Cyber Attacks on Broadcast Stations

By: Judy Endejan*

GSB Public Media Contact:

Judy Endejan
Seattle
jendejan@gsblaw.com
206.816.1351

An unfortunate fact of life today is that you may be hacked. Hackers, usually operating in distant countries, are moving down the food chain of American commerce to target smaller, more vulnerable entities such as broadcast stations. Public broadcasting stations may be particularly vulnerable as one station, WHQR in Wilmington, Delaware, discovered. During pledge week, WHQR received a ransom demand from a hacker in Latvia. The demand came when four station computers revealed pop-ups saying that the files had been encrypted and asking for money to free them up. Luckily, the station resolved the matter without jeopardizing its pledge drive, operations or membership database. Consult with your IT staff or consultant about the following ways you can protect your data in the event that a hacker targets your station:

1. **Encryption.** Encrypt your confidential financial data provided to you from donors and listeners. Keep the encryption key stored in an incredibly secure place, accessible only by top station management. If you encrypt your data, hackers may obtain access to it but they will not be able to read it and obtain sensitive financial information, such as credit card information, social security numbers, etc. By encrypting your data you will be able to take advantage of legal safe harbors. These exist for "secured data" which means that the data is "encrypted in a manner that meets or exceeds National Institute of Standards and Technology or is otherwise modified so that personal information is rendered unreadable, or undecipherable by unauthorized persons." See (http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf) from the National Institute of Standards and Technology for advice on how to protect your data through encryption.

2. **Manage Your Data.** Classify the data on your computers by sensitivity and delete in a secure manner any outdated extraneous sensitive information.

3. **Install Safeguards.** Employ physical and technological safeguards such as providing access controls and logging incidents.

4. **Limit Mobile Access.** Limit the number of mobile devices that contain data and the number of people with access to them.

5. **Audit Your System.** Audit systems to understand your system's vulnerabilities and put in place a method to monitor for intrusions.

6. **Cyber Insurance.** Consider purchasing cyber insurance. These are separate policies that cover anticipated losses from a cyberattack. Typically, these cannot be added as a rider to existing insurance policies. The cost of a cyber insurance policy may depend upon the security measures that you establish to protect your data and may not be very expensive. It is worth a call to your insurance broker to inquire

about adding cyberattack insurance to your suite of insurance policies. Cyber insurance will cover the cost of paying for demanded ransom if necessary. More important, cyber insurance can cover the notification costs if a data breach occurs. These can be enormous, depending upon what you have to do under applicable data protection laws.

7. **Know Your Data Protection Laws.** Understand the data protection laws of your state. These will tell you what you have to do when a breach occurs. Forty-six states have in place data breach notification laws. We are not aware of any data protection laws that have been enacted by Tribes and it is unknown whether principles of sovereign immunity would protect a Tribe from litigation in the event of a data breach. The federal government has several additional privacy laws that may be implicated, but not usually if a broadcast station is hacked. Generally, these laws require a company to notify affected consumers by letter written in plain language that lists the type of information breached, and provides the name and contact information of the reporting business. Sometimes a company will have to report a data breach to its state Attorney General. Sometimes companies are required to pay for credit card monitoring companies as one remedy for consumers who have had their financial information hacked.

8. **Prevention.** The best practice of all is to prepare so as to avoid a breach in the first place. While insurance provides great protection, other intangible losses flow from data breaches, such as loss of listeners, damage of your reputation in the community, etc. So prevention, as always, is the best medicine.

If you have further questions about how to prevent and/or respond to a security breach contact Judy Endejan (jendejan@gsblaw.com).

**This article was written for the Native Public Media Summit in April 2016. It contains information of a general nature and should not be regarded as legal advice. The firm will be pleased to provide additional details and to discuss matters contained in this memo as they may apply in specific situations.*