Office of Inspector General
Legal Services Corporation

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

LSC-OIG HOTLINE ADVISORY

Success Story: Grantee Mitigates Impact of a Ransomware Attack

---

Ransomware attacks are on the rise for all types of industries. Common causes of ransomware attacks include spam or phishing emails, employees being deceived, weak passwords and related access management issues, and employees accessing malicious websites. Cyber-security training for employees is a key element to prevent ransomware attacks.

The Legal Services Corporation (LSC) Office of Inspector General (OIG) Hotline receives information from grantees reporting fraud and related losses. Since October 2018, LSC grantees have reported multiple ransomware attacks against their IT networks. Many of these ransomware attacks have been disruptive, caused damage, and often lead to monetary losses.

Due to this trend, the OIG is issuing this Hotline Advisory to highlight some practices to successfully mitigate the damage and quickly recover from the attack. We use as a case study a recent ransomware attack against a grantee and its successful handling of the attack due to its IT infrastructure designed to guard against ransomware and other forms of cyber-security attacks as well as its incident response plan and efforts.

Multiple Server Backups

The grantee reported that the ransomware attack prevented them from accessing administrative, accounting, payroll, and human resources files located on three in-house servers. The grantee had a process of continuously backing up all three servers to local hard drives, as well as a daily backup to an online cloud service.

The grantee was able to use the daily cloud-based backup of the three servers to restore its administrative, accounting, payroll, and human resources data. Each day, the grantee received notice from the cloud service that the backup for that day was successful and that there were no errors. The grantee was able to use the prior day's backup to restore its files.

Protecting Client Data

The grantee stored its client data in a case management system (CMS) on a cloud-based hosting service separately from its network. By having the CMS and clients' personally identifiable information stored separately, and on a cloud-based hosting service, the cyber-criminal was not able to access the grantee's client data.

Using Cyber Insurance to Recover

Prior to the attack, the grantee had acquired a cyber insurance policy that assisted the grantee in recovering from the attack, including covering most of the costs to restore the network and investigate the attack.

The grantee reported the attack to its cyber insurer, which took immediate action and provided the grantee with an IT contractor to remove the ransomware virus from the grantee's network, clean the servers, and restore the network using the grantee's cloud-based backups. The IT contractor also reviewed the network to identify how the grantee was infected with the ransomware and what data was lost.

Conclusion

To guard against successful ransomware attacks, it is imperative that grantees plan ahead, instituting strategies to backup and protect data. Additionally, a well thought out incident response plan will greatly assist grantees in their recovery from any such attack. Finally, grantees might consider cyber insurance to assist in recovery efforts.

Guidance from the FBI

The Federal Bureau of Investigation (FBI) does not support paying a ransom in response to a ransomware attack. Paying a ransom does not guarantee that you or your organization will get any data back. It also encourages perpetrators to target more victims, and it offers an incentive for others to get involved in this type of illegal activity.

If you are a victim of ransomware:

- Contact your local FBI field office and local law enforcement to request assistance, or submit a tip to the FBI online.
- File a report with the FBI's Internet Crime Complaint Center (IC3).
- Contact the LSC-OIG Hotline.

Additional OIG Cyber-Threat Resources

Fraud Corners

Fraud Alerts

COVID-19 Fraud Scams

If you have any questions or would like additional information about this Hotline Advisory article, please contact Daniel O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at (202) 295-1651 or by email at dorourke@oig.lsc.gov.