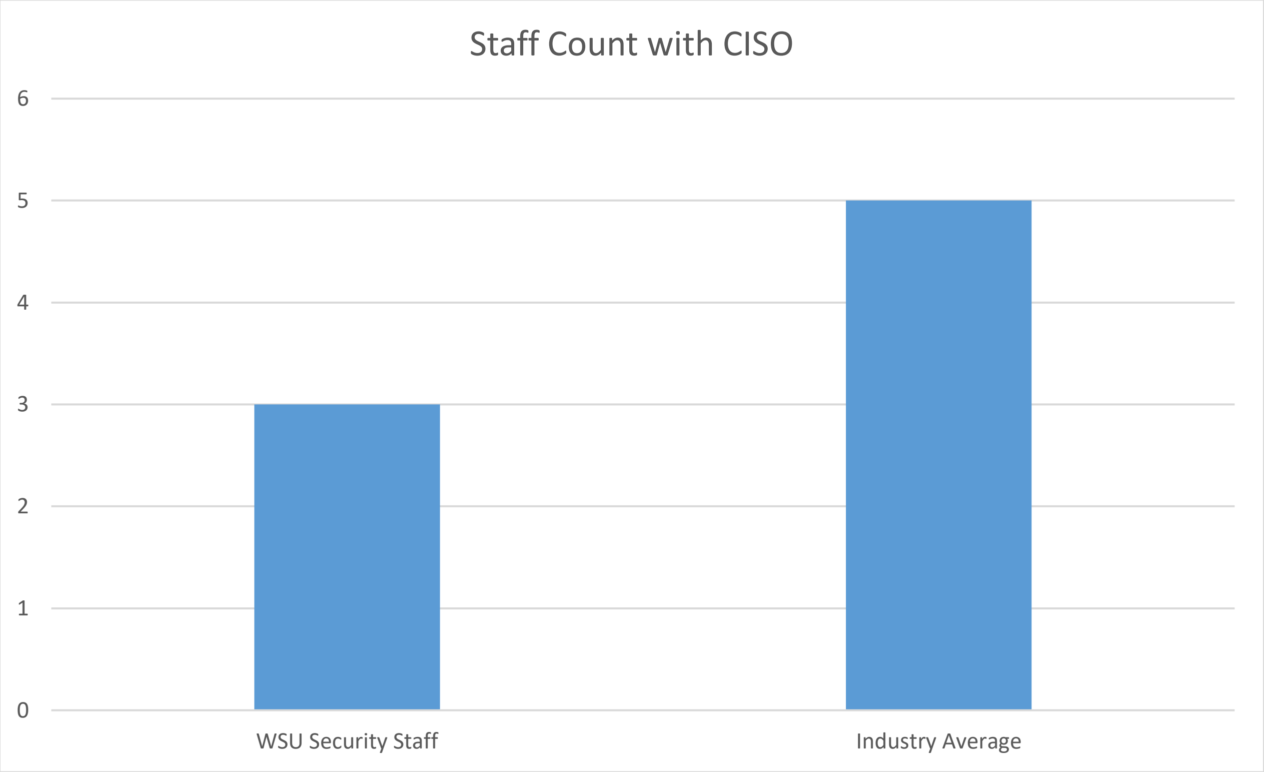
Department/Unit: **CaTS – IT Security** **Year: 2018**
Contact Name: **Mike Natale** **Contact Title:** **Chief Information Security Officer**

Unit Overview/Mission/Purpose

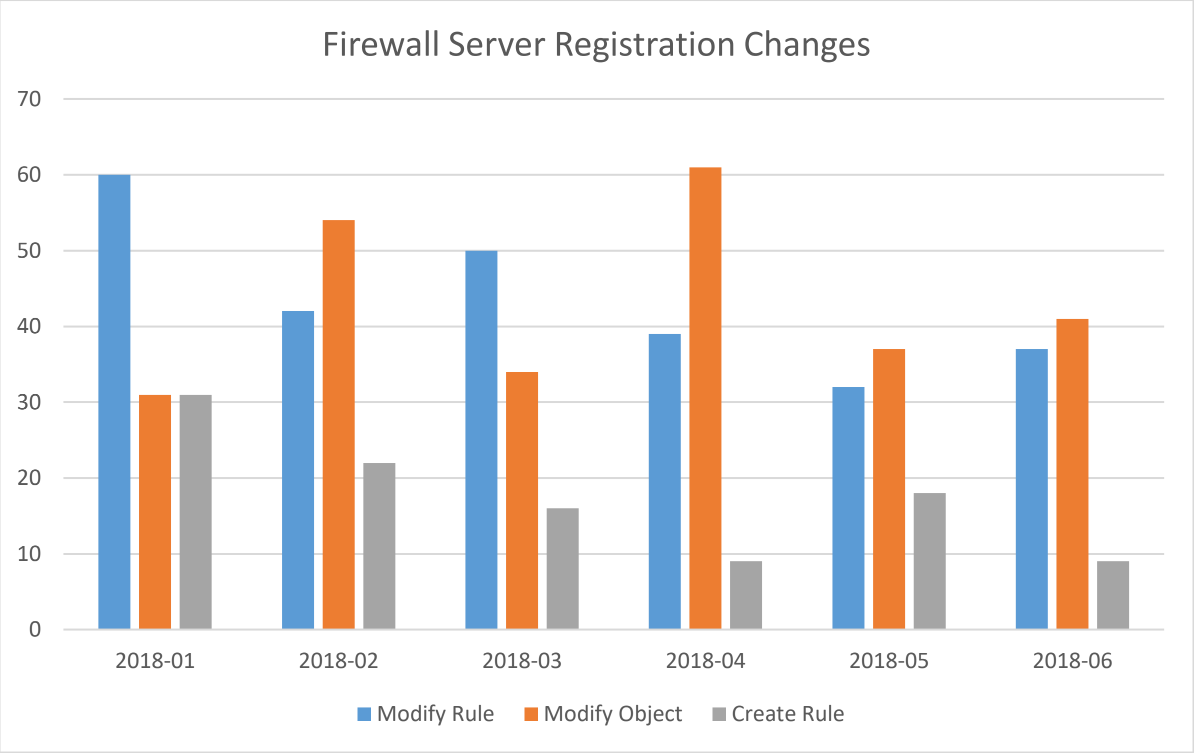
The mission of the Information Security Department is to support the central mission of the University by assuring the confidentiality, integrity, and availability of its information and information systems. This mission requires a balanced approach to information security – being mindful and diligent of security needs and requirements, while assuring availability and usability of university systems. This mission is accomplished by focusing on reducing risk; complying with relevant laws and regulations; raising awareness of security needs through advocacy and education; and applying trusted technology.

Staffing

	FY16	FY17	FY18	FY19
# Full Time Staff	4	3	3	3



Success Outcome 1:
Though short staffed, the information security department strives to be able to maintain a 1 business day response time to firewall rule change requests.



KPI 1.1
Data: Data shows the monthly firewall rule changes from January, 2018 to June, 2018.

Result: The work load is generally consistent through the school year with change requests dropping off in the summer months. This consistent work load allows us to be responsive to firewall change requests. We are generally able to respond within 1 business day for firewall rule change requests.

Response/Action Plan: Due to the limitation of the server registration program we are unable to track the exact time from request to completion. Moving the server registration process into ServiceNow would increase efficiency and allow for more accurate tracking for request types and response times.

Success Outcome 2:
Another measure of success is the number of P1 and P2 incidents impacting the university and the response time to resolve those incidents.

A P1 is defined as: an incident impacting teaching and learning, or support services, for the entire university or many departments. Core line of business or critical support services are affected.

A P2 is defined as: an incident impacting teaching and learning, or support services, for a single or few departments. General university support services are affected.

Firewall P1 and P2 Incidents 12/6/16 to 5/22/18			
P1	P2	Total	Avg. Time to Close in Hours/Minutes
3	4	7	1:33

Firewall P1 and P2 Incidents 12/6/16 to 5/22/18			
2016	2017	2018	Total
1	4	2	7

KPI 2.1

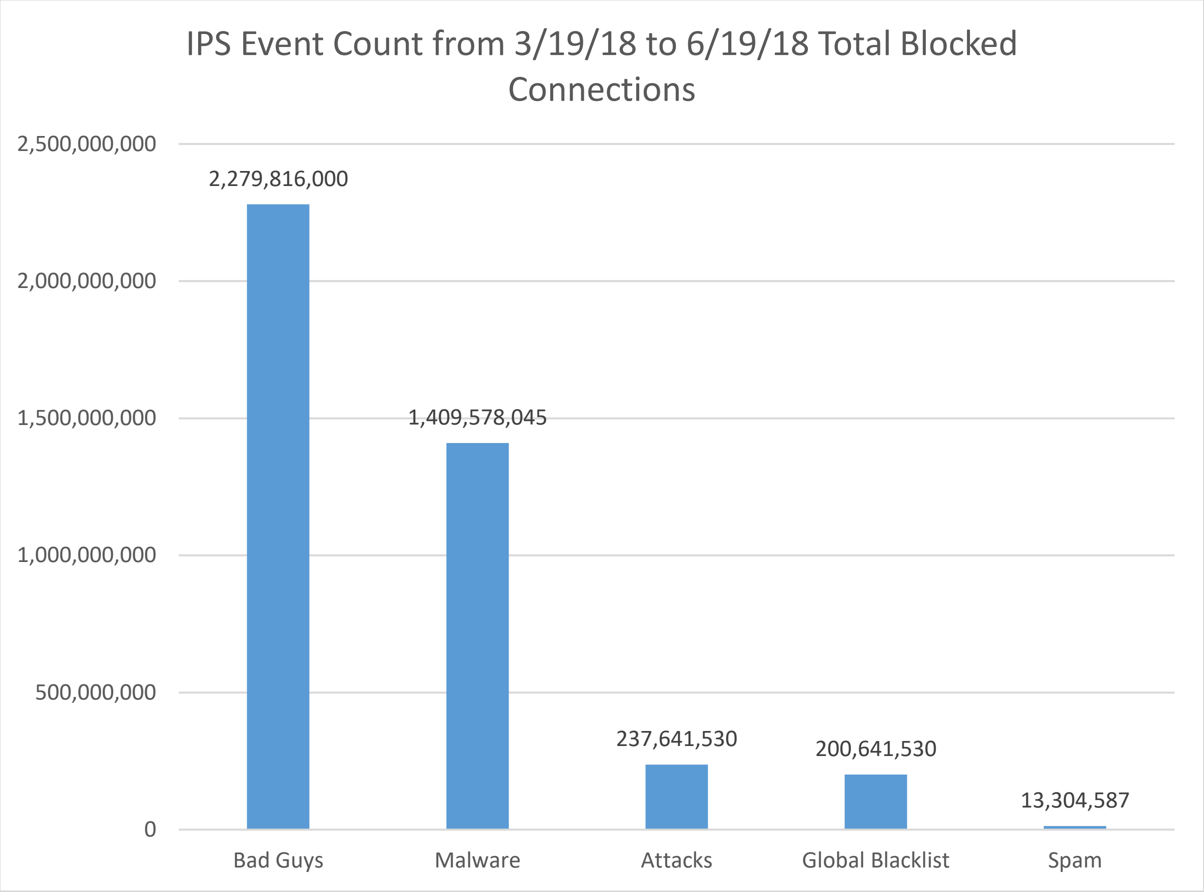
Data: There have been 3 P1 and 4 P2 incidents involving the firewall since ServiceNow has been utilized to track these incidents. The time period involved is from December, 2016 to May, 2018. 2017 is elevated due to the firewalls being replaced that year resulting in some performance issues which were resolved by tuning the traffic inspection.

Result: Generally the firewall performs well with very few incidents that impact the university. Uptime for the firewalls is in the 99.9% range.

Response/Action Plan: We continue to work with Check Point, the firewall vendor, to address performance and stability issues. Check Point has been responsive in the past by creating bug fixes to address the issues we have reported.

Success Outcome 3:

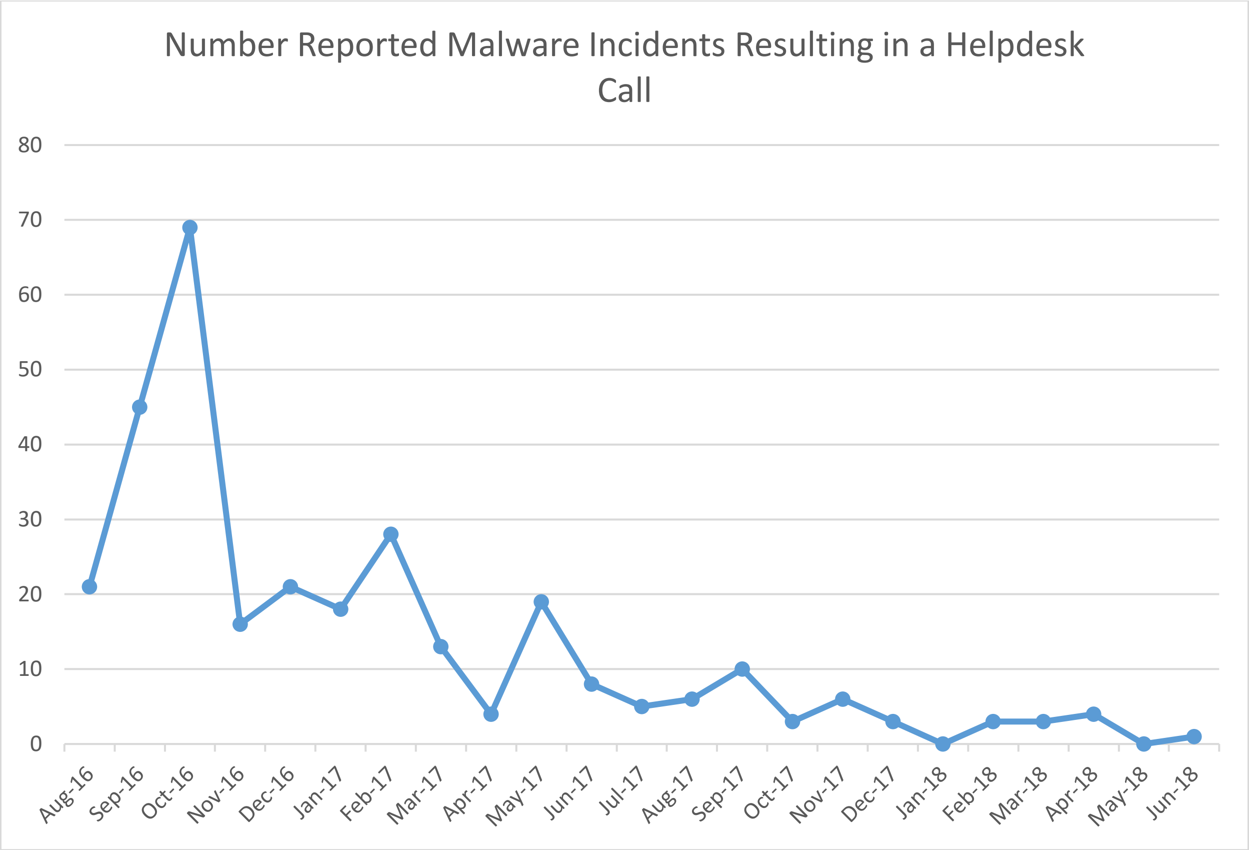
Successfully blocked attacks, malicious connections, and blocked malware indicates the necessity of having effective defensive measures in place. The number of reported malware events should be tied to the effectiveness of the defensive and preventative security measures in place. This includes firewall, Intrusion Protection System, and next gen antivirus/antimalware software.



KPI 3.1
Data: This data shows the various network intrusions blocked by the Intrusion Protection System for the period of March 19th, 2018 to June 19th, 2018.

Result: This metric illustrates the volume of attacks against the university. If the Intrusion Protection System is effective, the number of events affecting systems on the network should remain relatively low.

Response/Action Plan: The Intrusion Protection System is one factor in efforts to protect WSU systems. The deployment of next gen antivirus software is another component in our efforts to protect the university.



KPI 3.2

Data: This data illustrates a downward trend in the number of malware events being reported at the university. We contribute this downward trend to the effectiveness of our firewall and Intrusion Protection System along with CaTS selectively deploying the next gen antivirus/antimalware software on computers which have repeatedly been infected. In addition, this software has been deployed to departments that routinely handle sensitive data – HR, Payroll, and Bursar for example.

Result: This indicates our protective and defensive measures are working.

Response/Action Plan: Continue efforts to tune the Intrusion Protection System and further deploy the next generation antivirus/antimalware software SentinelOne to campus.

Concluding Remarks (optional)**:**

As SentinelOne is further deployed we expect to see the number of malware events to remain low. This equates to lower risk for the university, less downtime for users, and increased productivity.