

CASE STUDY

Crime: Sabotage

WHAT HAPPENED

Levii Dino Delgado was employed by the Henrietta Johnson Medical Center (HJMC) as an information technology (IT) administrator, providing on-site IT services to HJMC employees. Delgado was terminated from HJMC in August 2017. This resulted in Diamond Technologies, a third party IT firm located in Wilmington, Delaware, disabling Delgado's user account, which allowed for access to HJMC's computer network. Diamond Technologies' services included, but were not limited to, general IT support services, Cloud services, Microsoft Office 365 services, cyber security services, and disaster recovery and business continuity services. Despite being terminated, Delgado connected his personal laptop to the HJMC computer network through the HJMC Virtual Private Network (VPN) by using a separate administrator account. Delgado continued to access HJMC from this account without HJMC's knowledge or consent.

Delgado deleted all HJMC employee user accounts, deleted HJMC's file server, and disabled all HJMC's computer accounts. HJMC's employees were unable to log into their computers and access their electronic files, including patient files and other information necessary to managing and conducting HJMC's operations. As a result, the medical center's ability to see and treat its patients was impaired.

According to a press release from the U.S. Attorney's Office in Delaware, no patient information was compromised or accessed as a result of Delgado's actions.

Delgado pleaded guilty in February 2021 to one count of causing damage to a protected computer.

Delgado was sentenced to six months of home confinement and more than \$13,000 in restitution.

INDICATORS

- **Access Attributes:** Delgado had access to HJMC's computer server due to his employment as an IT administrator. His authorizations were revoked when he was terminated, but he maintained access through a separate administrator account.
- **Technical Activity:** Delgado accessed HJMC's system without having the proper authorization by connecting to the HJMC VPN with an administrator account of which HJMC was unaware.



Levii Dino Delgado

- Levii Delgado was age 36 at the time of sentencing
- Levii Delgado pleaded guilty to one count of causing damage to a protected computer
- Levii Delgado worked as an information technology administrator at the Henrietta Johnson Medical Center which provided care to underserved communities



CDSE

Center for Development
of Security Excellence

IMPACT

- U.S. Attorney Weiss stated, “The defendant abused his knowledge of his former employer’s computer network to deliberately disrupt the medical center’s capability to conduct business. As a result, the defendant directly impeded that entity’s ability to provide medical care to the communities it serves, putting patients at risk. My office is committed to prosecuting any individual who thinks attacking a former employer’s computer network is an acceptable reaction to getting fired.”
- “Several administrative rules promulgated by the U.S. Department of Health and Human Services (HHS) further define protected health information (PHI) and provide for its privacy and security. In general, outside of health care provision and billing, access to someone’s PHI is carefully guarded, and the individual must approve any release of such information.” FBI Law Enforcement Bulletin: Protected Health Information and Use-of-Force Investigations.

ADDITIONAL INFO

- HJMC was a Federally Qualified Health Center (FQHC) that had four medical centers in Wilmington, Delaware, which provided medical care to under-served communities.
- HJMC contracted the services of Delaware Health Net (DHN), a 26 U.S.C. § 501(c)(3) non-profit organization, to assist with, among other things, IT services. DHN employed Diamond Technologies.

Consider the following questions:

- Which countermeasures could be applied to prevent this from happening again?
- What factors could have made Delgado more difficult to detect?

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>)
- [Insider Risk Programs For The HealthCare and Public Sector Job Aid](https://www.cdse.edu/Portals/124/Documents/jobaid/insider/insider-risk-jobaid.pdf)
(<https://www.cdse.edu/Portals/124/Documents/jobaid/insider/insider-risk-jobaid.pdf>)
- [DHS- U.S. CERT “Combating the Insider Threat”](https://www.us-cert.gov/security-publications/Combating-Insider-Threat)
(<https://www.us-cert.gov/security-publications/Combating-Insider-Threat>)

Supporting Through Reporting!

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

Name: _____
Title: Supervisor/Security Officer/ITP

Agency/Department: _____
Senior Official/ITP Manager