Healthcare Special Edition

All organizations face the reality that data breaches have become inevitable. And the stakes are high: you hold personal data in trust for your customers, employees and patients. The volume of protected health information (PHI) maintained by healthcare organizations and the digitization of electronic health records have increased potential vulnerability for large data breaches. It is important to understand the underlying causes so as to mitigate and manage them effectively.

Beazley is a pioneer in the provision of data breach insurance and response services. Since the launch of Beazley Breach Response (BBR) in 2009, Beazley has managed over 4,000 data breaches for organizations in the healthcare sector, giving us an unrivalled view of the causes of breaches and evolving trends.

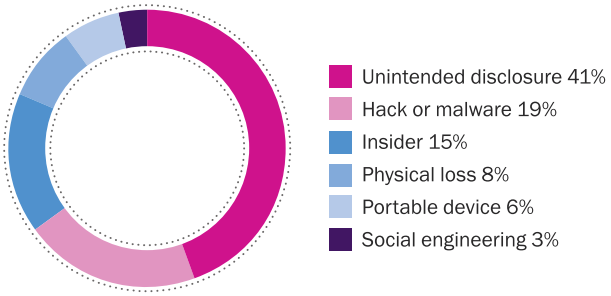
In this special report, we highlight issues currently trending in the healthcare sector.

Katherine Keefe
Global Head of Beazley Breach Response Services

Data breach trends

Beazley's quarterly Breach Insights report examines the major causes of data breaches reported by insureds across a range of industries. The chart below shows the causes of data breaches reported by healthcare insureds in the first nine months of 2017:

Causes of data breach in healthcare sector reported to Beazley Q1-Q3 2017



Unintended disclosure remains the highest cause of data breach

Unintended disclosure accounted for 41% of healthcare incidents reported to Beazley and shows no signs of abating. The high level of unintended disclosure incidents remains more than double that of the second most frequent cause of loss, hack or malware (19%). Whether it's an email containing PHI sent to the wrong recipient, discharge instructions given to the wrong patient, or a server containing PHI accidentally left open to the public, healthcare entities continue to struggle with human error on a regular basis.

Unintended disclosure incidents are a persistent threat and expose organizations to greater risks of regulatory sanctions and financial penalties. Yet they can be much more easily controlled and mitigated than external threats. We urge organizations not to ignore this significant risk and to invest time and resources towards employee training.

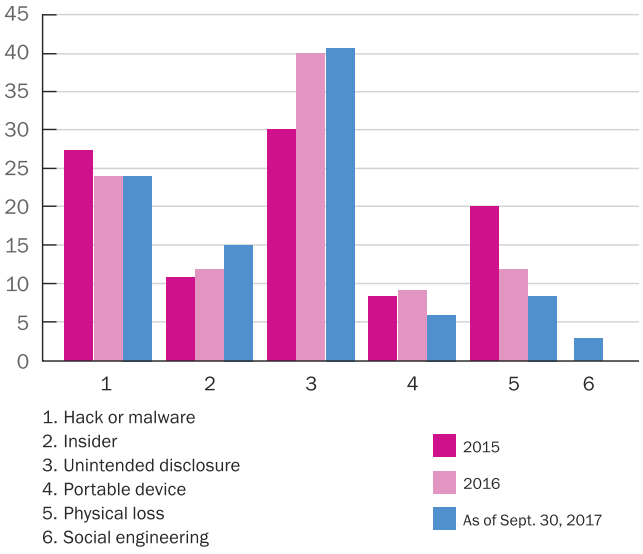
Insider and social engineering incidents on the increase

Healthcare insureds have also reported more insider incidents thus far in 2017. Insider incidents accounted for 12% of healthcare incidents in 2016, yet by the end of the third quarter of 2017, that percentage has increased to 15%. Typically insider incidents involve an employee viewing patient records without a work-related reason to do so, perhaps looking at a celebrity patient's record or the record of an ex-spouse or neighbor. These "employee snooping" incidents are usually discovered by audits run on the electronic medical records system or by another employee or patient reporting the suspected snooping. It is unclear what has led to the increase in insider incidents in healthcare, but what is clear is that increased employee vigilance and auditing will help organizations identify such behavior early on, reducing the number of affected patients and hopefully lessening the likelihood of regulatory inquiry.

Another noticeable trend across industries in 2017 is the nine-fold increase in social engineering attacks. A social engineering attack occurs when a hacker uses deception to manipulate individuals into divulging confidential or personal information. The two most prevalent types of social engineering attacks reported to Beazley are fraudulent instruction incidents and W-2 scams. Fraudulent instruction is a variant of business email compromise (BEC), in which a fraudster impersonates a trusted party such as a company executive, a payment system vendor, or a participant in a real estate transaction. The fraudster then provides fraudulent payment instructions to divert a planned payment or to cause a fraudulent payment to be made. If successful, the fraudster profits more quickly than by stealing data and selling it on the dark web or exploiting it by filing fraudulent tax returns. Social engineering can be quicker, easier and cheaper to implement for cybercriminals than stealing data and can be much more lucrative.

Organizations can combat social engineering attacks by training employees to better recognize phishing emails, encouraging that wire transfer requests be verified by phone if new bank account information is provided, and implementing two-factor authentication to prevent unauthorized users from using stolen credentials to log into email remotely.

2015-2017 Healthcare data breaches by cause reported to Beazley



Office for Civil Rights (OCR) stepping up its enforcement activities

There has been a marked increase in the Department of Health and Human Services OCR's enforcement activities in recent years. When a Health Insurance Portability and Accountability Act (HIPAA) covered entity or business associate reports a breach to OCR involving over 500 patients, OCR automatically opens an investigation (though OCR also reserves the right to open investigations on reported incidents involving less than 500 patients). A small though steadily increasing number of these investigations result in a resolution agreement, which includes a corrective action plan and a settlement amount.

The trend

As the number of investigations and resolution agreements have increased, so too has the average settlement payment. The combined total of 13 resolution agreements in 2014 and 2015 saw settlement amounts ranging from $125K to $3.5M (an approximate average of $1M each). In 2016, there were about 13 resolution agreements and so far in 2017 there have been nine. The 2016 and 2017 resolution agreement settlements range from $31K to $5.5M (an average of $1.8M each).

Why the increase?

Two reasons for the increase in enforcement activities and resolution agreement settlement amounts are likely: that OCR has more resources at its disposal and has far less patience for HIPAA non-compliance. Settlement payments from resolution agreements are funnelled back into OCR allowing OCR to pursue enforcement initiatives and increase staffing at regional offices. OCR representatives have also expressed frustration at entities' failure to comply with HIPAA's privacy and security rules, which have been on the books since 2003 and 2005, respectively. Hot button issues for OCR include failing to encrypt portable devices, conduct security risk assessments, and enter into business associate agreements with vendors holding protected health information.

Key takeaways

Organizations need to be aware that when they report a breach, it opens the door for OCR to investigate the entity's basic HIPAA compliance. The investigation in turn can lead to corrective action plans and settlements. And organizations should not expect a quick resolution; typically it takes 3-6 years from the time the breach was first reported to OCR to resolution, imposing a long-term drain on managerial resources as well as finances.

But with the increase in OCR's resolution agreements, a trend of OCR's hot button issues has emerged. Organizations should review previous resolution agreements (all of which are available on OCR's website) and familiarize themselves with what OCR considers to be best practices, such as:

- Device encryption
- Workforce education and training
- Updating of policies and procedures
- The elimination of old data
- Security risk assessments
- Risk mitigation plans
- Vendor management
- Using the minimum amount of PHI.

Healthcare claims examples

Below are a number of examples that we have handled for healthcare clients to demonstrate the variety of events that can lead to a data breach.

Phishing attack

A healthcare organization experienced a foreign phishing attack which exposed information in employee email boxes of nearly 20,000 pediatric patients. Employees had clicked on the phishing emails and either gave up credentials or launched malware into the network.

BBR Services coordinated a response which included legal assistance and a forensics investigation. The forensic firm found some evidence of data exfiltration. The data contained patients' names, clinical information, phone number, addresses, insurance information and some social security numbers. Unable to determine the extent of the exfiltration, the organization notified all potentially impacted patients. BBR Services also lined up a notification and call center services vendor as well as credit monitoring. OCR opened an investigation, which has since been closed.

Vendor breach

An IT vendor had inadvertently unsecured a file containing over 30,000 patients' billing information such that it was searchable on the internet using search engines. The hospital discovered the incident during security testing when a larger healthcare system acquired the hospital. The information exposed included names, social security numbers, dates of birth, addresses, treatment information, and insurance information.

BBR Services set the hospital up with privacy counsel and a forensic firm. Because the forensic firm could not rule out that unauthorized users viewed the patient information, BBR Services lined up notification services, a call center, credit monitoring and crisis management. The hospital was investigated by OCR and four attorneys general.

CBSL522_US_10/17

Unencrypted devices

A large health system lost unencrypted backup tapes that contained over 1 million pediatric patients' billing information including names, date of births, social security numbers, diagnosis codes and health insurance information. The tapes also included employees, physicians and vendors information totalling 200,000 individuals. The tapes were believed to have been lost during a remodeling project in the IT department.

BBR Services coordinated the response, which included use of legal, forensics, notification and call center services, credit monitoring, and crisis management. There was an OCR investigation that lasted over three years and was ultimately dismissed.

The Beazley Breach Response Services team

The BBR Services team focuses on the coordination of the expert forensic, legal, notification and credit monitoring services that insureds need to satisfy all legal requirements and maintain customer confidence. We also, indemnify your losses from lawsuits or regulatory actions, the risk of which may be reduced by a well-coordinated breach response but can never be completely eliminated. In addition to coordinating data breach response, BBR Services is responsible for maintaining and developing Beazley's suite of risk management services, designed to minimize the risk of a data breach occurring.

As a result we can help prevent an incident from becoming an existential threat, limit damages and reduce recovery times and give comfort to regulators, customers and the public.

Beazley invented this comprehensive approach. We do more of it than anybody else. To date we have helped insureds manage more than 7,000 data breaches swiftly and successfully. We can't guarantee your cyber security or prevent cybercrime. But we can put you in control of your response.

To find out more about our services and how we can help your organization, visit www.beazley.com/bbr

beazley

www.beazley.com/bbr