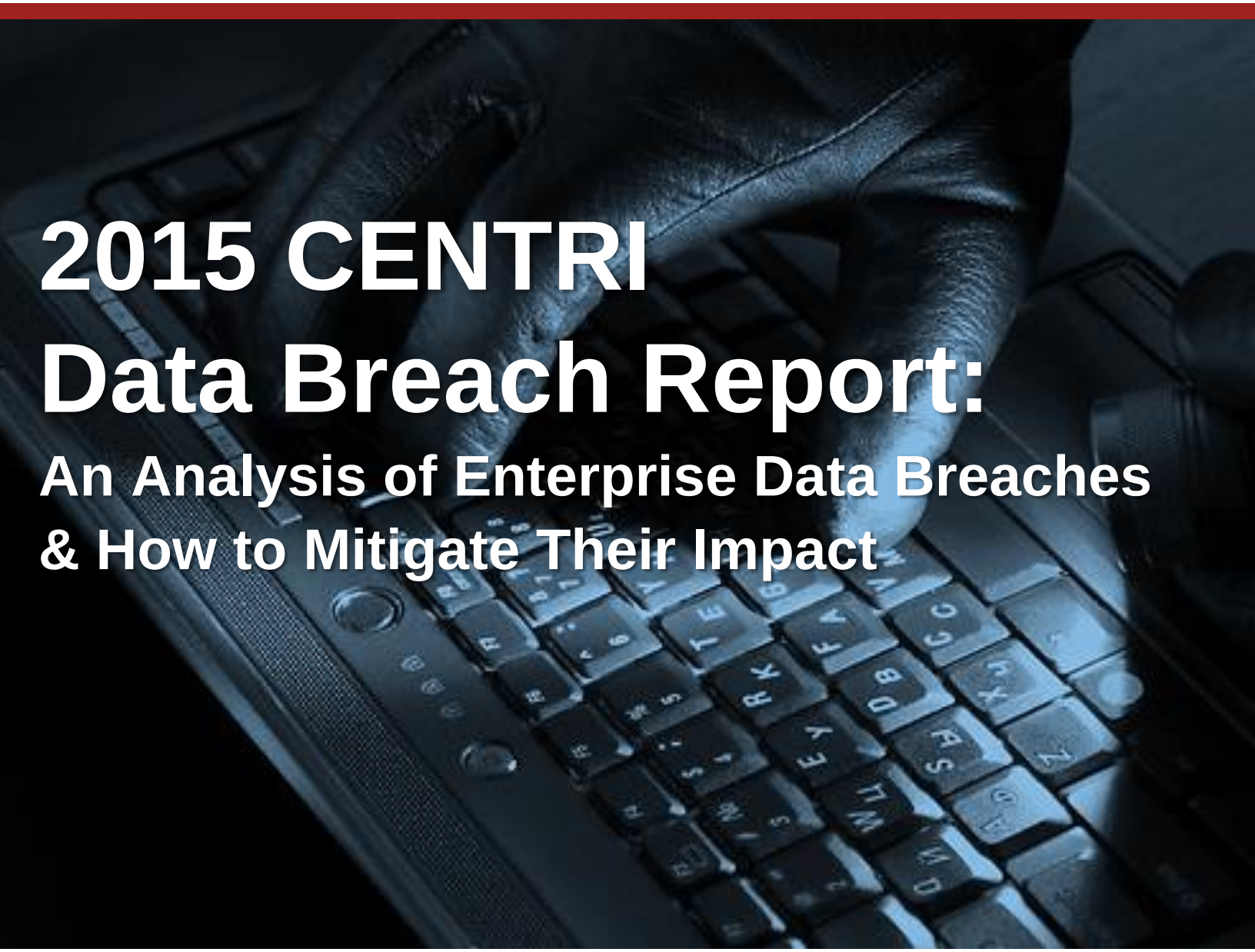
INDUSTRY REPORT



2015 CENTRI Data Breach Report:

An Analysis of Enterprise Data Breaches & How to Mitigate Their Impact

CENTRI

Protect your data

Introduction

This industry report attempts to answer the question: *Why are cyberattacks still successful?* Along the way it examines the types of problems that enterprises face, common types of attacks, the true cost of data breaches to major organizations and the tools available today to mitigate these threats.

Why Are Cyberattacks Still Successful?

Key Takeaway: ***While the world around us has dramatically changed, the way that we approach security generally has stayed the same for decades – deploy defensive perimeter defenses with reactionary tactics to deal with data breaches.***

Network based solutions alone are no longer adequate

Cloud computing and mobile first world exposes data

The amount of data and access points are growing exponentially

Problems Facing Enterprises Today

Security Breaches

Inconsistent Laws

Account Takeovers

Compliance Issues

Risk of Losing Customer Data

Mobile Malware

Old Encryption Methods

Insider Access

DDoS Attacks

Identity Theft

Man-in-the-Middle Scams

Overwhelmed IT staff

Key Takeaway: *It's no secret that enterprises have many security risks to contend with both internally and externally. However, very few organizations have the necessary solutions or strategies to cope with these issues when a crisis occurs. Many of these problems associated with data breaches can be mitigated with available data protection solutions today.*

Common Types of Cyberattacks

Key Takeaway: ***While most of these attacks are focused on ways through the network, the main goal is for thieves to access your confidential data. A layered security approach with secure data encryption alongside network protection is essential.***

Network Eavesdropping

Often referred as sniffing or snooping. The ability to monitor the network is generally the biggest security problem that administrators face in an enterprise

Brute Force Attacks

Also known as an exhaustive key search, consists of systematically checking all possible keys and passwords until the correct one is found

Browser Exploited Against SSL/TSL

In SSL connections, to allow decrypting HTTPS requests and steal information such as session cookies to be used to impersonate the user

Identity Spoofing

Creation of Internet Protocol (IP) packets that appear to originate from valid addresses with the purpose of concealing the identity of the sender or impersonating another computing system

Session Hijacking

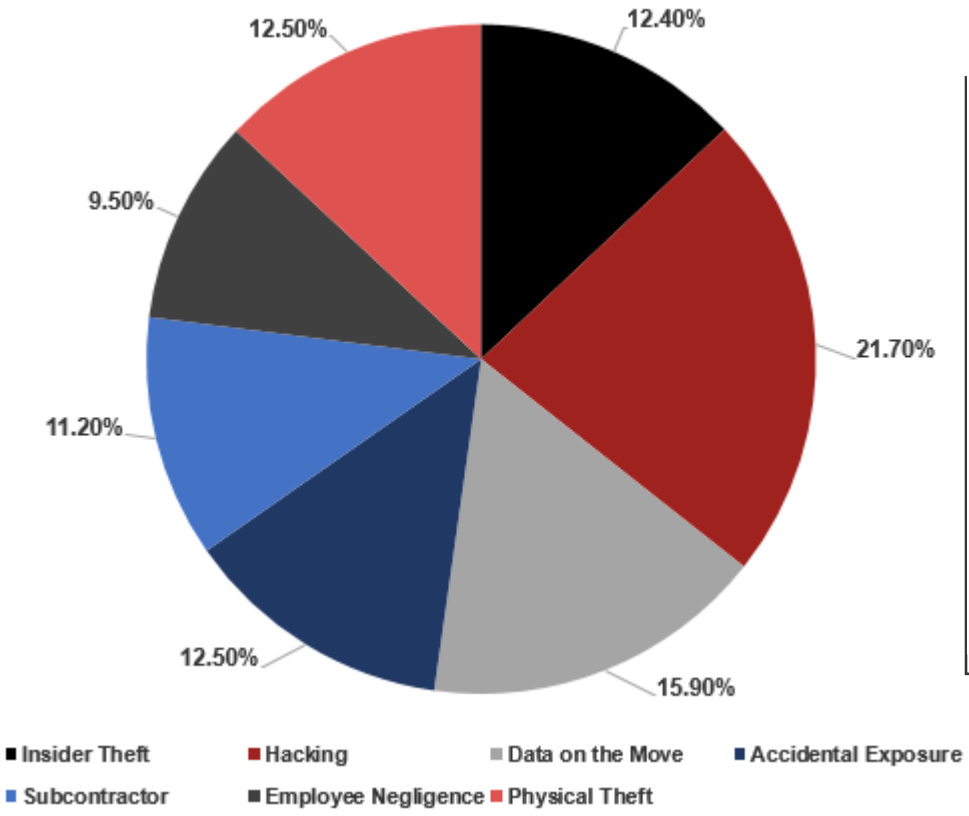
An attacker may watch a session open on a network. Once authentication is complete, they may attack the client computer to disable it, and use IP spoofing to claim to be the client who was just authenticated and steal the session

What Are the Sources of Attacks?

(2008-2014 average)

#1 Hacking
#2 Data on the Move
#3 Accidental Exposure
#4 Physical Theft
#5 Insider Theft
#6 Subcontractor
#7 Employee Negligence

Sources of Attacks



Key Takeaway:
While external hackers are still the #1 source, more breaches occur from internal sources combined from insider theft, accidental exposure and employee negligence. How are you protecting your enterprise from internal data breaches?

Current Limited Security Solutions to Deal with Data Breaches

Key Takeaway: ***Most solutions and processes today are designed to prevent data breaches from happening. There needs to be more focus on what to do when a breach inevitably occurs in order to secure the data most effectively.***

Use of monitoring technologies to detect anomalies

Monitoring network, systems and data in real-time and correlating analysis of security across your enterprise by actively analyzing the logs and alerts

Multifactor authentication and authorization

Requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction

Internal policies and staff education

Setting corporate standards for employees and establishing training programs for proper access to data and devices

Physical security measures in data centers

Designing access control systems to prevent unauthorized personnel into your data center

Security patch updates post-breach

Delivering a fix to your customers or stakeholders *after* the breach has occurred to bring back the service

Source: Tech Target http://searchsecurity.techtarget.com

The True Costs of a Data Breach

Based on real enterprise examples

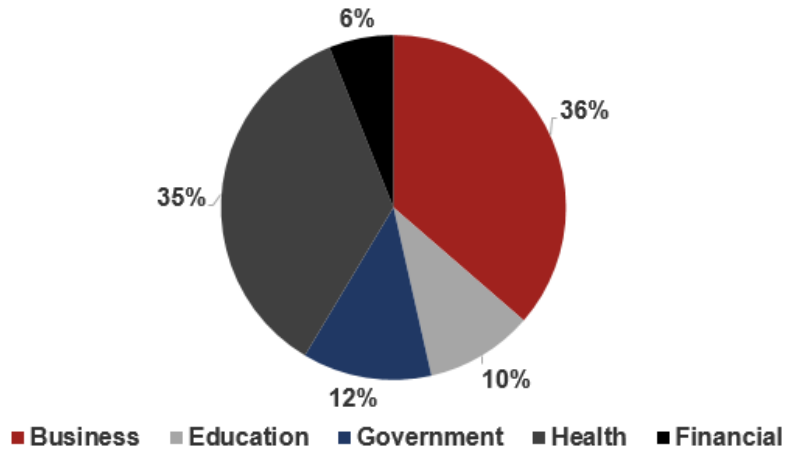
ELEMENT	IMPACT
Fraud losses, legal fees, security improvements	**$Millions to $Billions in costs** (Anthem)
Drop in stock value & profits	**5% to 10% drop in stock price** (Chase, Target)
Brand value	**Brand index scores drop immediately into negative values**
Credit rating	**S&P can cut credit rating** (Target)
Job security	**C-level executive shake-ups**
Customer churn	**High customer churn rate, some customers never return**

Key Takeaway: ***The intangible costs associated with a data breach such as stock value, brand value and customer churn can dwarf all of the other costs over time. Stolen unencrypted data is the biggest risk with a breach. With these large consequences, why aren't all firms securing their data better?***

Data Breaches by Industry

Key Takeaway: ***Data breaches happen to every industry but some are more frequent targets as the value of their data is greater. Look at your particular industry on average and ask yourself what steps you can take to lower these costs.***

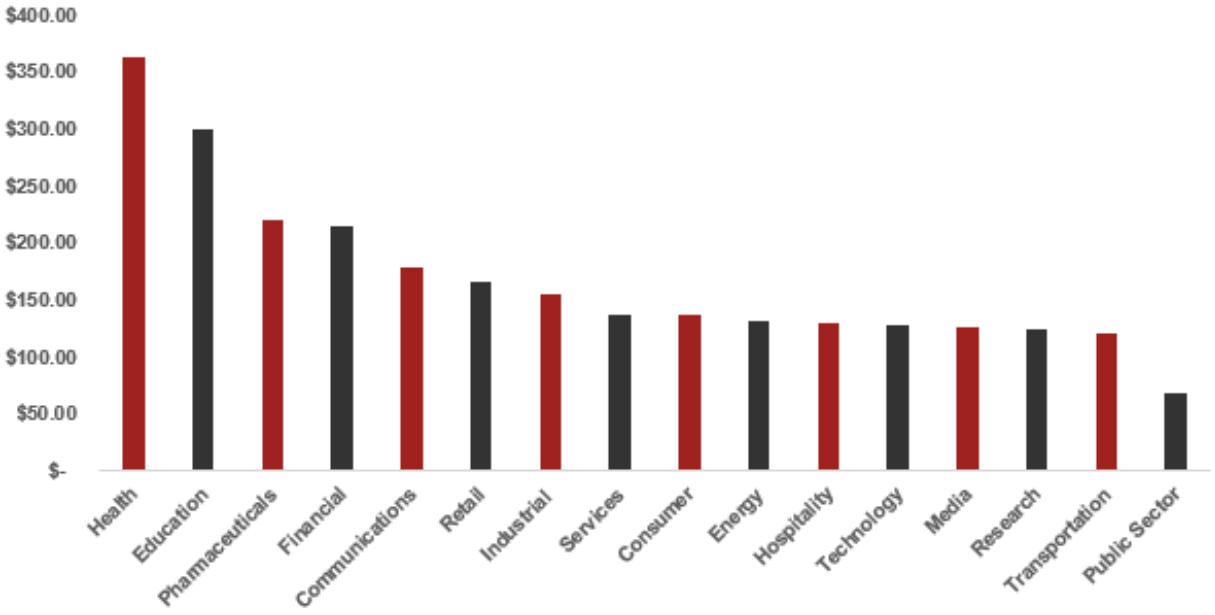
% of Breach Occurrences by Industry 2010-14



ITRC Breach Statistics 2010 – 2014 http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf

The top ten most costly data breaches by industry are: Healthcare, Education, Pharma, Financial Services, Communications, Retail, Industrial, Services, Consumer and Energy

Cost of Data Breach by Industry 2014



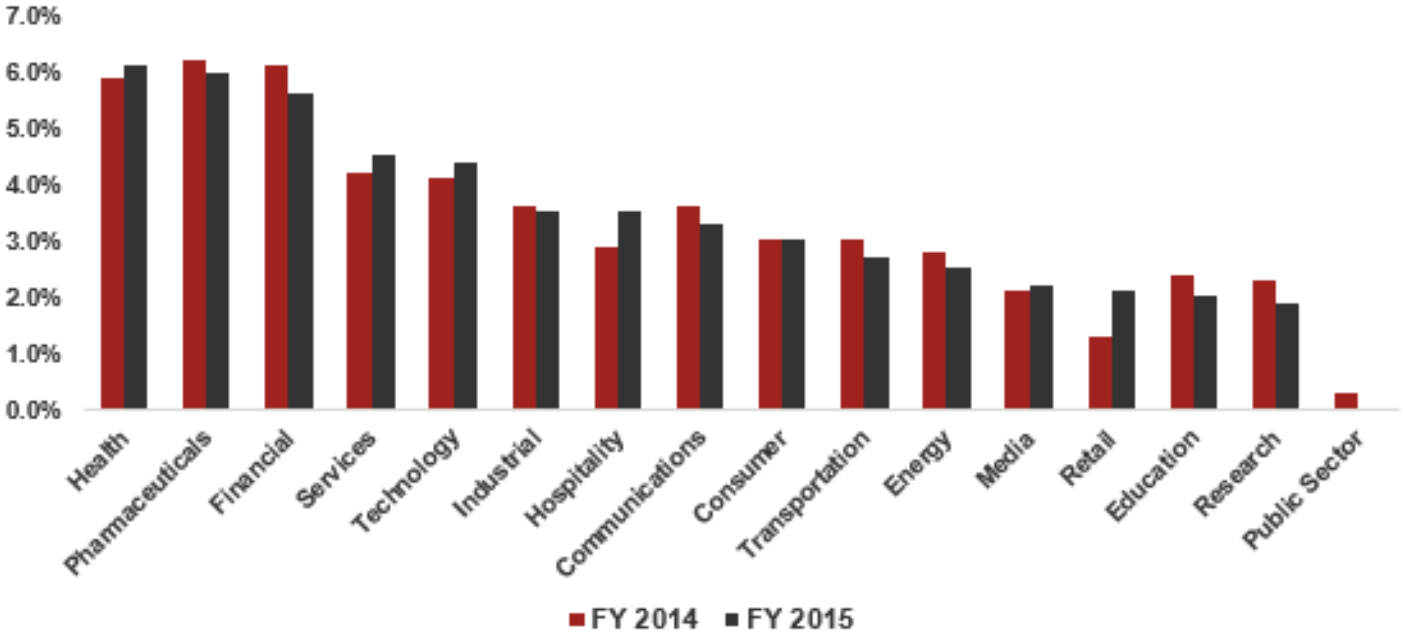
Source: 2015 Ponemon Cost of Data Breach Study

Customer Churn by Industry

Key Takeaway: ***Data breaches can cause customers to lose trust and leave your firm either temporarily or permanently. The top five industries below that customers leave most frequently after a data breach should look to end-to-end data protection solutions to mitigate their customer churn.***

#1 Health
#2 Pharma
#3 Financial Services
#4 Professional Services
#5 Technology firms

Churn Rates by Industry 2014-15



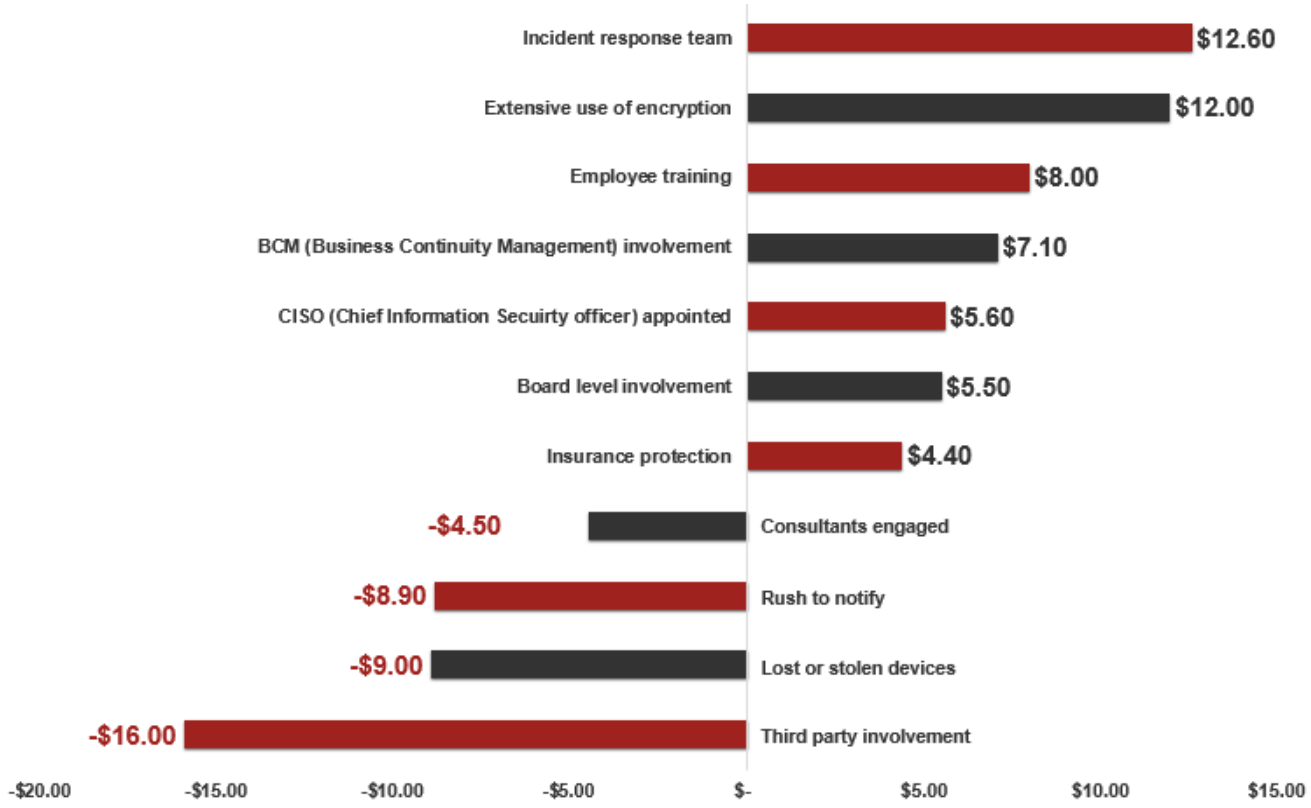
Source: 2015 Ponemon Cost of Data Breach Study

What Alleviates Your Data Breach Problem?

An incident response team, extensive use of data encryption and employee training are the top three areas that *decrease* your cost of a data breach and demonstrate preparedness

Third party involvement, lost or stolen devices and a rush to notify of a breach are the top three areas that *increase* your cost of a data breach and demonstrate a lack of preparedness

Factors Impacting Per Capita Cost of a Data Breach

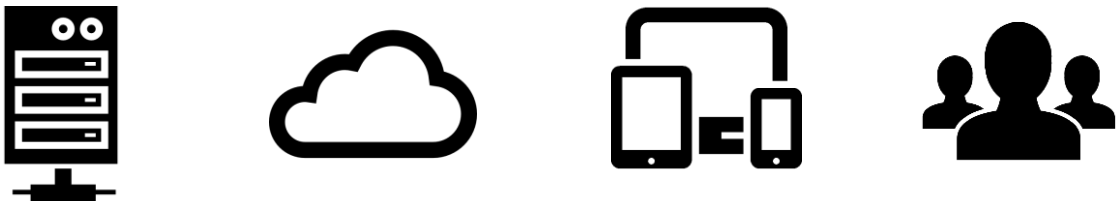


Source: 2015 Ponemon Cost of Data Breach Study

Key Takeaway: ***Extensive use of encryption can reduce the cost of a data breach by $12.00 per compromised record. In contrast, third party involvement in the cause of the data breach results in an increase of $16.00.***

What Can Modern Data Encryption Do For Your Enterprise?

Encryption means protecting data anywhere, everywhere all of the time. In your network, in your Cloud, on employee devices and outside your 4 walls



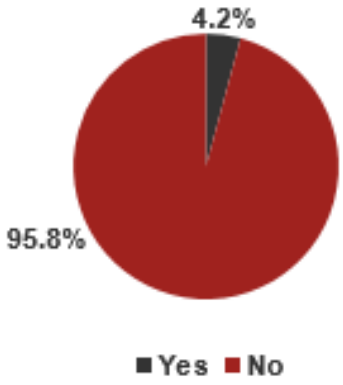
Are Enterprises Using Encryption Solutions Today?

Adoption has increased but nowhere near the level to protect data on the move or in storage

<50%

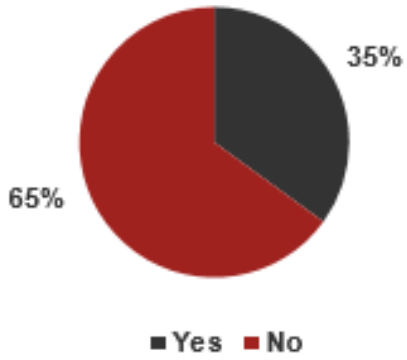
Use Encryption

2006: Do You Have an Enterprise-Wide Encryption Plan?



Source: 2006 Ponemon National Encryption Survey

2013: Do You Have an Enterprise-Wide Encryption Plan?



Source: 2013 B2B International Study

***Key Takeaway:** A data breach is something that sooner or later, almost every organization will experience. Being prepared with the appropriate response plan and training can go a long way. The best strategy from a technology perspective is to deploy a layered security approach that includes a modern end-to-end data encryption solution.*

Take Action With CENTRI

Networks can be compromised. Data breaches are eventually going to happen. The real question to ask yourself is has my organization adequately secured the data itself?

CENTRI's BitSmart is a patented software-only solution deployed on networks, clouds, mobile applications and other endpoints that optimizes, encrypts and secures your data and devices. BitSmart uses an ultra-fast and secure proprietary encryption algorithm that is both more secure and less resource-intensive, enabling ultimate performance and security simultaneously across devices, networks, and applications. BitSmart is a fast, lightweight installation that can help your organization start protecting your data in as little as 15 minutes.

Because it is highly efficient, BitSmart can be used to encrypt all internal data without impacting the user experience. BitSmart provides your organization, your partners, your employees and your customers the confidence of a comprehensive end-to-end security solution for sensitive enterprise data in transit and at rest.

CENTRI
Protect your data

About CENTRI

CENTRI provides next generation data encryption and optimization solutions for the connected world. Our technology helps organizations secure what matters most – their data – by seamlessly integrating into their existing applications and services in the cloud, data centers or mobile devices and the Internet of Things. Enterprises and governments rely on CENTRI to seamlessly protect the full lifecycle of their data – on the endpoint, in transit and in storage.
For more information visit centritechnology.com **or email us at** sales@centritechnology.com.

centritechnology.com /centritech /centritechnology /company/centri-technology

CENTRI Technology
701 5th Ave, Suite 550, Seattle, WA 98104
Main: +1 206.395.2793 | Fax: +1 206.629.9540 | sales@centritechnology.com

August 2015