The Anatomy of a Data Breach
What Your Clients Need to Know

Warren Kruse, MSc, CISSP, CFCE, EnCE, DFCP
Vice President of Data Forensics
Since 2009, the U.S. Department of Health and Human Services has cataloged more than 1,600 reports of data breaches in the healthcare sector involving 500 or more comprehensive patient medical records – and those were only the incidents that affected U.S.-based entities. In the UK, data loss and poor security are, incredibly, so profound an issue that their healthcare sector has won the dubious distinction of being named “the leakiest industry.”

In a recent blog post on altep.com, I examined some of the reasons healthcare is a favorite target of cyber criminals – a topic that is peripheral to the focus of this article. Nearly ninety percent of healthcare organizations surveyed suffered data breaches. News reports appear regularly (notable incidents have included those at Massachusetts General Hospital, Catholic Healthcare Services, and a recent breach at Banner Health in Phoenix – the largest data loss of 2016) and describe loss of PHI via a wide array of attack vectors. Estimated costs exceed $6.2 billion, and the list of potential areas of vulnerability your clients may be facing is astonishing, ranging from third-party partners to mobile devices (as in the CHS case), to unauthorized access by departed employees, and even the technologies and equipment used to provide services in the ordinary course of business.

Altep’s cyber security services team has first-hand experience with these situations. Most recently, we assisted with a complex breach involving hundreds of thousands of medical records which were compromised due to the inadequate security measures of a third-party service provider. Ultimately, several vulnerabilities were discovered and addressed. The client received ransom demands, records were listed for sale on the dark net, and law enforcement and insurance involvement were triggered. Of course, regulatory inquiries and litigation will soon commence. Even though their network is now secure and rigorous new protocols have been put in place, the client will be dealing with the after-effects, both operationally and reputationally, for years. It’s the stuff of nightmares, not only for the organization’s IT staff, administrators, and counsel, but for their patients as well.

In working with our clients, I’m often asked to explain how organizations can lessen the likelihood of a data breach. Inevitably the conversation leads to specifics – it’s hard to outline proactive measures without talking about the who, what, when, and how, so I’ve summarized those factors below.

Generally, when breaches occur, the media focuses on the number of records lost and the potential financial impact. Occasionally, experts examine the hidden costs, such as increased insurance premiums, loss of trust and privileges at insurance providers, and reputational damage. Sometimes the method of attack and the data sources that were compromised are explained; however, specific activities and events that took place during the key stages are rarely discussed in detail. Every situation is different, but a clear sense of what will likely occur, and a functional vocabulary to call upon during discussions with the response team are critical to ensuring that decision makers respond effectively, and that counsel can provide their clients with appropriate guidance regarding preparedness, potential exposure, and legal and operational obligations.
Typically, the data breach and subsequent activities occur in these stages:
1. Compromise
2. Awareness
3. Assessment
4. Recovery
5. Remediation and Notification

Initially, systems are compromised: hackers gain access to one or more servers or computers via one or more vectors of attack, such as a vulnerability, or security flaw in a software application or in the configuration of a network or firewall. Once the intruder is in, his goal is to maximize both dwell time, the amount of time he can go undetected and continue with his activities, and range, the number and variety of systems and data sources he can control.

Eventually, the organization becomes aware that systems have been compromised – in some cases, the hacker demands a ransom in return for stolen data, while in others, a routine security assessment or an observant user uncovers evidence of unauthorized use. Once the organization realizes that a breach has occurred, assessment is critical. How did the attacker gain access, and how far did his reach extend? What other vulnerabilities exist? What kinds of data were lost? How long was the attacker’s dwell time? The answers to these and other questions will determine the steps which need to be taken next.

During recovery, the response team addresses system, software, and network vulnerabilities with three primary goals: regaining control of all affected systems, preventing the hacker from accessing them again, and preventing future hacking attempts from succeeding. These efforts may include temporarily taking systems offline or bringing them down entirely, upgrading and/or reconfiguring network routers, switches, and firewalls, installing software upgrades and security patches, resetting user and administrator passwords, and setting up Privileged Access Management (PAM) – an approach by which system administrator permissions are enabled on a task-by-task basis, and expire after a specified period of time so that hackers can’t gain control of them.

Of course, the organization’s daily operations will likely be affected by both the hacker’s activities and recovery efforts, so establishing and maintaining timely, calm, and authoritative communication between leadership and staff is critical.

Once the response team has regained control of affected systems, the remediation and notification stages can begin. These often occur simultaneously, and are usually handled by two different groups: either the initial response team or a second group of remediation specialists and, of course, counsel.
During remediation, the team reviews all of the findings that were gathered during recovery, prepares a detailed remediation report to document specific tasks and actions that should be taken, and then performs those tasks to further correct vulnerabilities and strengthen defenses. Simultaneously, the notification team will assess the organization’s obligations, evaluating the types of data that were lost, determining which jurisdictions were involved, reviewing the various notification requirements, and preparing and sending appropriate notices to individuals whose PHI was stolen or compromised.

An Ounce of Prevention is Worth a Pound of Cure

Following are some of the immediate questions you should be asking regarding the security measures surrounding your clients’ enterprises. If the answers are in any way sub-par, an Information System Security Audit, performed by a reputable, objective team of specialists, may be critical and immediately necessary. Importantly, clients successfully completing these audits can improve their chance of obtaining reasonably priced cyber coverage - many organizations assume their liability policies will cover cyber incidents when in fact, they do not.

- What kinds of passwords are required? How often must they be changed?
- Are user accounts and permissions reviewed on a regular basis? Are accounts belonging to departed employees disabled as soon as the employee exits?
- Are export features in software applications permission-based? Which users are allowed to export patient information from databases? Can entire records be exported, or are exports limited to partial records?
- Do servers log all access and user activities? Where are the logs stored?
- Is remote access allowed? To whom, and by what means? Is two-factor authentication enabled?
- Are third parties involved in the organization’s daily operations? How? What measures are in place to assess their security practices? Could a third party’s lack of security create exposure for your client?
- Does the client have at least one well-qualified individual who is dedicated to information security? If not, does the client employ a third party managed security service provider to assess security and provide recommendations?
- How is access inside the network controlled? Do users have unlimited access to all resources, or is access determined on a need-to-use basis?
- Are mobile devices allowed? Are they provided and secured by the organization, or are employees allowed to bring their own devices? If so, are they secured? How?
- Are network penetration tests and information security audits performed on a regular basis? What are the results? Who is performing them?
- What policies govern the use of information technology? Access to data? Are the policies reviewed on a regular basis and kept up to date?
- Is there an incident response plan? Is it up to date? Has it been communicated to all employees?
- Does the organization have cyber liability insurance?
Conclusion

Due to the valuable nature of the information they control, healthcare organizations are at high risk for data theft. To guard against cyber attack, they must regularly scrutinize their security measures, data storage practices, and system access provisioning. In the event of a breach, they must be prepared to act swiftly to minimize the damage to the organization and, more importantly, the patients with whose care they were entrusted. Counsel can and should have an integral role in this effort by ensuring that their clients' leaders and decision makers are properly informed about the implications of an inadequate information security posture, and well aware of the advisability of enlisting third party experts to assist in safeguarding their valuable PHI.
[i] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf  
About the Author

Warren G. Kruse II, MSc, CISSP, CFCE, EnCE, DFCP
Vice President, Data Forensics,
Altep, Inc. - An Advanced Discovery Company
wkruse@altep.com
@warren_kruse

With more than 30 years' experience in law enforcement and forensic science, Warren is the author of “Computer Forensics: Incident Response Essentials.” The diverse range of matters Warren has assisted with includes theft of trade secrets, WikiLeaks investigations, misappropriation of intellectual property, breach of contract, internal employment disputes, fraud investigations, and wage and hour class actions, among others. Warren previously served as the President of the Digital Forensics Certification Board.
DECADES OF EXPERIENCE. PROVEN TECHNOLOGIES. UNSURPASSED SERVICE.

CONSULTING
- Litigation Readiness
- 30(b)(6) Witnesses
- Subject Matter Experts
- eDiscovery Liaisons
- Compliance Risk Assessment

DATA FORENSICS
- High Tech Investigations
- BYOD Strategy
- Expert Testimony
- Standard & Non-Standard Data Acquisition
- Incident Response

CYBER SECURITY
- Computer System Security Analysis
- Penetration Testing
- Data Incident Investigation
- Data Breach Notification
- Data Privacy

DISCOVERY
- Collection
- Early Data Assessment
- Electronic Data Discovery
- Paper Discovery
- Secure Hosting and Review
  ESI Vault®

To learn more about our certifications visit us at https://altep.com/about-us/certifications

For a list of our locations visit us at https://altep.com/contact-us#locations

@Altep_Inc. Altep, Inc.

www.altep.com • (800) 263-0940
© 2016 Altep, Inc. - All Rights Reserved

For more articles, visit www.altep.com/articles