Cyber Breach: a very real risk in healthcare

Imagine for a moment that you arrive to work and turn on your office computer only to realize that it has been infected by a virus. The virus has compromised the personal health and billing information of hundreds of clients. Not only this, but your staff's information has been compromised as well, including their social insurance numbers and banking information.

Or imagine that someone has broken into your car and stolen your laptop, containing information on your current and past clients, including their names, addresses, telephone numbers, and personal health information.

Or even this: At your client's request, you agree to fax a copy of their clinical record to a third party. Unfortunately, you enter the wrong fax number and the client's personal health information is faxed to someone else in error.

What do you do? What are your professional responsibilities and how do you respond to these breaches of privacy?

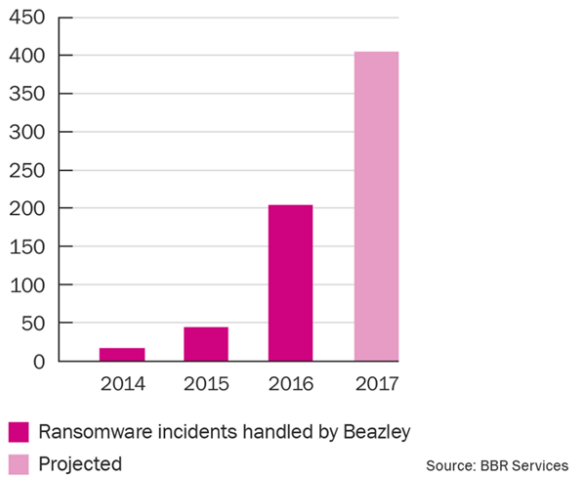
According to Beazley plc (Beazley)[1], a leading provider of data breach response insurance, unintended disclosure of records – such as a misdirected email – was the leading cause of data breaches in the healthcare industry in 2016 and 2017. At 41% of the total number of breaches reported to Beazley by organizations in the healthcare sector, the high level of unintended disclosure is unabated and remains more than double that of the second most frequent cause of loss, hacking or malware (19%). Hacking and malware (including cyber extortion) remained the most prevalent cause of data breach impacting all sectors at 34% of the total reported to Beazley in the first nine months of 2017.

Ransomware and cyber extortion on the rise in healthcare

Hackers are increasingly employing ransomware to lock up an organization's data, holding it until a ransom is paid in nearly untraceable Bitcoin. Hollywood Presbyterian Hospital in Los Angeles reported suffering a ransomware attack in February 2016 and ultimately paid the hackers $17,000 in Bitcoin. A year earlier, the FBI had issued an alert warning that ransomware attacks were on the rise.

This trend is borne out by Beazley's data. Breaches involving ransomware among Beazley clients more than quadrupled to over 200 in 2016 and the trend accelerated in 2017.

Ransomware attacks handled by Beazley



"Clearly, new malware programs, including ransomware, are having a big impact," said Paul Nikhinson, privacy breach response services manager for BBR Services. "Healthcare is a big target for hackers because of the richness of medical records for identity theft and other crimes," Nikhinson added. " In fact, a medical record is worth over 16 times more than a credit card record."[2]

What are your responsibilities when faced with a Cyber Breach?

As a healthcare provider, you are responsible for safeguarding the confidentiality and integrity of your client's personal, medical, and financial information while it is under your custody and control. These safeguards must be physical (e.g. locked filing cabinets), organizational (e.g. policies, security clearances) and technological (e.g. encryption, password protection). If client information has been lost, stolen, or otherwise accessed by unauthorized persons, you may also be responsible for notifying the privacy oversight body (for instance, the provincial Information and Privacy Commissioner) and/or regulatory body.[3] You should also familiarize yourself with any workplace policies and procedures that relate to privacy breach, including topics like privacy training, access management, privacy breach management, and discipline.

What are the Potential Costs of a Cyber Breach?

If you have been involved in a cyber breach, your client may look to hold you legally responsible for the financial damage and emotional harm they suffer when personal health and/or billing information is inappropriately disclosed. In addition to compensating your client for these damages, you will also likely accrue other costs. These costs can include those related to hiring a computer security expert to determine the cause of the electronic data breach; notifying individuals whose information may have been breached; costs related to mitigating reputational damage; and defence costs or penalties related to breach of the Privacy Law.

The average cost of a cyber breach in healthcare has been estimated at $359 (US) per record; the highest cost of all industry classes.[4] When this is multiplied by the dozens or hundreds of client records that could be accessed from your USB stick, computer, or office database, for example, the costs quickly add up and can be crippling for the average psychologist.

When faced with this emerging risk, Cyber Security and Privacy Liability insurance can be of significant help.

As a participant in the CPA/CPAP insurance program, you have some coverage through your professional liability insurance policy; namely $50,000 each of Cyber Liability and Privacy Event coverage. This means that you already have some protection for claims arising out of lost or compromised client information.

However, a data breach can be expensive and can potentially cost you hundreds of thousands of dollars. To better protect you, CPA and CPAP members are also able to access an additional, comprehensive Cyber Security and Privacy Liability offering designed specifically for healthcare professionals to help you manage the risk of holding increasingly large quantities of personally identifiable data of clients, employees, and others, and to mitigate the reputational damage resulting from a data security breach. This optional coverage is offered in partnership with BMS Canada Risk Services Ltd. (BMS Group), and is underwritten by Beazley plc (Beazley).

What protection does additional Cyber Security and Privacy Liability Insurance offer?

The optional Cyber Security and Privacy Liability insurance policy includes coverage for the following:

- $1 million aggregate limit
- Payment of damages to a third party, including coverage for your legal expenses;
- Costs associated with investigation into the cause of the breach;
- Costs involved to notify individuals affected by the breach;
- Costs to recover or replace compromised data;
- Ransom payments to recover encrypted data;
- Costs for business interruption due to cyber breach;
- Specialized breach response team including computer experts, legal services, notification services and breach mitigation;
- Costs associated with crisis management and public relations; and
- Coverage for regulatory defence costs and penalties resulting from a violation of a Privacy Law.

Risk management strategies to help protect your data
Attacks often succeed by exploiting misconfigured systems or human error, such as luring employees to respond to phishing e-mails.

In addition to securing appropriate insurance coverage, here are five steps healthcare businesses can take to help protect your data:

1. Train employees to be aware of the information they need to protect, educate them about best practices, principles and standards relating to privacy and confidentiality – and how to avoid falling for phishing attacks and other forms of social engineering.[5]

2. Review supplier contracts carefully to ensure that your clients' data is well protected when it is in the hands of suppliers or vendors.

3. Develop a robust incident response plan. Data breaches cannot be well handled on the fly. Advance planning can help avert serious reputational or financial harm. A well thought out and practiced incident response plan should guide management through the life cycle of a breach - from the initial suspicion that something is amiss to full-blown forensic analysis, legal advice, customer communications and public relations assistance.[6]

4. Categorize potential data risks by threat level. Over-reacting to a breach can be as damaging as under-reacting. [7]

5. Encrypt data and enable wiping of data (remotely where possible), particularly on mobile devices, laptops, and thumb drives, which are most likely to be lost or stolen.[8]

For more information on cyber risk or to purchase Cyber Security and Privacy Liability insurance, please contact BMS Group at 1-855-318-6038 or psy.insurance@bmsgroup.com.

References:

1. Beazley report July 2017. https://www.beazley.com/news/2017/beazley_breach_insights_october_2017.html
2. Beazley report March 2016. https://www.beazley.com/news/2016/beazley_breach_insights_2016_shows_sharp_increase_in_hacking_and_malware.html
3. For further information on Federal and Provincial privacy legislation and associated standards of practice, please contact your regulatory college. The Office of the Privacy Commissioner of Canada also provides resources for individuals and organizations, including a privacy breach checklist, handbook and information on steps to take in responding to a privacy breach: https://www.priv.gc.ca.
4. Ponemon Institute 2014 Cost of Data Breach Study http://ponemon.org
5. Resource: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf
6. Resource: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan
7. Resource: https://www.securestate.com/blog/2012/04/03/data-classification-why-is-it-important-for-information-security
8. Resource: https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/PublicSectorBenelux/deciphering-the-code-a-simple-guide-to-encryption-wpna-(2).pdf?la=en