IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

Adopting Encryption – Five Top Tips for SMEs

Bernard Parsons

Bernard Parsons
CEO and Co-Founder
Becrypt

Biography

Bernard Parsons is the CEO and Co-Founder of Becrypt (www.becrypt.com).

Establishing Becrypt in 2001 with the aim of addressing the growing security requirements of endpoint technology, Bernard has built the company into a leading supplier of end-user device security products and services, with a focus on product assurance, multiple platform support and flexible delivery: from being embedded within the platform, to hosted within the Cloud.

Furthermore, Bernard has ensured Becrypt helps the most security-conscious organisations to be positioned as leaders in enabling value from the use of secure technology.

For his dedication to digital technology, Bernard was bestowed with an MBE in the 2018 New Year's Honours List.

Keywords Disk encryption, Cyber security, Device security, Sensitive data, Encryption, GDPR
Paper type Opinion

Abstract

Whether you are a large enterprise or small business, you have to be more vigilant than ever when it comes to protecting your confidential data. For small businesses, typically organisations that are looking at adding encryption for the first time, driven by regulation such as GDPR – securing sensitive data must be a top priority. Based on on the experience and feedback that Becrypt has attained, the author of this article summarises the top-five issues that small businesses should think about if they are looking at adopting disk encryption, or if they're looking at undertaking wider rollouts of disk encryption.

Introduction

Data breaches are in the headlines almost every day. When these breaches occur if encryption is not implemented, then the data is at risk of being released to the public or utilised for malicious purposes. As small companies begin to evaluate and seek to harden their security focus in the face of these varied threats to their confidential data, they need to ensure that ensure encryption plays a major role in that strategy. Here are our top tips to make this possible:

1. Ease of use

Organisations must look for products that are easy to use, easy and quick to install; an obvious requirement that is partly about reducing the time and expertise required to install products in the first place. But an important

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

subsequent point is also total cost of ownership. If a product is not easy to install, it is usually a good indicator that actually there is a level of complexity that will remain as a long-term business overhead.

The more complex a product is, the more complexity there is to manage, leading to higher levels of required expertise and the more potential for support issues to occur over time, driving up the product's total cost of ownership for the organisation.

2. Accessible support

Encryption can be a business-critical asset, as well as a business-enabling technology. It is therefore important that you are working with an organisation – whether that's a vendor or the vendor's partner – that can offer good, and accessible technical support to you.

Even if you get the first point right, choosing a product that is easy to use will reduce the amount of required technical support. However, you should still think about the potential for requiring support over the total life of the product because in a couple of years, the business may be looking at doing something slightly differently, such as looking at encrypting new devices that may be non-standard (such as RAID Servers), and you will need to ensure that you can pick up a phone and talk to someone with sufficient expertise.

The option of phone-based support is important; being able to jump onto a call in a reasonable amount of time and actually talk to an expert. Therefore, we would certainly recommend testing this process with a vendor or the partner before you go ahead and procure.

3. Proof of encryption

A good first step is to encrypt laptops, as it seems there will always be someone within the organisation who will lose their laptop. Encryption turns what would potentially be an information-loss, into just the loss of a physical asset, protecting the organisation's information and addressing the organisation's liabilities.

However, under regulation such as GDPR, there is often a requirement to prove that devices actually were encrypted in the event of a loss, in order to avoid some of the reporting requirements within these regulations. Proving that a device loss is not an information loss and avoiding the need to undertake breach notification, is something you want to be able to think about in advance. If you are deploying a product that includes centralised management, that functionality should already be there. But many small businesses will choose to deploy in a more stand-alone configuration, without the need to stand up a central management platform.

With standalone installs, it is important to ensure that the product has a reporting capability of some kind, such as online, so that the encryption status of your estate of devices can be reported.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

4. Extendibility

In the first instance, you may be looking at deploying encryption within an estate of Windows devices. But it could be the case within a year or two that you have other requirements; you might need to manage encryption on Mac devices, or on smartphones and mobile devices within that same suite of products. Therefore, it is a good idea to look for vendors that have multi-platform offerings, helping to future-proof your technology choice. This will ensure that you are not tied to a vendor, but at least ensuring that your existing vendor is an option as your requirements grow.

5. Best Practice

It is a good step to encrypt devices, and be able to prove that you have encrypted them. However, there is an increasing regulatory requirement to demonstrate that you have gone through some process of ensuring that the technology you are adopting represents best practice. For example, GDPR explicitly references ‘state-of-the-art’ technology.

To fully ensure that you are managing liabilities, you need to evidence that you are not just adopting technology, but that it's appropriately ‘state-of-the-art’. Achieving this level of confidence can only be done by looking at technology that has third-party validation, normally through product assurance or product certification. This provides independent validation that the product is of an appropriate quality.

There are a variety of common certification schemes relevant for encryption products. One of these is the US standard, Federal Information Processing Standard (FIPS), which ensures that algorithms have been correctly implemented. However, organisations must be wary of adopting technology just because it has a FIPS certification. The majority of products use the same algorithms, such as Advanced Encryption Standard (AES); FIPS ensures that a third-party has validated that the vendor has correctly implemented the algorithm.

This is similar to having a locksmith check the quality of your house locks, confirming that they are of good standards. However, they are not going to mention anything about whether you frequently leave all the windows open every time you leave. FIPS will tell you that the algorithms have been implemented correctly, but vendors can, and still do, implement products inappropriately that leave vulnerabilities.

A good example of such vulnerabilities in encryption products is within Solid State Drives (SSDs). Recent research from Radboud University in The Netherlands has highlighted vulnerabilities in not just one vendor, but a whole range of vendors’ SSDs. The fundamental reason they highlight, is that actually implementing encryption well is not easy, and it is easy to make mistakes. Vendors can take shortcuts, which means that security researchers can then find resulting vulnerabilities; in this case they were able to bypass the encryption within SSDs.

Organisations are better off looking for certification schemes that are more comprehensive. One example is the Commercial Product Assurance (CPA) scheme, run by the UK National Cyber Security Centre (NCSC). CPA works alongside FIPS for validating algorithms, but it says more about the overall product quality and implementation, looking at the security architecture to make sure that it has been designed and implemented in a sensible way.

It also looks at the vendor coding and build standards, thereby reducing the risk of there being a vulnerability in the product. The risk is never fully mitigated, but it certainly goes down to a point that allows you to say that, as an organisation, you are adopting best practice.

Alongside security and liabilities, organisations also to be concerned about the cost of being caught out by products with publicised vulnerabilities. Subsequently, they also need to think about the cost of then changing to a different solution.

Conclusion

In summary, these are the five things that we would suggest organisations, particularly SMEs, want to think about as they adopt encryption. It's not rocket science and most good vendors, or their partners should be able to easily walk you through these steps.