A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

RISK COMMUNIQUÉ

Glatfelter Commercial Ambulance SM
A Division of Glatfelter Insurance Group

Cyber Security - Data Breach Precautions

429 million identities were exposed due to data breaches in 2015. [1] The data stolen across breaches is more valuable than in previous years. Likewise, the impact of a data breach on an organization is much greater. While most breaches continue to be caused by criminal or malicious attacks, one of the biggest consequences to organizations that have experienced a data breach is the loss of their customers' trust.

Emergency Service Organizations often handle personal information related to residents, businesses and patients, as well as their own employees. Electronic files such as billing information, social security numbers, health information, human resource records, and legal records contain confidential information which must be secured. Electronic exposures that present a potential for loss, injury, or other damages are known as cyber risk, and can significantly impact an ESO and the customers they serve.

Activities that create cyber risk include: [2]

- Patient Care Reports and EMS billing activities
- Credit card data collection and online payment processing
- Data storage(online and traditional shipping of paper records or back-up tapes)
- Housing private patient data on laptops
- Business partners and contractors that touch customer data (3rd party billing)
- Providing online content or media
- Cloud and outsourced computing
- Social media sites (Facebook, LinkedIn, Instagram, Twitter) that collect and display private information
- Human Resources activities

Causes of data breach as identified in 2015 include: [1]

- 46% of data breaches were due to malicious attacks
- 22% of data breaches were due to information accidentally being made public
- 21% of data breaches were due to theft or loss of computers or drives
- 10% of data breaches were due to insider theft

Not all data breaches result in identities being exposed; however, the cause of the breach does impact the likelihood of this occurring. In 2015, 48% of data breaches where identities were also exposed were the result of data accidentally being made public. This could have been due to a company sharing data with the wrong people or a misconfigured website inadvertently making private records public. There was a much higher risk for identities being exposed when hackers or insider theft was the cause of the breach. Records for 2015 show that 52% of data breaches where identities were exposed were due to attackers. [1]

What are attackers looking for?

According to research by Symantec (2016), "The more details someone has about an individual, the easier it is to commit identity fraud. Criminals are targeting insurance, government, and healthcare organizations to get more complete profiles of individuals."

A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

RISK COMMUNIQUÉ

Glatfelter Commercial Ambulance SM
A Division of Glatfelter Insurance Group

The following is a ranked list of the information pursued among data breaches occurring in 2015. [1]

- Real names were the most commonly sought after piece of information – 74% of all data breaches
- Home addresses, birth dates, government IDs (such as SSNs), medical records, and financial information – 40 to 30%
- Email addresses, phone numbers, insurance information, and user names/passwords – 10 to 20%
- Credit card data is still a target but the black market value of this information is lower since credit card companies and card holders are quick to notice anomalous spending patterns and stolen card data and other financial information has a limited shelf life.

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 data: [3]

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.
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-logon after a period of inactivity. Train employees to never leave laptops or PDAs unattended. Restrict tele-working 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 ESO 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 ESO. Some forensic service vendors also can assist with data recovery and restoration.

[1] Symantec Corporation. (2016, April). *2016 Internet Security Threat Report.* Retrieved from https://www.symantec.com/security-center/threat-report

[2] Greisiger, M. (2010, December 16). Cyber Risks: How to Protect your Business in the Digital Age. *Business Insurance*. Retrieved from http://www.businessinsurance.com/article/99999999/WP05/101219943

[3] Hartford Steam Boiler. (2015). Protecting Your Small Business from a Data Breach [Web log post]. Retrieved from https://blog.hsb.com/2015/09/01/small-business-data-breach-protection/