CapSpecialty
A Community of Insurance Specialists

ARTICLE

We've Got One Word For You: E-N-C-R-Y-P-T-I-O-N

News about data breaches inundates us weekly and, sometimes, daily. The potential release of sensitive data (secure patient, customer, employee and business information) to an untrusted environment as a result of cyber attacks, insider criminal activity, technological malfunctions or employee negligence is a huge concern for every organization responsible for protecting this information. Additionally, the threats are increasing as more sensitive data is being digitized and transmitted electronically and the use of mobile devices and public cloud services grows. Planning, implementation and maintenance of a comprehensive data security plan is required to guard against current and future threats. One critical element of any data security plan that is too often neglected or delayed is encryption.

Every organization and business, large or small, that creates, maintains or transmits sensitive information in an electronic format (and that includes just about every organization that you can think of – private companies, government agencies, and nonprofits) must appreciate the protections that are provided by encryption. Why? Because organizations and businesses are responsible for protecting sensitive information in accordance with applicable federal and state laws, industry standards and good business practices. Organizations can face significant costs, penalties and/or legal liabilities as result of a data breach.

ENCRYPTION IS A "SAFE HARBOR"

It is difficult to overstate the importance of encryption in protecting data. Forty-seven U.S. states currently have security breach notification laws that require notification to individuals whose sensitive information has been compromised by private or government entities. However, many of these laws provide for an exemption or "safe harbor" from such reporting requirements if the data was properly encrypted ("Security Breach Notification Laws." National Conference of State Legislatures (NCSL). 12 Jan. 2015. Web. 27 Jan. 2015. <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>). California is one such state which provides a safe harbor provision to its data breach notification law, if the organization that was breached can prove that the data was appropriately encrypted. A key finding from California's State Attorney General's Data Breach Report 2012 stated, "[m]ore than 1.4 million Californians would not have been put at risk, and 28 percent of the data breaches would not have required notification, if the data had been encrypted" <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf>.

Additionally, under the Health Insurance Portability and Accountability Act (HIPAA), a covered entity(CE), as defined by the law, must report "unsecured" breaches of protected health information (PHI) to affected individuals, the U.S. Department of Health and Human Services (HHS) and, in some cases, to the media. However, if the data is encrypted, reporting a breach is not required because properly encrypted data is not considered "unsecured". Encryption provides a safe harbor. (Eisen, Judith and Gulick,Stacey. "What is a Breach Under the HITECH Breach Notification Regulations?" ABA Health eSource. American Bar Association. May 2012, Vol. 8, Number 9. Web. 27 Jan. 2015. <http://www.americanbar.org/newsletter/publications/aba_health_esource_home/aba_health_law_esource_0512_eisen.html>; <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>).

Encryption - is the conversion of data into a form that cannot be read without the decryption key or password <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>.

Key - a piece of data used to encrypt data (scramble text to make it unreadable) and decrypt (unscramble, convert to readable text). To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt <http://www.healthit.gov/providers-professionals/2-install-and-enable-encryption>.

The goal of encryption is to protect data from being accessed and viewed by unauthorized viewers. Every business and organization should consider how encryption fits into their overall data security risk assessment and plan. Unfortunately, this message is not always being heeded: *proper encryption makes data unreadable and unusable even if it is lost or falls into the wrong hands.*

STATISTICS AND CASES

- Many data breaches happen at small and medium-sized businesses ("2013 Data Breach Investigations Report." Verizon. 2013. Web. 27 Jan. 2015 <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf>). Data breaches at large companies make front page news stories, but businesses and organizations of all sizes are susceptible to breaches.

- A 2012 joint survey by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association gathered data from 450 compliance and ethics professionals in their membership databases about data breaches experienced by their companies. A wide range of industries were represented and the survey stated that, "60% of the respondents' organizations had suffered an incident in the last year". In this survey, "lost device[s] such as a memory stick" and "lost paper files" accounted for 65% of the breaches. (Society of Corporate Compliance and Ethics and Health Care Compliance Association. "Data Breach Investigations Report." Society of Corporate Compliance and Ethics. 17 Jan. 2013. Web. 27 Jan. 2015 <http://www.corporatecompliance.org/Resources/View/ArticleId/881/Data-Breach-Incidents-Responses.aspx>).

- *Information Exposed: Historical Examination of Data Breaches in New York State*, a report from the Office of the New York Attorney General that analyzed data breaches that occurred between 2006 and 2013, concluded, "The trend is clear: Data security is a serious challenge for organizations of all kinds," citing the diversity of organizations in size and type that reported breaches. Retailers and healthcare providers were found to be particularly at risk for data breaches in the report <http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf>.

- One report analyzing data breaches that had been reported to HHS found that, in 2013, 83.2% of the total patient records breached were due to theft, and 35% of the overall breach incidents involving protected health information were the result of the loss or theft of unencrypted mobile devices ("Breach Report 2013: Protected Health Information (PHI)." Redspin, Inc.Feb. 2014. Web. 27 Jan. 2015. <https://www.redspin.com/resources/whitepapers-datasheets/Request-2013-Breach-Report-Protected-Health-Information-PHI-Redspin.php>).

- A private dermatology practice located in Massachusetts entered into a reported settlement for $150,000 with HHS for potential violations of HIPAA after an unencrypted thumb drive containing electronic protected health information was stolen from an employee's car and was not recovered <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/apderm-agreement.html>.

- An unencrypted laptop stolen from a Concentra Health Services facility resulted in a $1.7 million settlement of potential violations of HIPAA. Concentra had started the encryption process, but HHS found its efforts were inconsistent and incomplete. QCA Health Plan, Inc. reported to HHS that an unencrypted laptop containing protected patient health information was stolen from an employee's car resulting in a $250,000 settlement for potential violations of HIPAA <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html>.

- HHS, through the press release about the two breaches above, stated: "Covered entities and business associates must understand that mobile device security is their obligation. Our message to these organizations is simple: encryption is your best defense against these incidents" <http://www.hhs.gov/news/press/2014pres/04/20140422b.html>.

PROTECTING PERSONALLY IDENTIFIABLE INFORMATION

Below are some things to keep in mind as you work on incorporating encryption into your overall security data breach plan.

Know The Rules

Find out what data security and data breach requirements apply to your organization. Many state data breach notification laws require private and government entities to report data breaches to the state and notify individuals whose personally identifiable information has been compromised. Each state has its own requirements about what triggers a report, whether notice must be given to the State Attorney General, whether a breach of paper records as well as electronic data triggers notification requirements, deadlines for notifications, whether encryption provides a safe harbor, etc.

Under Federal law, covered entities (CEs) and business associates (BAs), as defined by HIPAA, must comply with the HIPAA Privacy Rule, Security Rule and the Breach Notification Rule . They are subject to the penalties and fines under the Enforcement Rule for non-compliance. Covered entities are health care providers (if they electronically transmit specific transactions with health plans for which HHS has developed standards), health plans, and health care clearinghouses. For more information, including a question and answer decision tool to determine if you are a CE or BA, see <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities>.

Many businesses may not even realize that they are BAs, and are directly subject to the HIPAA Security Rule and portions of the Privacy Rule. Some may think that they are not BAs because they are not healthcare providers. However, a BA is an entity that is performing a service or functions on behalf of a CE and has access to patients' protected health information. Entities that can potentially be considered a BA under HIPAA include: a billing service, transcription service, consultant, accountant, lawyer, answering service, cloud provider, medical record storage company, and others <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities>. It is essential to evaluate whether your organization is a BA and, therefore, must be in compliance with HIPAA requirements to avoid potential liabilities for HIPAA violations. HHS has information available to help organizations make that determination (see Resources), however, these organizations should probably also consult an attorney to determine their status under HIPAA.

CEs and BAs must do security risk assessments and put a risk management plan in place to prevent data breaches, including planning for encryption needs. In addition to complying with the Federal HIPAA law, CEs and BAs are subject to state laws, which could provide even more stringent notification deadlines and/or additional requirements.

Please be aware that other industry-specific federal laws, industry standards and/or good business practices could impact your particular organization. Organizations need to ask the following questions:

- Is your organization subject to industry specific federal laws/rules that include explicit safeguards for customer information, e.g., financial institutions under Gramm-Leach-Bliley ACT and the FTC Safeguards Rule <http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>.

- Is your organization following good business practices that set a standard of best practices in the industry for securing customer information? In the event of a breach, your practices for securing personally identifiable information will be judged in relation to standards in the industry. Falling short of those standards can increase your losses as well as put customers' information at risk for things like credit card fraud and identity theft, to name a few. (E.g., payment card industry data security standards for payment cards, "pci Security Standards Council." n.d. PCI Security Standards Council, LLC. Web. 27 Jan. 2015 <https://www.pcisecuritystandards.org/>).

- Data security is a highly technical and regulated area; do not go it alone. Get professional advice from IT security experts and legal counsel, as necessary, to make sure any encryption method used is appropriate for the problem you are trying to prevent or solve and it fits into the organization's overall data security plan for the type of data to be encrypted, e.g., encryption for data at rest or data in motion.

THE REAL COST OF A DATA BREACH

It is understandable that organizations worry about the resources (including financial) required for data security planning, including encryption. The cost and effort required to encrypt data depends on the type of data and device involved, as well as how it fits into the overall data security plan. Encryption capability that meets the requisite standards may be available without charge or may need IT skills to set up. A risk assessment and data breach security plan will provide answers about what is needed. However, the real cost of a data breach, compared with putting adequate security in place, may be unanticipated and not considered by most businesses. The costs of notifying all the individuals involved, providing credit monitoring, and analyzing the causes of the breach to remedy the problem are just a few of the issues that contribute to the overall cost burden for the organization, and post-breach costs are increasing. Other costs, depending on the type and circumstances of a breach include, but are not limited to:

- Lost sales
- Lost staff time due to dealing with data breach issues
- Crisis management, public relations services
- Attorney services
- Payment of penalties
- Legal defense
- Legal settlement
- Data recovery services
- Cost of unavailability of crucial data for business operations
- Reputation damage costs (hard to quantify but seen, for example, in turnover of clients requiring increased efforts to attract new customers and win back previous customers)

PREVENTION AND PROTECTION ARE KEY

Organizations must do the ongoing work of performing a security risk assessment and implementing a data breach prevention plan to protect sensitive information. Encryption is an essential part of such a prevention plan. Encryption may not only be needed to protect data on laptops and other mobile devices, but, depending on your data security assessment of where and how sensitive data is transmitted or maintained, also for email, PC's, servers, etc.

However, even with the most diligent attention to prevention, all breaches may not be prevented and new threats to data security will emerge. Protection afforded by cyber security and privacy insurance coverage can help organizations limit the loss impact from a potential breach.

RESOURCES

HIPAA

For covered entities and business associates, as defined by HIPAA, HHS has provided specific guidance about encryption as part of an overall data security plan:

The U.S. Department of Health and Human Resources, Office of Civil Rights, Guidance to Render Secured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (provides links to the encryption processes that have been tested by the National Institute of Standards and Technology (NIST) and judged to meet the HIPAA Security Rule standards for data at rest and data in motion <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>.

HIPAA Security Rule Guidance Material (includes a list of many resources, with links) <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>.

Tips to Protect and Secure Health Information: Install and enable encryption (includes links to the NIST Special Publications regarding encryption processes that can help meet HIPAA standards; also links to other information about mobile device privacy and security) <http://healthit.gov/providers-professionals/2-install-and-enable-encryption>.

HIPAA Security Series, 4. Security Standards: Technical Safeguards <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>

State Breach Notification Laws

National Conference of State Legislatures <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

California's State Attorney General's Data Breach Report 2012 <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf>

Massachusetts' Office of the Attorney General - Guidance for Businesses on Security Breaches <http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/security-breaches.html>

Office of New York State Attorney General Information Exposed: Historical Examination of Data Breaches in New York State <http://www.ag.ny.gov/pdfs/data_breach_report071414.pdf>

Federal Trade Commission Guidance – Safeguards Rule, Gramm-Leach-Bliley <http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>