Network Attack Report 2-28-17

As the Library prepared to open for business on Thursday, January 19th technology staff discovered most of our servers were inoperable, and an onscreen demand for a payment in bitcoin for an access code to regain control. The Library made the decision not to consider payment, and we immediately contacted the FBI cybersecurity unit. The FBI over a period of days asked for data to be downloaded, which they used to establish what malware had been used. The Department of Homeland Security separately asked for this data to be sent to them on disk by mail. Neither agency has been on site. The attack affected over 700 computers system-wide and prevented checkout and computer access at all Library locations on the 19th.

Technology Services staff, working around the clock, began the complex task of regaining access to the affected servers and using the Library's backup system to restore them. Rudimentary services began to be restored over the weekend. All Library locations remained open and some portions of our network which were unaffected continued to be heavily used throughout the recovery. SLPL's website, including the catalog, databases, and downloadable materials, remained active and busy. The powerful wireless network remained in heavy usage in all locations.

For most patrons, the Library was functioning normally two days after the attack. Once the Library had regained control over the network, staff made patron services the first priority. The ability to check out materials was restored on January 20 and the hundreds of "reservable" computers for patron use throughout St. Louis were available again on January 21. Printing for patrons was one of the last public services to be restored. Many individual staff computers are still affected, and must be completely erased and recreated. Much work remains to be done behind the scenes.

The staff of the Library continued to serve the public, providing the best customer service possible under difficult circumstances. Patrons were thoughtful and understanding in regards to limited services. The support of the public was overwhelmingly positive and very much appreciated. Staff were able to use library owned laptops and Chromebooks to connect to the wireless network and assist patrons. Many used personal devices to provide customer service. Staff and patrons alike commented on how being "unplugged" was like going back in time — with library tables filled with people and books and staff using traditional reference resources and ingenuity to assist with questions. For example: A patron came into Central Library looking for a particular poem for her brother's funeral. Entertainment, Literature, & Biography Room staff found the Library did not have a copy in its poetry collections. With Inter Library Loan services down, staff reached out to several other libraries, and San Francisco Public Library was able to send a copy of the poem.

Marketing responded to more than forty media inquiries related to the ransomware attack, issued patron update messages to the public, and kept system staff informed throughout the restore. In addition, Marketing served as the Help Desk for the system, fielding and filtering staff and patron calls related to technology issues. The Library's website and social media

platforms were used to communicate with the public about the attack and the restoration of services.

Using information from the FBI and staff research, Technology staff identified a server dedicated to the Library's voicemail system as the point of entry. This server was well within its service life, but hackers were able to find and exploit software required by the vendor, and jump to other, more key systems. That server was immediately taken offline.

Staff prioritized patron services and then ranked staff functions. Restoring functions such as the lighting systems and the wireless communication system in Central Library were given priority.

The Library's sophisticated intranet system was affected by the attack and is still offline, and greatly missed. Technology Services created a workaround system which has enormously improved system communications, but much functionality remains to be restored. Systems that handled key functions such as incident reports, or maintenance and custodial service requests, have been replaced with temporary workarounds.

As of 3-20-17, most staff members have access to their emails and saved files.

Preventative Measures Being Taken

In addition to a number of temporary measures taken while the network was being restored, a number of permanent changes have been made or are being made.

A system designed for government and military networks was installed and provides a screen outside the Library's firewall.

Although our firewall is also well within its rated service life, we have researched updated and more rigorous new firewall designs, and have decided to install a new system.

The Library had budgeted and begun installing a new backup system before the attack occurred. There will be levels of automatic backup through the Library's network, and a level of backup kept entirely isolated. There will be a third level of remote storage off site in the cloud.

The Library is requesting proposals from network security firms to provide a Security Policy Review to audit and review our digital protection, and make recommendations for any improvements. The security posture review will focus on following best practices to guard against future intrusions.