SOPHOS
simple + secure

CLASS
NETWORKS

Eight things senior managers need to know about data encryption

Securing sensitive data is a must for every organisation. Today's encryption solutions don't slow down your users, so you're not compromising productivity for security.

Here are eight things senior managers need to know about encryption to keep their data secure.

1. Every organisation holds sensitive data
   Sensitive data is anything you don't want to fall into the wrong hands, and every organisation has it. No matter how big or small your company, as long as you have staff on your payroll you have sensitive data you need to secure. It includes your staff's salaries, bank account numbers, customer credit card numbers, trade secrets and health records, to name but a few.

2. Data loss happens
   The IT industry has been striving for decades to let us share data quickly and easily. It has been hugely successful. We now expect, even demand, that complex information can cross the globe instantly, and be available wherever we are—work, home, out and about.

   The downside of this IT progress is that it's now easier than ever to lose data. Most of us have sent an email to the wrong recipient in error—hoping that it didn't have a sensitive attachment. Furthermore, you can upload files to USBs and CDs in seconds, which then can easily be lost. Not forgetting the now-ubiquitous mobile devices such as laptops, tablets and smartphones which are specifically designed to let us access data outside the workplace. Accidental loss accounts for 75% of all data breaches, so it's an obvious candidate for security focus.

3. Criminals are after your data

The days of writing viruses for fame and glory are long gone. Much of today's malware is created specifically to steal data undetected. Some data, like credit card numbers, is obviously valuable and a target for the bad guys. However, they are increasingly targeting diverse, less obvious data and finding ways to profit—from email addresses to company intellectual property.

Of course, hackers are not the only data thieves. Organisations also need to beware of rogue employees stealing data as well as the theft of USB storage devices and other hardware containing sensitive information.

4. Losing sensitive data can cost you dearly, even if you don't get fined

Many countries and industries have specific financial penalties for data loss (such as U.S. healthcare regulations, or the UK Information Commissioner's ability to levy £500,000 fines).

However even if you are unlikely to incur a regulatory fine, the penalties can still be severe. These can include the financial costs of cleaning up the leak, such as notifying the affected parties and protecting them against future damage (for example, insurance against identity theft). Worse still, should lost R&D secrets get into the hands of your competitors it can have long-term implications for your bottom line. Reputation damage is also an increasing risk as consumers become more aware of the damage of data loss.

Your employees are also a significant factor. Just imagine what would happen if people's salaries got out. Or if news of an impending merger or acquisition leaked. The loss of employee trust and commitment, along with the costs of staff attrition, could impact you financially too.

To work out the financial implications of a data breach for your organisation, consider first what sensitive information you hold. Then think about the costs you could incur if it falls into the wrong hands. For example, if your customer database is a key asset, how much would it cost you in lost sales if a rogue employee took it with her when moving to a competitor? Consider the clean-up costs of telling your customers that you've lost a CD containing their credit card numbers, as well as the future business downturn due to loss of trust.

Having a view about what you have to protect and how you could lose it will help you make sensitive data control decisions.

5. Data encryption isn't a one-size-fits-all solution

If your data is encrypted it can't be read by the wrong person. However, each organisation has different encryption needs. The right solution for you will depend on many factors, including the types of data you hold, what you do with the data (for example, if you send it by email or share it with third parties), the industry you work in, and the resources at your disposal. Those working in highly-regulated industries will need more stringent solutions with comprehensive reporting capabilities. While others may just need to make sure a lost laptop isn't going to casually reveal data.

There are three states of data:

- **at rest** e.g. stored on a computer or server
- **in use** e.g. being actively used, such as someone working on a payroll spreadsheet
- **in transit** e.g. being moved around, such as being sent by email or carried a USB drive

When considering how to protect your sensitive data, you need to think about what data you have in each of these three states. If you store a lot of data on laptops and USB drives then device encryption is essential. If sending sensitive attachments is a potential issue then email encryption is a sensible option.

Encryption solution	What it secures
Full-disk encryption	Data stored on desktops and laptops
File and folder encryption	Data on central servers
Removable media encryption	Data on portable devices such as USB drives, CDs, removable hard drives
Cloud encryption	Data that is stored on the Internet, such as in Dropbox
Email encryption	Data sent by email, either in body copy or as an attachment

6. It doesn't have to be costly or complex either

There are a number of encryption options for organisations to choose from. These range from straightforward encryption that's automatically integrated in your endpoint security to government-level solutions.

7. Encryption is just part of the solution

Yes, encryption is central to securing your data, but user education is also crucial. Data only exists because people use it, and it has no value if people can't access it. While technology can significantly reduce your risk of data loss, it can never eliminate it. So alongside putting the right technology in place you also need to educate your users.

Other technologies that work to complete the data security picture include device control, application control and anti-malware products.

8. Data security—what's coming next

It is broadly agreed that we are in an information and knowledge economy. In the short term 4G, the next generation of smartphone connectivity, will give download speeds of up to 100Mbps as standard. That means entire databases can be downloaded in seconds, to any device and in any location across the globe. Smartphones and tablets will eclipse the traditional PC as the devices of choice for business users.

In a recent survey Sophos conducted with Computing, 70% of business users have one smartphone for both business and personal use. This will increase the mobility of data and blur the home-work boundaries even more.

0800 160 1920
contact@classnetworks.com
www.classnetworks.com

CLASS NETWORKS

© Copyright Sophos Ltd. All rights reserved.
All trademarks are the property of their respective owners.

SOPHOS