INFOSEC

ADVISORY BULLETIN

Second Quarter 2017

Encryption and Safeguarding Your Data

What is encryption?

Encryption is the method of protecting data from being accessed by an unauthorized party putting our customers and partner's privacy in jeopardy. As an example, if you have customer data not encrypted on a laptop and the laptop is stolen, the data can be recovered and accessed by unauthorized person. If the data were encrypted, the data would be protected from being accessed ensuring privacy for our customers and partners.

There are many types of encryption but the basic principle remains the same, data is encrypted with an algorithm rendering data only readable when a decryption algorithm is available. This keeps the data stored or transmitted in an unreadable format so that unauthorized parties are not able to access and use the data.

Why should you encrypt data?

In today's world of identity theft and cyber criminals using data against us, we owe it to our customers and partners to ensure non-public and sensitive data does not fall into the hands of an unauthorized party.

Also, in the business vertical of insurance and finance there is oversight from state and national groups. In some cases, this oversight documents detailed guidelines on requirements for information and cyber security practices to protect customers and partners. The requirements, from the date and national groups identify certain types of data that require protection by data encryption.

AMERICAN LAND TITLE ASSOCIATION
1800 M ST NW, SUITE 300S
WASHINGTON, DC 20036
P. 202.296.3671 | F. 202.223.5843
WWW,ALTA,ORG | SERVICE@ALTA.ORG

State and National Groups to Consider

- State reporting legislation: www.alta.org/business-tools/cybersecurity.cfm
- Gramm-Leach Bliley Act: www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm
- Federal Trade Commission: www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
- National Association of Insurance Commissioners: http://www.naic.org/cipr_topics/topic_cyber_risk.htm

What should be encrypted?

Any device or service that holds non-public or sensitive data should be encrypted to ensure you are implementing reasonable security measures to protect customer and partner data. Encryption can seem like a difficult task, but in many cases can be invoked rather easily. Like most technologies, however, if you don't feel comfortable, make sure you consult with a professional that can help you and your organization.

When thinking about encrypting data you must consider data in at rest and in transit. Data in transit is data that is moving between computers and websites/online applications. Data at rest typically resides on hard disk of servers, computers, cloud servers and USB drives. Regardless if it is at rest or in transit, data must be safeguarded from being accessed by unintended parties and should be considered for encryption.

Devices and services to consider encrypting

- Workstation
- Laptops
- Servers
- USB storage devices / thumb drives
- File shares
- Mobile phones
- Tablets
- Websites
- Cloud, hosting or software as a service

With **workstations, laptops and servers,** you can encrypt only the files and folders that have sensitive data, but this is a manual process with the potential for human error. The best method is to encrypt entire drives when possible making it difficult for anyone to boot the device or access any data on the drive. As a best practice, a professional should always be engaged, and backups or other recovery methods need to be in place, in the event of a lost password of encryption key. If you have **file shares** outside of a workstation or server, such as a network attached storage device or other type of file share technology, ensure that the technology allows for encryption.

USB storage/thumb drives pose considerable risk because these devices are small and portable. These storage devices tend to have high capacity and are especially dangerous to unauthorized access due to their mobility and ease of access.

Most people receive and access data on **mobile smart phones** and **tablets**. These mobile devices can be easily lost or stolen falling into the hands of unintended parties. When thinking of these devices we don't typically think about encryption but these devices are recommended to be encrypted along with your workstations.

Most mobile devices encrypt the entire device by enabling the use of passcodes; however, some mobile operating systems require you to active the encryption even if passcodes are in use.

There are **websites** for all types of activities from marketing, customer interaction portals, or even web based applications. These resources and services can contain non-public information or sensitive data and should be encrypted to safeguard data in transit. This type of transit encryption is performed by transport layer security (TLS). When using a web browser to access these resources and services the browser would use *https://* at the beginning for a URL rather than *http://* making a request to the website. The browser then uses the public key from the website and encrypts the transport of data to and from the website keeping data secure.

Many companies use **cloud, hosting, or software as a service** technical solutions to perform day to day functions; this can range from, but not limited to, title software, email, accounting applications, customer relationship management tools, data backup, and more. Outsourcing the heavy lifting of a technology infrastructure can be effective in cost, ease of access, and availability, however, there are a lot of questions that should be asked to be sure the provider is right for you. Top of mind should be "is my data encrypted at rest and in transit?" If you have non-public or sensitive data stored and or processed with this provider, then the answer should be yes the data should be encrypted. Encryption protects the data at the provider's data center ensuring you are protected.

Conclusion

In todays fast pace technology world, title agents utilize many technology mediums to store and access non-public and sensitive data. Keeping this data protected from unauthorized access is our responsibility. We all have good intentions to keep data out of unintended individual's hands, however, there are circumstances out of our control that require us to encrypt data at rest and in transit to safeguard the data protecting our customers, partners, and even ourselves.