TIP Jar

Tech TIPs: Preventing Data Breaches

Spring 2017

Public agencies are increasingly the targets of malware and ransomware attacks. So what can you do to protect your agency? The National School Boards Association (NSBA) offered some tips in Jill Greenfield's August 2016 Inquiry & Analysis, "Protecting Personal Information: Managing and Preventing Data Security Breaches." We share those tips here with NSBA's permission. The following is an adapted version of the report's advice on preventing data breaches.

While the tips were drafted with school districts in mind, cities, counties and other public agencies may also find them useful. Inquiry & Analysis is a publication available to members of the NSBA's Council of School Attorneys, and the full article may be viewed on the association's website. NSBA has also published a data security guide, which is available here.

Know what data exists, what is being collected and where it is stored.

- Only collect necessary personal information.
- Be transparent with users about what data is collected and how it is used.

Install a firewall, an intrusion detection/prevention system (IDPS) and antimalware software.

Store and transmit data securely.

- Encrypt data that includes personal information stored on servers or on mobile devices.
- Any personal information being transmitted, particularly via email, should be redacted or encrypted.

Control access to data.

- Consider requiring strong passwords and multiple levels of user authentication.
- Set limits on the duration of data access and administrator privileges.
- Determine which personnel have access to specific categories of user personal information.
- Place public access computers on a separate network.

Keep software up to date.

- Develop a patch management plan to keep the system protected.

Delete data when it is no longer needed (subject to state and federal requirements).

Teach employees with access to personal information about appropriate uses for that data.

- Create an acceptable use policy that outlines appropriate uses for the agency's systems and incorporate security policies into employee responsibilities.

LS Lozano Smith
ATTORNEYS AT LAW

As the information contained herein is necessarily general, its application to a particular set of facts and circumstances may vary. For this reason, this TIP Jar piece does not constitute legal advice. We recommend that you consult with your counsel prior to acting on the information contained herein.

- Encourage employees to verify who has access to a given network location before saving, posting or sending personal information.

Instruct employees to be cautious of suspicious advertisements, emails, attachments and websites.

Encourage employees to use cryptic passwords and not to share them.

- Change initial and temporary passwords as soon as possible.
- Use different passwords for work and non-work accounts.

Inventory and secure portable devices.

- Keep laptops in sight or locked to a work station or other secure location.
- To avoid theft, don't leave papers, computers or other electronic devices visible in an empty car or house.
- Consider extra security measures like encryption for portable devices.
- Monitor inexpensive assets like thumb drives that can contain personal information.

If your agency has a "Bring Your Own Device" (BYOD)/personal device program, establish security policies.

Destroy or securely delete data before reusing or disposing of equipment.

- Securely erase printers, fax machines and photocopiers before resale, disposal or return to vendor.
- Shred paper records with personal information before disposal.

Restrict physical access to areas where personal information is stored.

- Secure access to any areas where sensitive data is stored.
- Consider locking office doors and filing cabinets, installing card access control to offices and having auto log off functionality on computers.

Do the due diligence.

- Interview vendors and review their security policies regarding employee background screening and data management.
- Examine the vendor's insurance coverage and any prior legal complaints, litigation or regulatory actions, with your attorney's assistance.

Know which online services are being used in your agency.

- Have policies and procedures to evaluate and approve online services.

Draft data security contract language.

- Work with your attorney to specify how data should be handled while it is in use and how it will be returned or erased.

De-identify information that goes to vendors.

Create a response plan.

- Typically, public agencies have crisis management plans in place for emergency situations. Establishing a similar plan for responding to a data breach will promote better response coordination and a quicker response.

As the information contained herein is necessarily general, its application to a particular set of facts and circumstances may vary. For this reason, this TIP Jar piece does not constitute legal advice. We recommend that you consult with your counsel prior to acting on the information contained herein.