

RISK COMMUNIQUÉ

Cyber Security – Data Breach Precautions

Public entities often handle a lot of personal information related to residents, businesses, organizations and other members in the community, as well as their own employees. Taxes, billing information, social security numbers, health information, human resources, arrests, public school/education, youth organizations and legal records are examples of electronic files that need to be secure and confidential.

Using electronic communications for business transactions and providing public services is increasing, however, so are data breach incidents. Data breaches can be the result of innocent errors, intentional staff maliciousness or outside hackers. Cyber risk typically involves the potential for loss, injury or other damages from an electronic exposure that could impact a public entity and the public customers they serve. Activities that create cyber risk include¹:

- E-commerce business Web sites
- Credit card data collection and online payment processing
- Data storage(online and traditional shipping of paper records or back-up tapes)
- Housing private customer data on laptops
- Business partners and contractors that touch customer data
- Providing online content or media
- Cloud and outsourced computing
- Social media sites (Facebook, MySpace, Twitter) that collect and display private information
- Human Resources Activities

Cyber Security Tips

There are several important steps that a public entity may take to help protect public and personal information. Here are 10 tips to help safeguard sensitive data²:

1. **Keep Only What You Need.** Reduce the volume of information you collect and retain to only what is necessary. Minimize the places you store personal data. Know what you keep and where you keep it.
2. **Safeguard Data.** Lock physical records in a secure location and restrict access to employees who need to retrieve private data. Consider employee background checks. It may be beneficial for vendors/contractors (who touch your systems or data) to undergo due diligence as to their own information security practices and to provide an insurance certificate that includes cyber liability coverage. Consider language in service contracts for defense and indemnity in the event of a mishap that impacts your data. Use language that specifies the contractor will notify you of any breach in a timely manner.

This is a sample guideline furnished to you by Glatfelter Public Practice. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your GPP Risk Control Representative. www.glatfelterpublicpractice.com

RISK COMMUNIQUÉ

3. **Destroy Before Disposal.** Cross-cut shred paper files before disposing of private information. Also destroy CDs, DVDs and other portable media. Deleting files or reformatting hard drives does not always erase data. Instead, using software designed to permanently wipe the drive or physically destroying the drive may be better options.
4. **Update Procedures.** Using Social Security numbers as employee IDs or client account numbers is not recommended. If you currently do so, consider an alternative ID system.
5. **Train Employees.** Establish a written policy about privacy and data security and communicate it to all employees. Educate them about what information is sensitive and their responsibilities to protect that data.
6. **Control Use of Computers.** Restrict employee use of computers to business. Consider blocking access to file sharing peer-to-peer Web sites, inappropriate Web sites and unapproved software.
7. **Secure All Computers.** Implement password protection with a condition to re-logout after a period of inactivity. Train employees to never leave laptops or PDAs unattended. Restrict teleworking to company-owned computers with non-generic passwords that are changed regularly and not shared by systems administrators.
8. **Keep Security Software Up-To-Date.** Keep security patches for your computers up-to-date and apply default settings on new servers. Firewalls and anti-virus software are beneficial.
9. **Encrypt Data Transmission.** Data encryptions may be an option to consider. Try to avoid using Wi-Fi networks as they may permit interception of data.
10. **Manage Use of Portable Media.** Portable media such as DVDs, CDs and USB flash drives, are susceptible to loss or theft. . Encrypting laptops if sensitive data is housed on the device is also an option.

If a data breach occurs, it is important that the public entity tries to quickly reduce the potential damage and reduce the flow and distribution of data. React immediately and carefully follow the breach incident response plan and determine the nature of the problem. Outside forensic computer investigators and a privacy lawyer (aka Breach Coach) could be beneficial to the organization. Some forensic service vendors also can assist with data recovery and restoration.

References:

- 1, 3. Business Insurance, White Paper, "Cyber Risks: How to protect your business in the Digital Age," 2010
2. Hartford Steam Boiler, Whistlestop Express, "Ten Ways Your Customers Can Help Prevent a Data Breach"

This is a sample guideline furnished to you by Glatfelter Public Practice. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your GPP Risk Control Representative. www.glatfelterpublicpractice.com