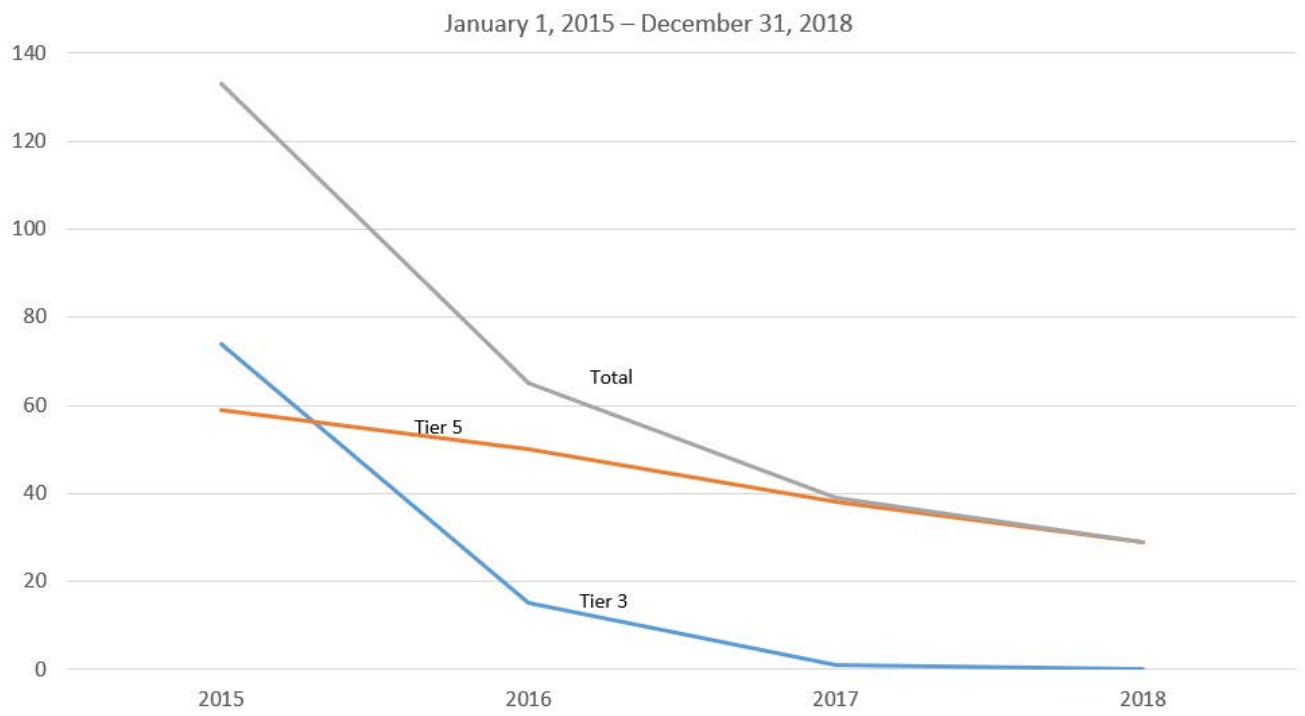
Number of Information Security and Privacy Incidents (2015-2018)[55]



Tier-5 response recommendation indicates that malicious code or software has been detected on an agency machine, but it is not fully compromised and there is no risk of sensitive information loss

Tier-3 response recommendation is both an incident notification and a request for agency assistance
• The Tier-3 designation indicates that a machine is fully compromised and there is a possibility that sensitive information could have been accessed or lost
• Further investigation by the agency is required to determine if the affected user had access to sensitive information.
• An incident will never stay classified as a Tier 3; it will either be escalated to a Tier-2 if the agency reports sensitive information was definitely or potentially involved, or downgraded to a Tier-4 if the agency reports no sensitive information was involved

Tier-1 response recommendation indicates a very serious incident of a criminal nature, usually brought to the attention of Security Operations Center (SOC) through law enforcement agencies (SLED, FBI, Secret Service, etc.)

---

[55] S.C. House of Representatives, House Legislative Oversight Committee, "Agency Presentation – Legal and Compliance Unit (October 1, 2019)," under "Committee Postings and Reports," under "House Legislative Oversight Committee," under "Corrections, Department of," and under "Meetings," https://scstatehouse.gov/CommitteeInfo/HouseLegislativeOversightCommittee/AgencyWebpages/Corrections/SCDC%20Legal%20and%20Compliance%20Presentation%20(10.01.19).pdf (accessed October 18, 2019), slide 140-141. Hereinafter "Legal Presentation."