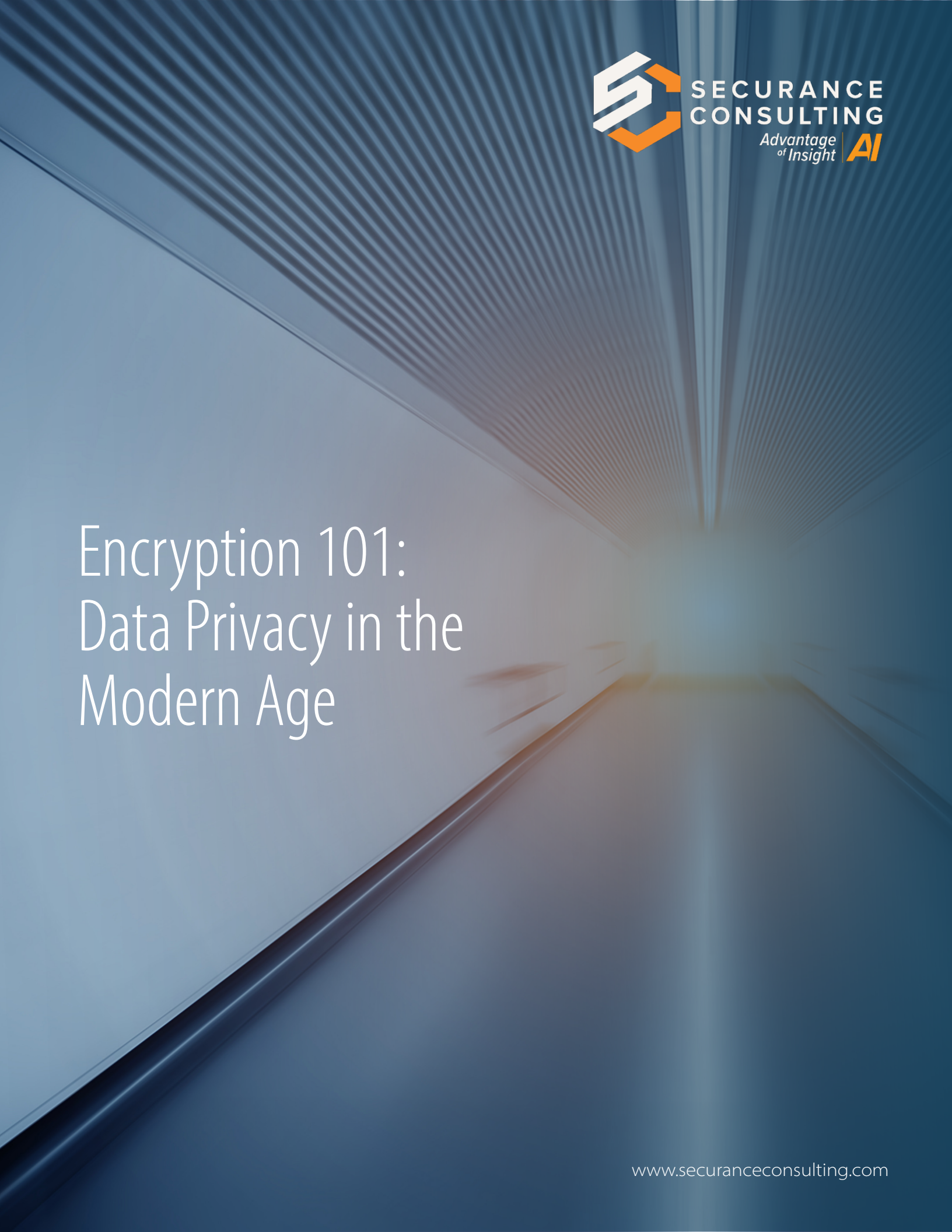


Encryption 101: Data Privacy in the Modern Age

www.securanceconsulting.com

INTRODUCTION

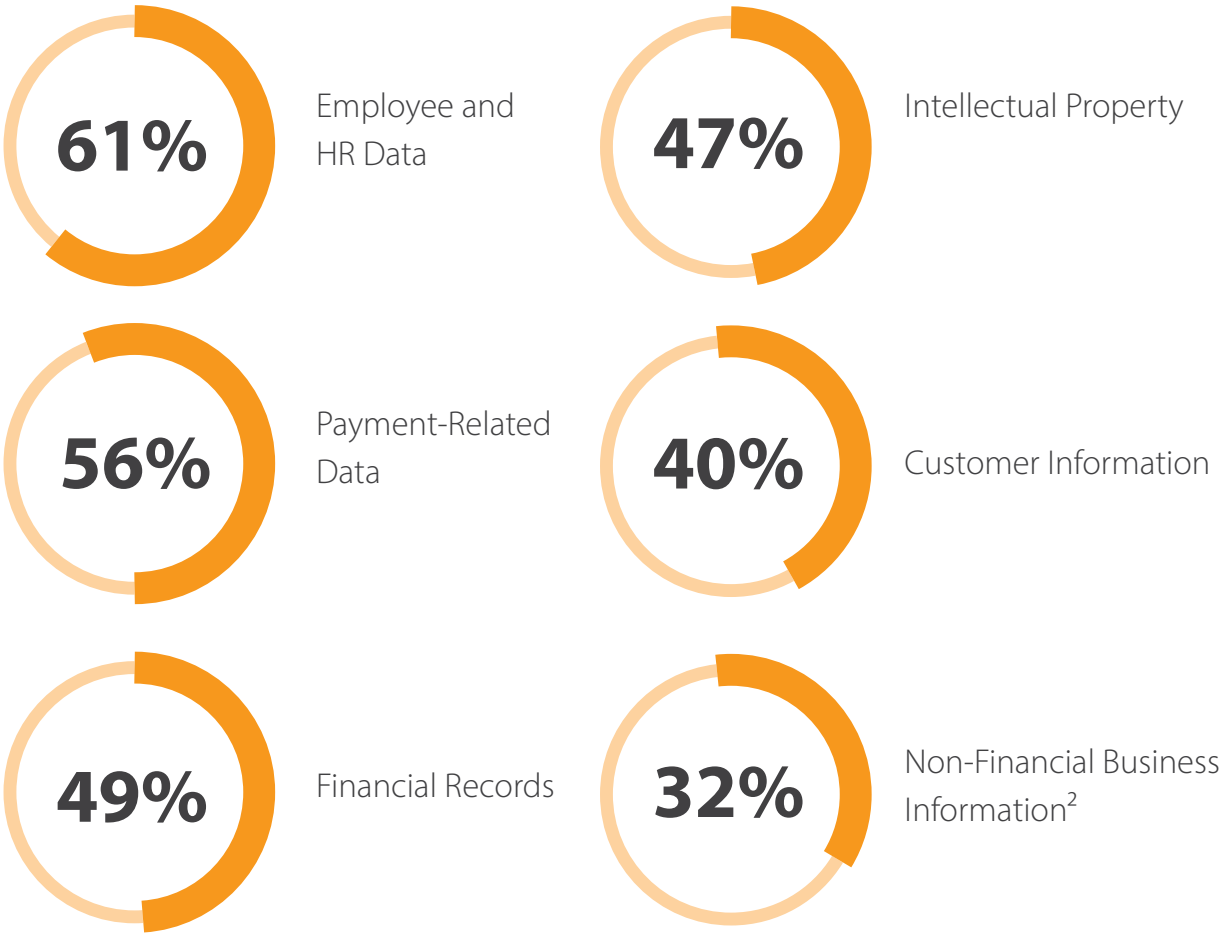
If information were money, we wouldn't leave it lying around for just anyone to take. We'd put it in the bank, or, at the very least, lock it up and put a password on it. In reality, the right kind of information is money to hackers around the world, who sell personal and proprietary data on the dark web (the Internet black market). This practice has evolved from selling stolen hardware, such as cell phones and laptops, because the business of selling private information has become much more lucrative than selling the devices that house it.

In 2019, **13 million Americans** fell victim to identity fraud due to stolen personal information, resulting in a whopping **$16.9 billion** (yes, with a "B") in total losses. The types of fraud committed include employment or tax-related, credit card, phone or utilities, bank, loan or lease, and government documents or benefits fraud.[1]

One credit card is not much use to a hacker, but add an address, a mother's maiden name, and a social security number, and your identity is as good as theirs— but they won't suffer from your ruined credit.

Arguably, the simplest way to protect private data is to use encryption.

Data Most Commonly Encrypted:



> Cybercrime will cost the world in excess of **$6 trillion** annually by 2021, up from **$3 trillion** in 2015.[3]

WHAT IS ENCRYPTION?

Encryption is an arithmetic tool used to translate data into another form, so it can't be read by prying eyes. Think of it as recognizable words becoming lines of indecipherable code. Modern day encryption is the natural evolution of classic cryptography, such as the codes used by Allied and Axis powers in World War I, which used paper and pen cryptography to disguise secret messages. The earliest known method of encryption was used by ancient Egyptians, in the form of nonstandard hieroglyphics. Before time immemorial, humans took precautionary measures to mask private information from unauthorized recipients— and it's arguably more important now than ever, given the rapid advancement of technology.

The only way to quickly and authentically access encrypted data and translate it back into a legible format is with a decryption key or cipher. Simply put, decryption keys are the passwords for encrypted information. On a more technical note, they are deciphering algorithms built to reverse-engineer the encrypted data.

The opposite of a decryption key is (surprise!) an encryption key. Put simply, this type of key scrambles data, thus encrypting it. Depending on the encryption method employed, a single key may suffice, or two keys, referred to as a "key pair," may be necessary. A key pair is comprised of one public key and one private key. The former may be shared, because it is meant only for encryption. The latter, however, is understandably not shared, as it has the ability to decrypt any data encrypted by the public key.

Types of encryption

Multiple types of encryption exist, because there are varying levels of sensitive information. It's expected that health records, banking information, and Federal agency data, for example, will have heavier encryption than a personal online photo album. Ideally, all information that belongs to one person will remain the property of that individual and be accessible by trusted parties only, such as healthcare providers and banking institutions.

ROT13

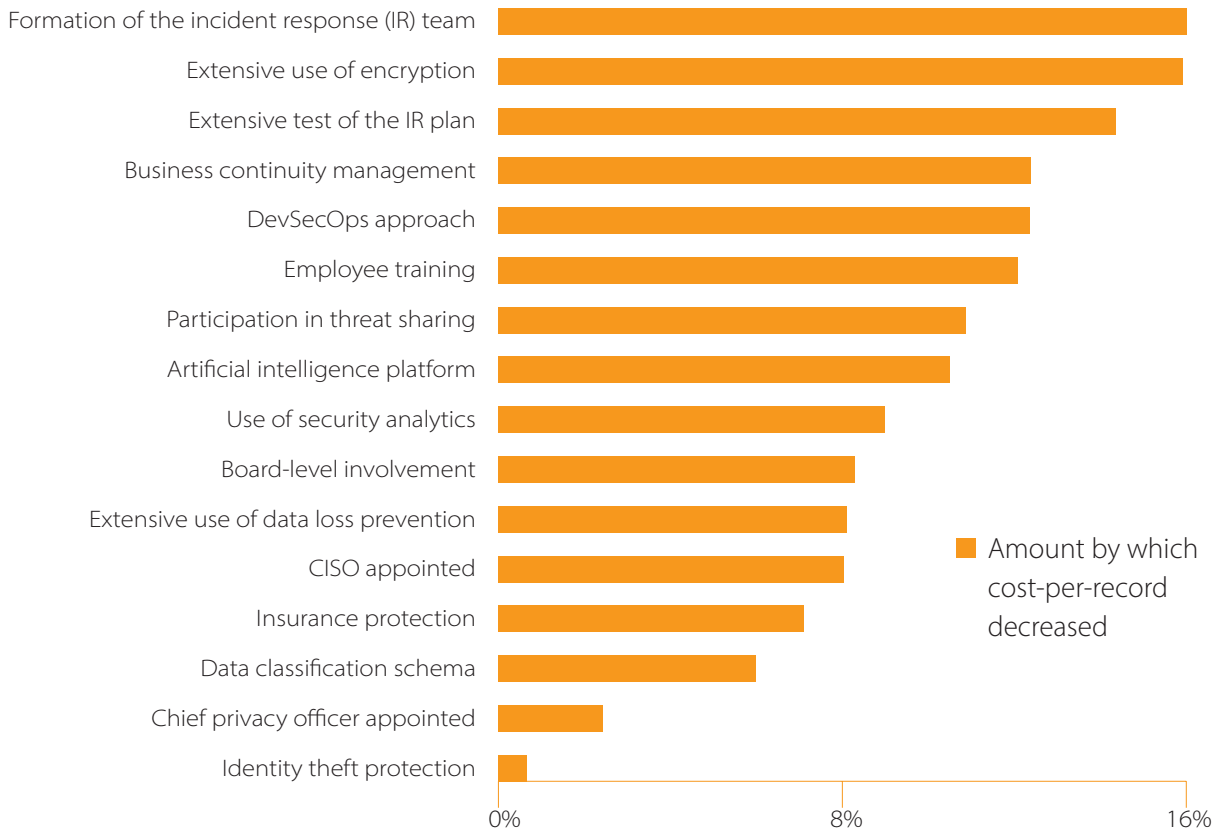
ROT13 is based on rotation and is the easiest method of encryption. In this method, each letter of the plain text is substituted with a letter thirteen places ahead in the alphabet. If "H" is "U," then "L" is "Y," and "O" is "B." A plain text code of "hello" becomes "uryyb."[4] As one of the oldest encryption methods, it doesn't stack up against modern day cybercrime. Thus, more sophisticated methods have been developed to ensure data security.

> Encrypted data is called ciphertext, while unencrypted data is called plaintext.

AES

On the opposite end of the spectrum is the Advanced Encryption Standard (AES), a symmetric encryption algorithm used by the United States government because of the level of security it offers. AES uses a block cipher, which encrypts information in predetermined parts, as opposed to a stream cipher, which encrypts data bit by bit. Many states have enacted Safe Harbor Laws, which protect organizations that use strong encryption like AES in the event of a data breach. If the organization is compliant, the Safe Harbor Laws exempt them from having to provide notice of the breach to customers. Encryption-friendly laws, such as this, not only provide an incentive to encrypt data, but also help organizations preserve their brand image and reputation, potential sales, and strategic relationships.[5]

Strategies to Reduce the Cost of a Data Breach



Key Findings from the 2019 Cost of Data Breach Study: Global Overview, IBM, 2019[14]

Regardless of encryption type, end-to-end encryption should be employed for high-value data. The following controls should also be considered:

- Storage-based encryption should not be the primary form of encryption.
- The point of encryption depends on any required data reduction operations.
- Data retention requirements should be considered when deploying encryption.
- Encryption strength should be a minimum of 112 bits, with 128 bits as the recommended minimum.
- Cryptographic modules should be validated using recognized criteria.
- Use of multiple encryption steps is recommended, such as encryption at the application layer that is then stored on a self-encrypting drive.
- Proper audit log entries must be generated for all encryption activities (e.g., activation, rekeying, and verification.).[6]

PROTECTING SENSITIVE DATA

Encryption is used to protect digital data in three states:

» **Data at rest** – "At rest" refers to data that is being stored on a disk, whether that disk is a hard drive, USB, or storage area network (SAN). This is the most secure of the three states; however, that security must be comprised of multiple layers, including firewalls, an antivirus program, and encryption, in order to prevent malicious attacks.

» **Data in transit** – Data "in transit" or "in motion" refers to information that is being transferred between networks or systems. Data in transit is the most vulnerable, because anyone with the right skillset can intercept the information as it makes its way across networks to its final destination. It is therefore wise to implement desktop, gateway, and mobile email encryption, as well as secure socket layer (SSL) encryption to protect data transfers from unauthorized users.

» **Data in use** – "In use" refers to data in computer memory or data currently being utilized by applications. It is more vulnerable than data at rest, since, by nature, it is accessible to anyone who needs it. Because the user pool is so high, access must be tightly controlled to ensure data does not fall into the wrong hands. Full memory encryption is steadily gaining traction as an effective method of ensuring data security in this state.

There are two basic classes of cryptographic algorithms, defined by how many keys are used with the algorithm:

» **Symmetric Cryptography** – Uses a single password as both the encryption and decryption key. Algorithms used for this type of cryptography are highly secure, but because there is only one key, it must be changed frequently to avoid compromise.

» **Asymmetric Cryptography** – Uses a key pair, one each for encryption and decryption. This method is generally believed to be more secure than symmetric cryptography.

> Only **45%** of companies have a consistent enterprise-wide encryption strategy.[7]

ENCRYPTION FOR COMPLIANCE

Various regulations require organizations to implement encryption methods in order to be compliant. The Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), and the Gramm-Leach-Bliley Act (GLBA) are three standards that require encryption.

HIPAA

164.306 of HIPAA states that covered entities must "implement a mechanism to encrypt and decrypt electronic protected health information" (ePHI) or find an equivalent solution to meet the regulatory requirement. While the Privacy and Security Rules are vague on how to specifically implement encryption, the consensus is that encrypting data is undeniably a healthcare best practice. The following are methods of protecting PHI with encryption:

» Double up on encryption when possible. Sending an encrypted file over an encrypted connection is safer than only choosing one of the two.
» Do not use file transfer protocol (FTP) to transfer patient data between payers and other business associates.
» Use a virtual private network (VPN) when sending PHI remotely.
» Do not store data on portable devices. If there is no other option, employ full disk encryption (FDE) or file/folder-level encryption while data is stored locally.
» Perform a HIPAA risk assessment to determine which areas of the organization require encryption and where gaps exist in the current security environment.[8]

CJIS

CJIS is the largest division of the Federal Bureau of Investigation (FBI). As one can imagine, anything having to do with Federal security requires more than basic data protection. To comply with CJIS, organizations must use a minimum of 128 bit encryption, and decryption keys must be at least 10 characters long and include a mixture of upper and lowercase letters, numbers, and special characters. These keys must be changed regularly, depending on the fluctuations of need for authorized access.[9]

GLBA

GLBA requires financial institutions to utilize encryption for the transmission and storage of all non-public personal information.[5] A major area of concern is email, because it is the primary communication medium for financial institutions and their clients. With client-side email encryption, an organization can control access to sent emails and attachments or even revoke access at will. Digital privacy is key to complying with GLBA and helps build and maintain customer trust while reducing the risk of a data breach.

> Due to the intensity of compliance and regulations, the costs per breach to organizations in the healthcare and financial services sectors top all other industry groups.[10]

CHALLENGES

Data breaches are the main reason encryption has become fundamental to security. Whether in the cloud, on mobile devices, or on home computers off the corporate network, organizations must take precautions to secure confidential information.

Theft

Juniper Research predicted that data theft will jump 175 percent by 2023, from 12 billion records stolen in 2018 to 146 billion. However, small businesses, which are extremely susceptible to cyberattacks, will contribute only 13 percent of all digital security spending. More worryingly, most will spend less than $500 annually on security. With more and more data and business being digitized, the chances of a business, no matter the size, becoming the victim of malware, ransomware, and data theft significantly increase.[10] If adequate encryption measures are put in place to ward off ne'er-do-wells, criminals might just decide the effort isn't worth it and move on to a different target (hopefully, also with security measures in place).

Extensive use of encryption was second only to forming an effective incident response team in reducing the cost of a data breach.

Top Drivers for Encryption:

2017 Global Encryption Trends, Thales, April 2017[2]

Discouragement

Unfortunately, bad guys also use encryption. It is commonplace for hackers to create ransomware that encrypts an organization's data, rendering entire systems unusable until the hacker's demands for currency are met. ***The global financial impact of ransomware reached $11.5 billion***— up from $5 billion in 2017— and shows no signs of slowing down, which can discourage organizations into questioning the utility of additional investments in cybersecurity.[12] Of course, the fact that encryption can be used against an organization should not deter it from using encryption itself. On the contrary, the more secure an organization's networks and systems, the less likely malicious attackers are to gain access to information they shouldn't have. Encryption can help in this regard by reducing sensitive data's visibility while in transit, at rest, and in use.

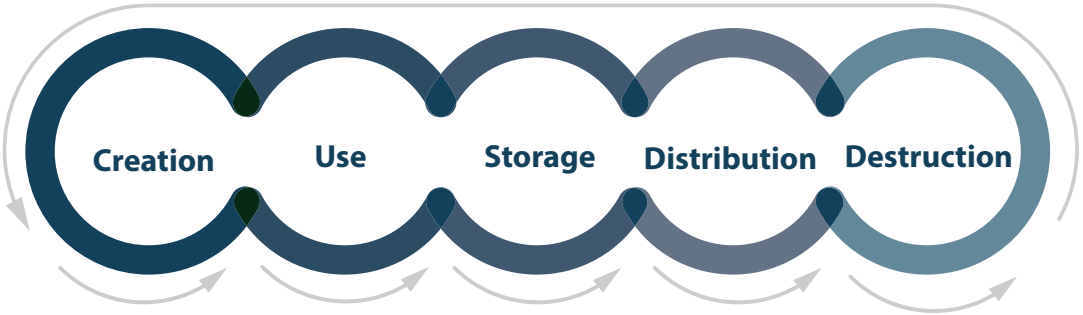
False sense of security

While necessary for well-rounded security, encryption is not the "be all, end all" of security. It must be implemented in tandem with other measures, such as data loss prevention solutions and identity and information access controls. Some organizations gain a false sense of security when they implement encryption and choose to rely on fewer controls than are actually necessary to ensure data protection. The best practice for any organization or industry is to implement multi-layer security, which includes, but is not limited to, encryption, firewalls, antivirus solutions, spam filters, digital certificates, and intrusion detection systems.

> The financial hit resulting from theft of trade secrets ranges from 1 to 3 percent of an entire nation's gross domestic product (GDP), with costs ranging from **$749 billion** to **$2.2 trillion** annually.[3]

Key Management

Security is all about controlling access. Who must be able to view certain data, and who can live without it? As organizations encrypt more and more data, key management becomes that much more of a concern. Effective key management entails the protection of keys during their full lifecycle, including:



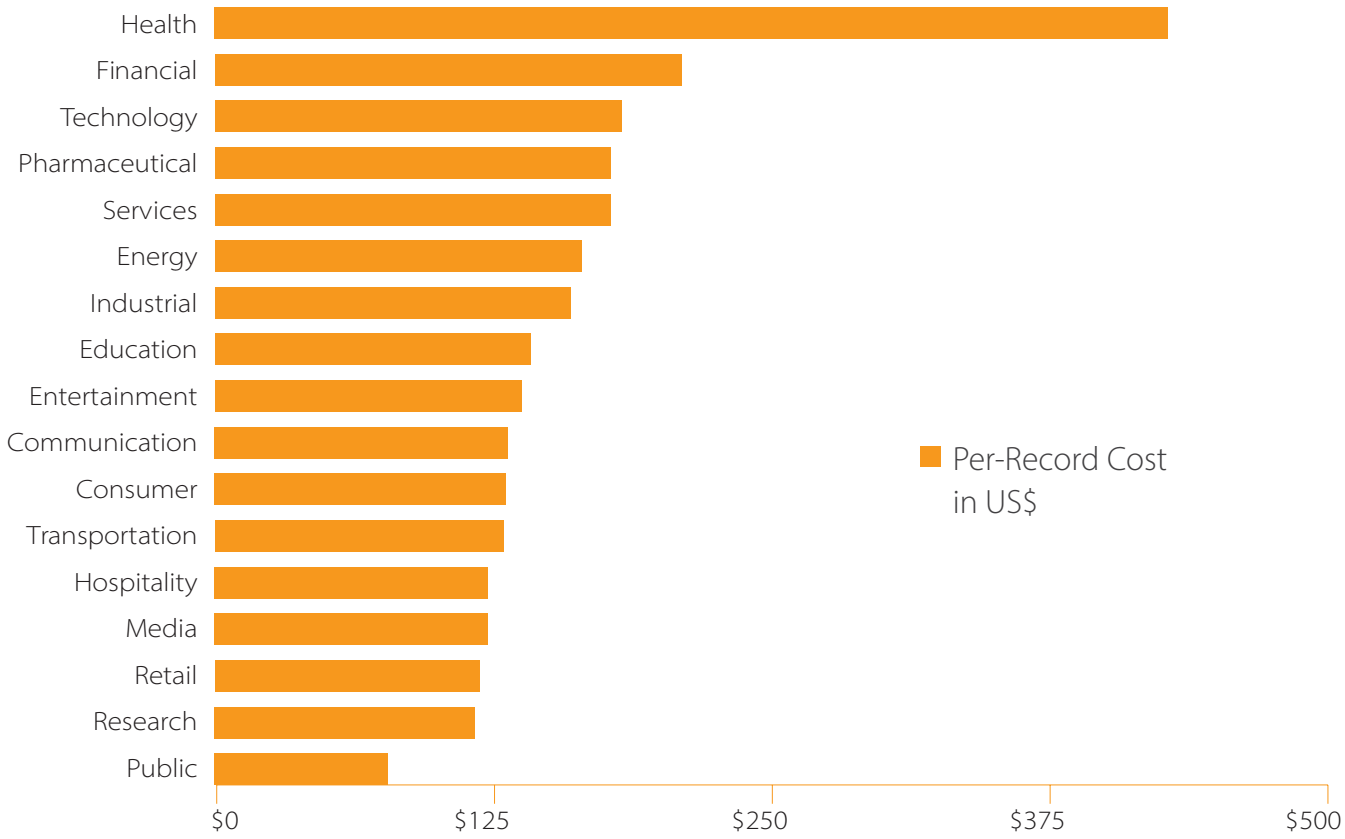
The National Institute of Standards and Technology (NIST) provides recommendations for effective key management in NIST Special Publication 800-57. These guidelines accomplish the following:

- Define security services that may be provided and key types that may be employed in using cryptographic mechanisms.
- Provide background information on the cryptographic algorithms, which use cryptographic keying material.
- Classify the different types of keys and other cryptographic information according to their functions, specify the protection each type of information requires, and identify methods for providing this protection.
- Identify the states in which a cryptographic key may exist during its lifetime.
- Identify the multitude of functions involved in key management.

» Discuss a variety of key management issues related to the keying material, including key usage, cryptoperiod length, domain-parameter validation, public key validation, accountability, audit, key management system survivability, and guidance for cryptographic algorithm and key size selection.[13]

In their 2018 Cyber Incident & Breach Trends Report, the Online Trust Alliance found that 95 percent of breaches could have been prevented by implementing basic security measures, such as encryption, patching, and cybersecurity awareness.

Average Per-Record Cost by Industry Sector



Key Findings from the 2019 Cost of Data Breach Study: Global Overview, IBM, 2019[15]

Key avoidable causes for incidents include:

» Lack of a complete risk assessment, including internal, third-party, and cloud-based systems and services
» Lack of effective vulnerability and patch management processes
» Misconfigured devices or servers
» Unencrypted data and/or poor encryption key management and safeguarding
» Use of end-of-life (i.e., unsupported) devices, operating systems, and applications
» Employee errors and accidental disclosures (e.g., loss or improper disposal of data, files, drives, devices, and computers)
» Failure to block malicious email
» Users succumbing to business email compromise and other social engineering tactics[14]

> The average cost of a data breach is expected to exceed **$150 million** in 2020.[3]

CONCLUSION

If you like it, then you should encrypt it

Whether an organization must comply with regulatory requirements, protect intellectual property or client information, or simply keep internal HR records secure, following encryption best practices will benefit its reputation, finances, and IT security.

Having effective encryption best practices in place will help an organization minimize security breaches and the impact any potential breach could have on operations. Reliable controls can also decrease resource strain in the IT department, as well as the overall security budget.

To get the most out of encryption efforts, organizations should encrypt data at rest, in transit, and in use; layer encryption for optimal security; and practice secure key management. If data were money, we would think twice about: how we store it; who has access to it; and the ramifications for losing it. Even if we put it into a safety deposit box, what guarantee do we have that the key to unlock it is also secure? As with all security, taking a step back and looking at the entire picture can aid an organization in planning the most effective encryption strategy, which will help decrease the chance of an expensive and time-consuming data breach in the future.

ABOUT SECURANCE

Securance has two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

[1] https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis

[2] https://www.thalesesecurity.com/2018/global-encryption-trends-study

[3] https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

[4] https://www.micron.com/~/media/documents/products/white-paper/self_encrypting_drives_white_paper.pdf

[5] https://www.symantec.com/content/dam/symantec/docs/white-papers/keeping-your-private-data-secure-en.pdf

[6] https://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Encryption-KM-TechWhitepaperR1.pdf

[7] https://www.ncipher.com/global-encryption-trends-study

[8] http://resource.onlinetech.com/encrypting-data-to-meet-hipaa-compliance/

[9] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

[10] https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[11] https://www-cdn.webroot.com/5415/0396/2242/The-Future-of-Cybercrime-and-Security-Juniper.pdf

[12] https://risksense.com/wp-content/uploads/2019/09/RiskSense-Spotlight-Report-Ransomware.pdf

[13] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf

[14] https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf

[15] https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

SECURANCE CONSULTING
Advantage of Insight AI

13904 Monroes Business Park • Tampa, FL 33635 • 877.578.0215

www.securanceconsulting.com