- On August 13, 2015, a company representative spoke to Stafford and demanded that he cease and desist his attempts to unlawfully access Business A's computer systems. Despite the company's demand, Stafford attempted to access the company's network approximately 17 times.
- On September 14, 2015, Stafford used the credentials of another former co-worker to access a network file storage system in the company's Baltimore office, intending to cause the same type of damage. However, Business A had changed the password after Stafford's attack on the Washington, D.C., files.

INDICATORS

- Declining work performance - Stafford's work performance in his new role was problematic, leading to demotion and, ultimately, dismissal.
- Disgruntlement – Stafford was disgruntled over his demotion, which fueled his further decline in performance.
- Technical Activity – Stafford had tried to access company data several times before he succeeded.
- Access attributes – Stafford's position as an IT professional gave him the knowledge of other user's credentials

IMPACT

- The deletion of the files caused severe disruption to the company's operations and the loss of some customer and user data.
- Changing the password hindered the company's efforts to determine what happened and restore access to its remaining files.
- Washington users were unable to access their stored files for approximately three days, until the data could be restored from backups.
- Customer and user data that was not included in the most recent backup prior to Stafford's deletion of the files was permanently lost.
- The actual loss to Business A that resulted from Stafford's damage and attempted damage to their computer systems, including the cost of restoring the deleted systems, investigating what happened, and responding to the intrusion, was at least \$38,270.
- Business A also incurred legal fees totaling \$133,950.60 and a fee of \$21,037.50 for a forensic investigation.

ADDITIONAL INFO

- While the employee's account was disabled after he was terminated, he was able to use co-workers' accounts to access the systems, using his company issued laptop which he failed to return. The risk of shared credentials can be mitigated by requiring multi-factor authentication, particularly to any privileged accounts.
- Mobile Device Management systems can be used to manage and wipe laptops; leverage this capability just as you would for a lost or stolen smartphone/tablet to render it unable to access corporate resources, as well as delete any company data.

Consider the following questions:

- How can your organization improve the handling of the separation process to mitigate the risk from misuse of a company-issued device, like a laptop?
- What policies and procedures protect your organization from the unique risks posed by privileged users?

Resources for further exploration:

- [Insider Threat Indicators Job Aid](https://www.cdse.edu/Portals/124/Documents/jobaid/insider/INTJ0181-insider-threat-indicators-job-aid.pdf)
<https://www.cdse.edu/Portals/124/Documents/jobaid/insider/INTJ0181-insider-threat-indicators-job-aid.pdf>
- [Privileged User Cybersecurity Responsibilities eLearning course](https://public.cyber.mil/training/privileged-user-cybersecurity-responsibilities/)
<https://public.cyber.mil/training/privileged-user-cybersecurity-responsibilities/>
- [Cybersecurity and the Use of New Personal Devices](https://securityawareness.usalearning.gov/cdse/multimedia/shorts/cyber/Block10/Introduction/page_0010.html)
https://securityawareness.usalearning.gov/cdse/multimedia/shorts/cyber/Block10/Introduction/page_0010.html

IF YOU SEE SOMETHING, SAY SOMETHING!

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

Name: _____
Title: Supervisor/Security Officer/ITP

Agency/Department: _____
Senior Official/ITP Manager