SOPHOS
Security made simple.

The State of Encryption Today

Results of an independent survey of 1700 IT managers

The way in which people work today has changed significantly since businesses started using encryption products to secure their data. On average we each have 2.9 devices that we expect to be able to use for work purposes. And we don't just work from the office. We work from home, the car, the airport, the café and we need our data to keep up with us, and to stay secure whichever platform or device we choose.

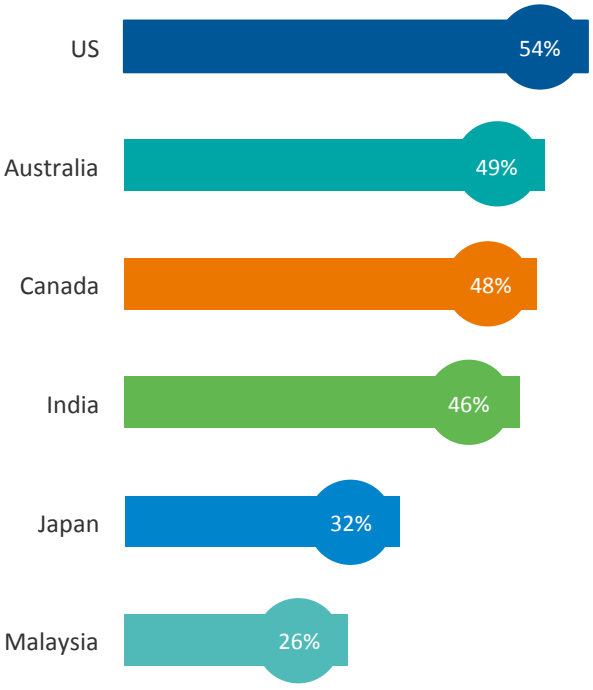
This survey was conducted to better understand where businesses are succeeding with using encryption to secure their data. It also identifies gaps in organizations' encryption strategies as we continue moving toward a business world that demands secure access to data wherever the user is and whichever device they choose to use.

Are organizations encrypting?

44% of organizations are making extensive use of encryption to secure their data and a further **43%** are encrypting to some degree. That may sound like a reasonable number, but if you consider that over 700 million records were compromised in 2014[i]; then add in numerous high-profile breaches such as Sony, Experian, KBox and the Japan Pension Service where sensitive data wasn't always encrypted, the problem starts to become clear.

Further divisions emerge when comparing encryption levels in companies of different sizes. Only 38% of smaller organizations (100-500 employees) are encrypting extensively, compared with 50% of larger organizations (501-2,000 employees). According to a 2014 Verizon report[ii], 53% of confirmed data loss incidents were in organizations of less than 1000 users.

World-wide similar conclusions can be drawn. While encryption adoption is relatively mature in the U.S., where 54% of organizations are making extensive use of it, only 26% do the same in Malaysia.



Organizations making extensive use of encryption to secure sensitive data

Why are organizations encrypting?

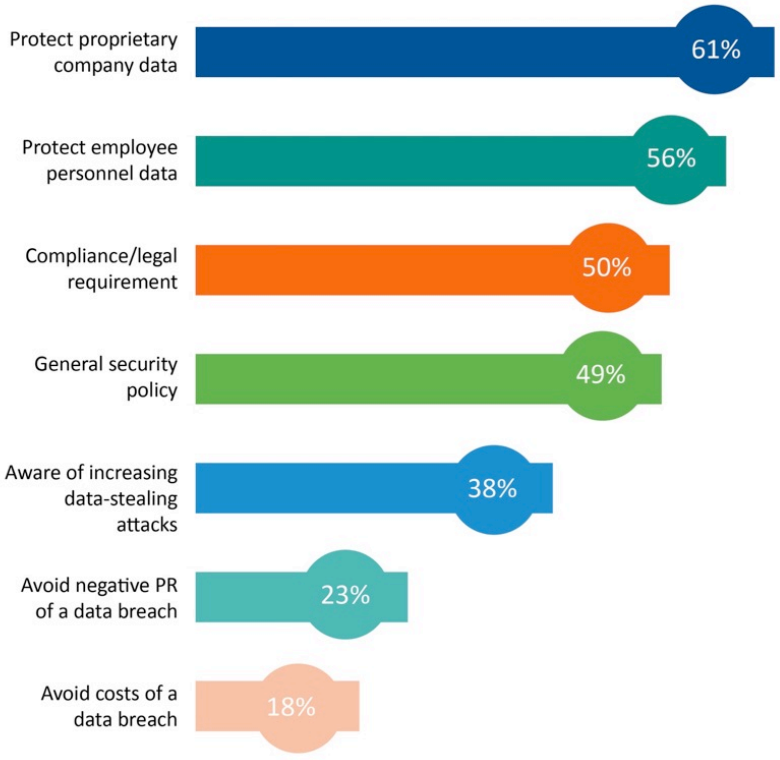
As you would expect, organizations are encrypting their sensitive data for a variety of reasons, based on both internal and external factors.

To protect proprietary company data came out as the top encryption driver with 61% of companies citing it as a reason they encrypt sensitive information. This translates into it being the top reason for four out of six countries and both smaller and larger companies.

Taking the number two spot with 56% is *to protect employee personnel data*, with the US being the only country to rank this as its top reason.

Unsurprisingly, the heavily regulated financial sector identified *compliance/legal requirement* as its main driver for encrypting. Japan also chose *compliance/legal requirement* as its number one, the only country to do so, which reflects the legislative situation in that country.

On-going, high-profile data breaches seem to be having an effect in driving people to protect their data with encryption – 38% of organizations cite it as a reason to encrypt, with India (49%) and Malaysia (45%) rating it particularly highly.



What drove your organization to encrypt sensitive data?

Data and devices – the winners and losers

Now that we've seen why organizations are encrypting, let's take a look at whether they are achieving their goals.

To recap, the top two reasons that organizations are encrypting their sensitive data:

- To protect proprietary company data
- To protect employee personnel data

Data security

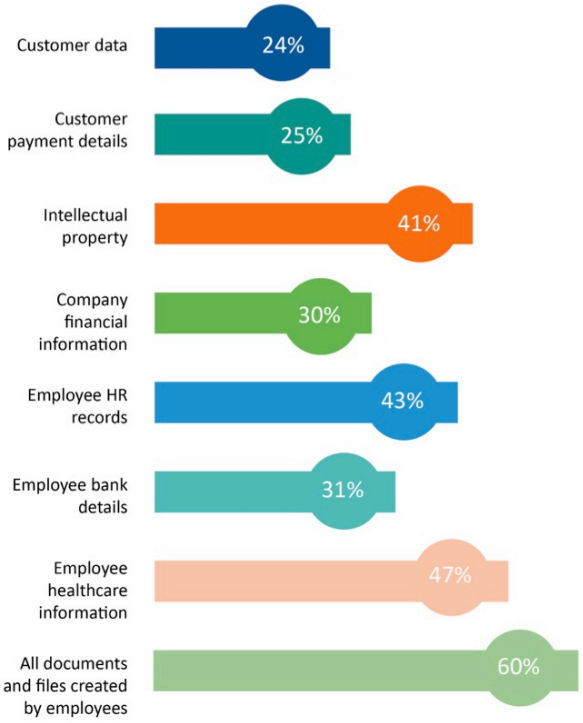
Unfortunately these good intentions aren't always translating into security action. A little over a third (31%) of organizations don't always encrypt their financial information and 45% are failing to always encrypt their intellectual property.

Customer data fares better, but even so 25% of organizations aren't always encrypting customer payment details.

This story takes a turn for the worse when employee data is brought into the mix. 31% of organizations are not always encrypting employee bank details, 43% aren't always encrypting HR records and 47% aren't always encrypting employee healthcare information.

That many organizations are taking the security of their customer data seriously is an encouraging trend, but this shouldn't and doesn't have to be done at the expense of other data types. Our findings indicate that currently, organizations are giving their employee data the short end of the security stick.

What data is not always secured with encryption?



Device security

There are holes in organizations' encryption strategies when it comes to types of data that are protected, but does the same apply for devices? Yes. Particularly in regard to 'newer' technologies which are being left behind when it comes to data security.

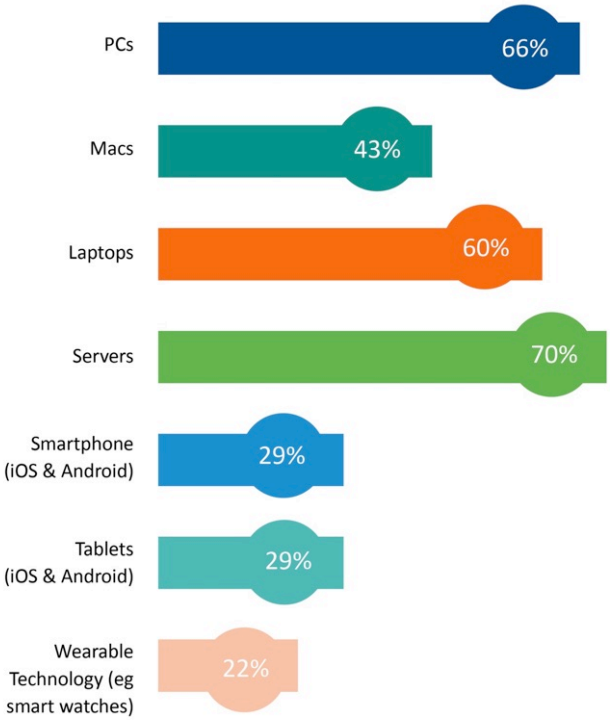
As you would expect, 'traditional' business devices are relatively well accounted for. 70% of organizations always encrypt their servers, 66% their PCs and 60% their laptops.

But despite Macs becoming a more prominent feature in many IT setups, this isn't always translating into increased security. Only 43% of organizations always encrypt their Macs making them a common data security weak-spot.

This security hole only widens when you take into account smartphones (29%) and tablets (29%), both of which are seeing a rapid increase in business use. These are a particular cause for security concern as more and more people are using them in their day to day working lives.

When it comes to device choice – user convenience and productivity are coming to the fore, with data expected to stay available and stay secure.

Unfortunately in the wider world, data security via encryption is playing catchup when it comes to these trends.



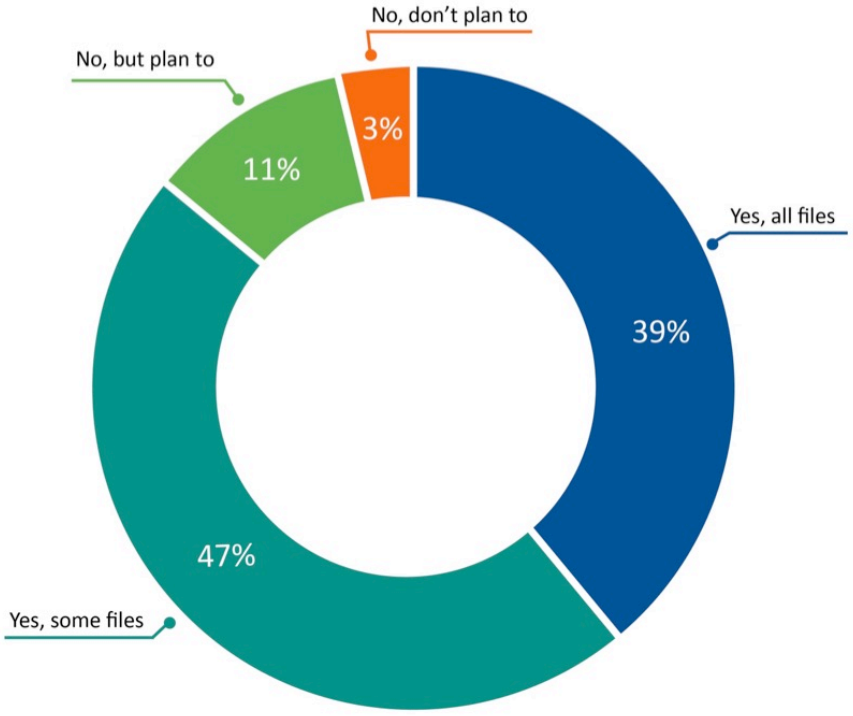
What devices are always secured with encryption?

Data in the Cloud – The new Wild West?

84% of organizations are concerned about the security of data that is stored in the Cloud. And with good reason.

When you store data in the Cloud, do you know where it is actually held? Who has access to it? Do you have control of the encryption keys or are they controlled by your cloud service provider?

Despite these concerns 80% of organizations permit their company data to be stored in the Cloud. With strong encryption uptake this wouldn't be a reason for concern, but of those organizations that allow data to be stored in the Cloud, only 39% are encrypting all of the data that they put up there. And as a result, potentially sensitive data is being left vulnerable in the event of a data breach.



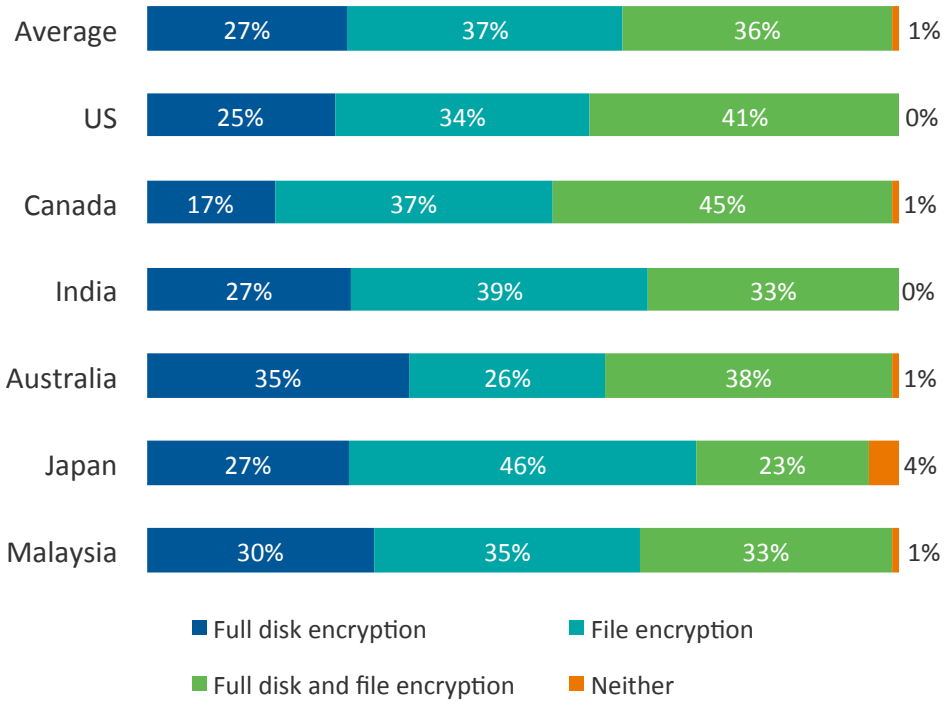
Does your organization encrypt files that are stored on cloud-based storage solutions (e.g. Dropbox, Google Drive, OneDrive, etc.)?

Types of encryption – Full disk, file or both?

Where they are choosing between the two, more organizations are using file encryption (37%) than full disk encryption (27%). However 36% of organizations are using both full disk and file encryption – given they are complementary technologies this is a wise approach.

Full disk encryption keeps the entire disk secure, which means that in the event that a device is lost or stolen, the data will be kept safe. *File encryption* works by encrypting individual files, meaning that when they leave the originating device they stay secure (which is not the case with full disk encryption). So in effect, 36% of organizations are getting the best of both security worlds.

Canada (45%) and the US (41%) are leading the pack when it comes to using both types of encryption and from an industry perspective, Telecoms (50%) and Financial services (41%) are ahead.



What types of encryption products are your organization using for their sensitive data?

Barriers to encryption

Encryption is a valuable security tool to ensure that even in the event of a breach your data cannot be read or used against you. So why is something so effective not standard practice for all organizations?

1. **Lack of budget 37%**
   The top reason cited by organizations that aren't making extensive use of encryption is lack of budget. It's an understandable concern. But it's worth considering whether the initial financial outlay outweighs the significant potential cost of a data breach, both financially and to an organization's reputation.

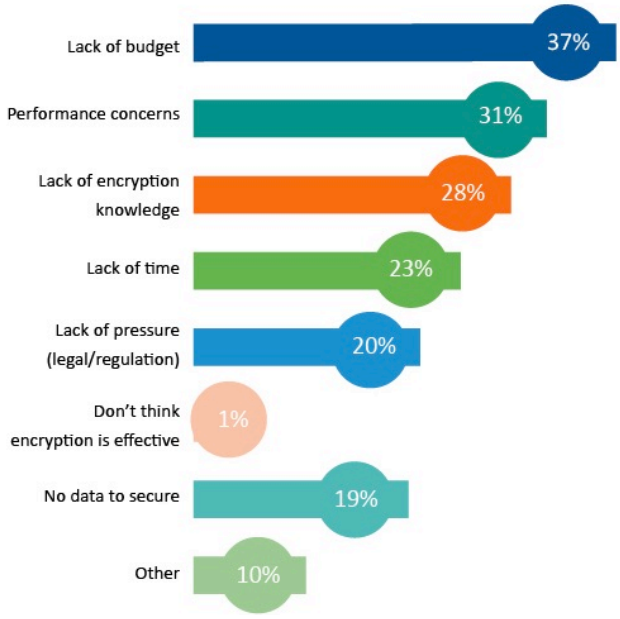
2. **Performance concerns 31%**
   A popular encryption myth is that it will kill database and application performance. Properly designed and implemented encryption will not only protect your critical data, but will have minimal performance impact that is imperceptible to users.

3. **Lack of encryption deployment knowledge 28%**
   Encryption has a reputation for being complex and costly. Finding the right IT partner will help you to navigate smoothly through the encryption process and deal with questions such as identifying what data needs to be encrypted, where it lives and who needs access to it.

In addition to these top three encryption barriers, a fifth of organizations cite a lack of legal or regulation pressure as a reason to not encrypt. A further 19% think that encryption is not an effective tool for securing sensitive data.

These are worrying results given that a business' success is increasingly reliant on its ability to leverage - and by extension *protect* - its data.

Learn more about encryption and how you can get started



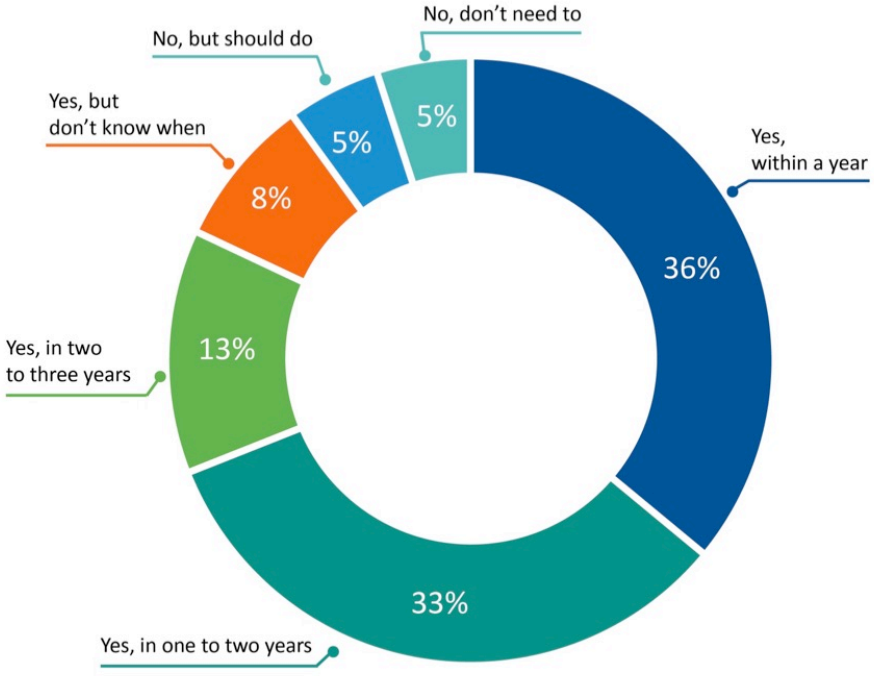
Why does your organization not always use encryption to secure sensitive data?

The future is securing data with encryption

While encryption today isn't as widespread as security experts would hope, the signs are encouraging.

The majority of organizations are in agreement that improvements to the way in which data is stored need to be made. 75% agree that employee data storage needs improvement, 74% agree for customer data and 77% for company data.

This ties into what organizations are planning for the future. 97% of organizations polled in this survey are already using encryption to at least some degree or plan to in the future. Of these, 69% are planning to extend their data protection approach with encryption over the next 1-2 years.



Does your organization plan to extend their data protection using encryption?

Conclusion

Encryption security practices haven't kept up with the modern worker. While businesses are seeing increasing use of macs, smartphones and tablets, this isn't being mirrored with a corresponding increase in data security via encryption. As a result, these devices are weak spots in many organizations' security posture.

These security gaps also exist when it comes to encryption of different types of sensitive data. Understandably while most businesses are giving a high priority to securing their customers' data, the same can't always be said when it comes to protecting their employees' data. Despite being highly motivated to secure their employees' data, the reality doesn't match up with the intention.

Data stored in the cloud is also at risk, with the percentage of organizations **always encrypting data (39%)** being much lower than those who **permit cloud storage (80%)**.

The good news is that despite these current security holes, the majority of organizations agree that changes should be made and plan to extend their data protection strategy with encryption in the near future.

Next steps

Encryption is the foundation of any data protection strategy. If these survey results encourage you to review your own strategy, Sophos recommends you start by answering the following questions:

1. **How does data flow into and out of your organization?**
   Do you receive emails with file attachments, or send them out? Do you receive data on USB sticks or other forms of removable media? How does your organization store and share large amounts of data internally and externally? Do you use cloud based storage services like DropBox, Box, OneDrive, etc.? What about mobile devices and tablets?

2. **How does your organization and your people make use of data?**
   What are their workflows and how do they go about making their day-to-day jobs more productive? What tools, devices or apps do they use and do any of those present a possible vector for data loss?

3. **Who has access to your data?**
   This topic can be both an ethical and regulatory discussion. In some situations, users should not ethically have access to certain data (e.g., HR and payroll data).

4. **Where is your data?**
   Centralized and mostly contained in a data center? Completely hosted in the Cloud? Sitting on employee laptops and mobile devices?

As a recognized Leader in encryption, Sophos has many years' experience in helping organizations secure their data with encryption. We would be pleased to help if you would like support in moving forward with your encryption strategy.

Survey methodology

In total 1,700 IT decision makers were interviewed across the US, Canada, India, Australia, Japan and Malaysia.

All respondents were from organizations with 100-2,000 employees and organizations were from all sectors (excluding government).

The research was conducted by Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

[i] Verizon. (2015). 2015 Data Breach Investigations Report

[ii] Verizon. (2015). 2015 Data Breach Investigations Report

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

2015.12.09 WP-NA (GH)