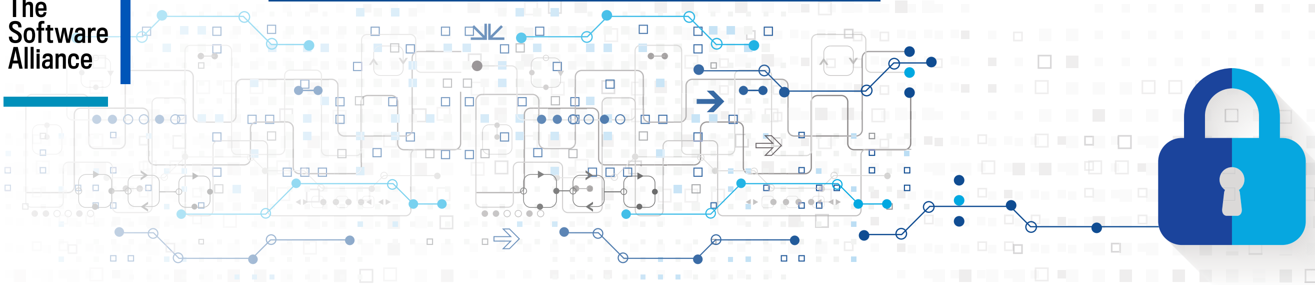
The Software Alliance

BSA

ENCRYPTION BACKGROUNDER

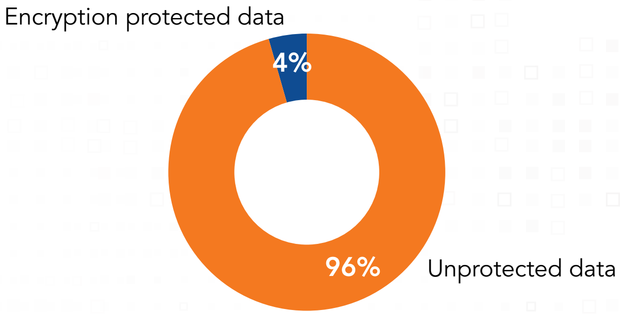


Encryption Is a Critical Safeguard Against Data Breaches

Encryption is a critical tool for protecting sensitive data, including personally identifiable information that can be used for identity theft, financial data exploited for fraud and other financial crimes, proprietary business information and intellectual property, and even government secrets. Although strong encryption cannot prevent a data breach, it can block cyber attackers from accessing the sensitive data once its stolen, thus mitigating the risk.

RECORDS BREACHED IN 2016:
1,378,509,262

Percentage of 2016 Data Breaches Where No Encryption Was Used



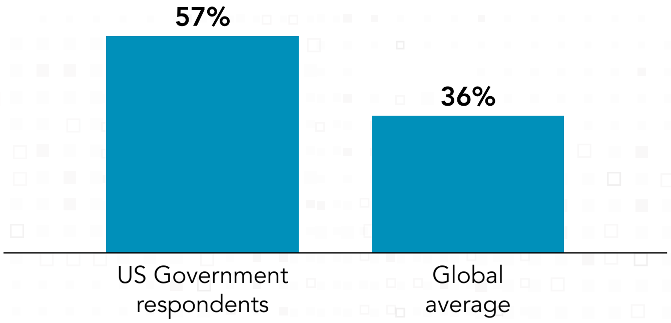
Source: *2016 Mining for Database Gold: Findings From the Breach Level Index*, available at https://breachlevelindex.com/assets/BLI-ebook-2016/mobile/index.html#p=1.

Data breaches have real-world effects. The average data breach costs $3.62 million, according to the Ponemon Institute.[1] More than 143 million Americans were victimized in a single data breach incident involving the credit report agency Equifax, and many of these Americans were subsequently targeted for identity theft and fraud. Such breaches not only cost money, but can lead to the theft of intellectual property that undercuts businesses' ability to compete, or to the theft of sensitive government information that compromises national security. For example, a 2015 breach of the Office of Personnel Management led to the theft of security clearance background investigation records of roughly 21.5 million current, former, and prospective Federal employees and contractors, an intelligence boon to the perpetrator.

Because encryption is among the most important tools for managing the risk of data breach, it is widely mandated by government and critical infrastructure organizations. Strong encryption is recommended by the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, now mandatory for US Government agencies.[2] It is also directed for financial sector entities and Smart Grid operators.

Weakening encryption would increase the risk of data breaches, threatening individuals, critical infrastructure, the economy, and ultimately national security. Instead, policymakers should defend the integrity of encryption technologies while working to expand its use across public and private stakeholders.

US Government Agencies Are Especially at Risk of Breach



Source: 2018 Thales eSecurity Data Threat Report, available at https://dtr.thalesesecurity.com/.

[1] IBM, 2017 Ponemon Cost of Data Breach Study, available at https://www.ibm.com/security/data-breach.

[2] National Institute for Standards and Technology, *Framework for Enhancing Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018), available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.