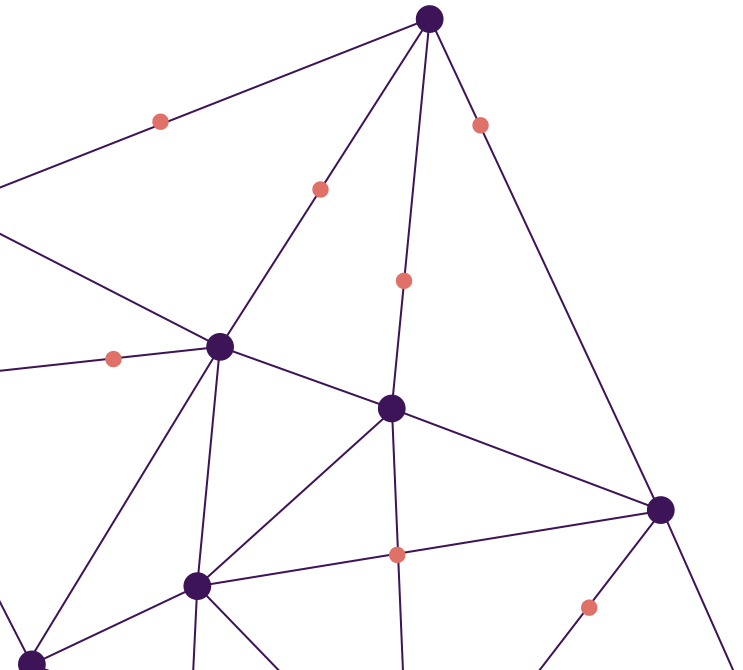
Briefing Paper

Protecting your business from data theft

Why it matters, common mistakes and practical solutions

#becrypt.com



Commercial Sector

This section at-a-glance:

- The value of a business increasingly depends on its confidential data and intellectual property
- Many businesses are not adequately protecting their data at rest
- Data theft costs US businesses billions of pounds every year
- This paper addresses the mistakes businesses are making and provides best-practice protection guidelines

Why you need to read this paper

For many businesses, an increasing share of their value comprises proprietary data, unique Intellectual Property (IP), insights, trade secrets and other confidential information that's stored digitally within their organization.

But – and it's a really critical 'but' – despite the huge amounts of money spent on cyber security, significant number of businesses are suffering potentially critical losses of value because of their failure to adequately protect their data at rest. That's the data stored on the numerous tablets, laptops, desktops, servers and removable media being used across their business. It's a glaring hole in the cyber security strategy of far too many companies.

Theft of confidential data – whether extracted from stolen devices or copied from poorly protected machines – is costing US businesses billions of pounds every year.

This paper looks at some of the common mistakes that are leaving businesses unnecessarily exposed. We also provide a set of best practice recommendations that all businesses should be following to protect themselves from the risk of IP theft.

Despite the huge amounts of money spent on cyber security, businesses are suffering potentially critical losses of value because of their failure to adequately protect their data at rest

This section at-a-glance:

- The non-quantifiable value is even bigger
- Data is increasingly a source of competitive advantage and business value
- The impact of data breaches include regulatory fines, lost customers and lower profit margins
- The US has the highest data breach cost in the world

Data drives business value

In a world where ideas, information and innovation are the key drivers of value, protecting data has never been more critical for businesses of all types.

In many sectors a firm's value is largely dependent on the intellectual property and proprietary know-how that exists within their business, whether it's drug formulas in Pharmaceuticals, software code in Technology, customer data in Retail or exploration data in the Oil and Energy.

The quantifiable value of IP is huge – a study by the World Intellectual Property Organization (WIPO) found that the global IP market now produces $180 billion a year in licensing fees and royalties (up from $2.8bn in 1970).[1]

But this actually represents only a fraction of the total value to businesses of their digital data assets. That value is increasing as businesses get better at exploiting the potential of data to yield new insights and enable new business models. In one recent global survey of senior decision-makers, 61% of respondents acknowledged that "data is now a driver of revenues in its own right and is becoming as valuable to their businesses as their existing products and services."[2]

Loss of data is loss of competitiveness

The damage caused by a cyber-criminal stealing your confidential customer information or a competitor gaining access to your IP can be huge. The impact of stolen data can be felt in multiple ways, including:

- **Lost sales and lost customers**
- **Damage to reputation**
- **Lower profit margins**
- **Regulatory fines**
- **Loss of jobs**

In recent years there have been numerous examples of major data breaches that have caused significant damage to the companies affected, including Target, JPMorgan Chase, Target and Adobe Systems. 61% of organizations now think data theft is the greatest threat to their reputation.[3]

61%
of organizations
now think data theft is the greatest threat to their reputation

This section at-a-glance:

- Trade in stolen data is now big business
- The majority of data breaches are a result of either malicious attack or human error
- When breaches do occur, the costs are significant and increasing

The threats to your data are substantial and growing

Whether it's organised criminal gangs, unscrupulous competitors, hostile states or opportunist thieves, there are many people out there keen to get hold of an organization's valuable data. Trade in stolen data is now big business.

Breaches from cyber attacks are common and increasing. In the US alone, there were 781 publicly reported data breaches in 2015. Of these nearly 40% were in the business sector, and 35.5% in the Health/Medical sector.[4]

While the causes of data breaches are varied, the majority are a result of either malicious attack or human error. Recent research into the root causes of data breaches found that 47% involved a malicious or criminal attack, and 25% involved a negligent employee or contractor.[5] In 2015 there were 182 data breaches in the US attributed to a malicious insider.[6]

And when breaches do occur, the costs are significant and rising. The US has the highest cost per data breach in the world, at an average of $6.5m per breach.[7]

$6.5m
average cost of a data breach in the US.

In 2015 there were 182 data breaches in the US attributed to a malicious insider

This section at-a-glance:

- Mobile working is increasing exposure to data theft from a laptop, desktop or mobile device
- Data breach losses include the value of the data; the increased risk of a targeted attack on the company's people and systems; and fines levied by regulatory authorities

Theft from devices is a common source of data breaches

Enabling a workforce to be productive increasingly means allowing personnel to work and access systems and information anytime and anywhere. But the trend toward more mobile working is increasing exposure to IP theft from a laptop, desktop or mobile device.

Theft of data from devices may fall into the category of human error, such as a briefcase left on a train or a laptop carelessly disposed of. Enter the opportunist thief. Alternatively, data theft may be a deliberate, malicious act – the work of a disgruntled employee, say, or a corporate spy taking advantage of an unattended machine to copy confidential company data onto a USB drive.

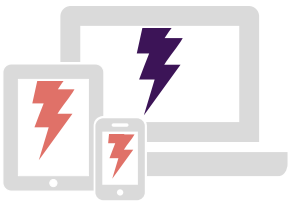
Unencrypted laptops leave personal data at risk

There have been numerous recent examples of lost or stolen laptops resulting in data breaches. In August 2015 an unencrypted laptop thought to contain patient data was stolen from a former physician at the University of Oklahoma, while a few months previously Oregon Health Co-op reported a data breach involving the records of 15,000 members stored on a stolen laptop.

The problems aren't confined to healthcare though. In May 2015 SterlingBackCheck, a New York-based background screening service, revealed that data on 100,000 people, including social security numbers, had been compromised as a result of laptop theft.

The losses arising from such an incident typically fall into three categories:

- The value of the data stored on the device itself – this could range from the thousands to the millions of pounds, depending on the nature of the data.
- The increased risk of a targeted attack on the company's people and systems – the typical corporate laptop contains a wealth of information that could help a cyber criminal further penetrate an individual or an organization's defences.
- Fines levied by regulatory authorities, particularly if the breach involves a loss of personal information – in June 2012 for example, a hard drive containing unencrypted Electronic Protected Health Information (ePHI) was stolen in Alaska from an employee of the Alaska Department of Health and Human Services (DHHS), leading to a $1.7 million fine.



Data on 100,000 people, including social security numbers, was compromised as a result of one laptop theft

This section at-a-glance:

- Companies lack data management and protection policies
- Lack of data at rest protection is based on common misconceptions
- Security that's too rigid is almost worse than no security at all
- Central visibility and control of data, devices and usage is vital

Businesses are failing to protect themselves

Despite significant investments in cyber security products in recent years, many businesses are failing to adequately protect themselves from IP theft. The most common problems we see are:

Policy black holes

Too often, companies simply lack policies governing how data is managed and protected on portable devices. This is often accompanied by limited awareness among employees about the implications of their actions and what they can do to reduce risk.

Failure to protect data at rest

Frequently, businesses fail to adequately protect data stored on desktops, laptops and portable media – their data at rest. This glaring hole in their cyber security strategy tends to be allied to a number of common misconceptions:

- Many businesses assume that, because users need to enter a password to log on to their Windows domain, their data is protected. It's not. Any moderately determined cyber criminal could still easily access the data stored on the devices' hard drive.
- Many companies have invested in Endpoint Protection products to protect devices from malware and targeted attacks, assuming that this offers adequate protection for their data. It doesn't. If someone has actually got hold of the physical device, or copied data on to removable media, then most Endpoint Protection products do nothing to protect that data.
- Some organizations have gone further and invested in full disk encryption. But even that doesn't offer full protection if data can be easily copied onto unencrypted portable media (such as USB drives and smartphones).

Over-restrictive or complex security

It's important to appreciate that making security too restrictive or complex is almost as bad as having no protection in place at all. If security prevents people doing their jobs effectively, employees are likely to find ways to bypass it. This creates new vulnerabilities that the company may have even less awareness of and ability to control.

Limited visibility and control

Even businesses that are aware of the issues are often hindered by limited central visibility and control of their data – they are not clear about what data actually exists, what devices are being used to store that data and how the data is being used and copied.

This section at-a-glance:

Our top 10 best practice guidelines:

1. Understand what you've got
2. Have effective policies in place
3. Use industry-certified encryption
4. Protect against leakage from removable media
5. Don't reply on single layers of security
6. Keep it simple and seamless for the user
7. Don't get in the way of people doing their jobs
8. Have effective management controls and auditability
9. Limit administrative complexity
10. Educate your users

Top 10 best practice guidelines

Based on our 15 years' experience of helping governments and businesses secure their valuable data, we've identified the following top 10 best practice guidelines for keeping your IP safe from theft.

1. Understand what you've got and the relative value of your different types of data

It's impossible to design and implement an effective security policy unless you know:

- what types of data are being stored on your employees' devices
- the relative impact of different types of data being lost or stolen

2. Ensure you have effective policies in place to limit your risk exposure

It's vital that you have policies in place to govern how your data is stored, copied and shared – particularly in relation to removable devices and media. Review and refresh these policies regularly to ensure they reflect both the changing needs of your business and the evolving nature of cyber threats.

3. Use industry-certified encryption to protect your data at rest

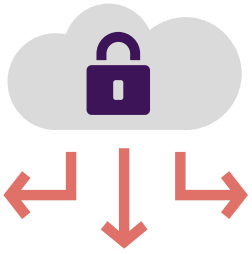
Implementing full disk encryption across your device estate significantly reduces the risks of your valuable IP being compromised via a lost or stolen device. It also helps to limit the impact of a breach if one does occur. But be aware that not all encryption products are created equal – it's important to use technology that has the validation of industry-standard certifications.

4. Protect yourself against data leakage via removable media

More breaches occur from data being copied onto removable media and devices, rather than lost or stolen laptops. Even if the copying is for a genuine business reason (rather than malicious intent), it still creates increased risk. A USB drive is far easier to lose or steal than a laptop. And the impact of such data leakage can be far more damaging because it's often invisible – reducing your ability to take remedial action. You need to control how data is shared via removable media, and ensure that any data that is copied to a peripheral device is fully encrypted.

5. Don't rely on single layers of security

Multiple layers of protection reduce your vulnerability to malicious or accidental breaches. For example, as well as requiring user authentication via password, you could implement technology on your devices that prevents the hard disk being unencrypted if removed from the device.



Implementing effective security measures begins with understanding what data is currently being stored and by whom; how is it being used and shared; and what it could cost your business if it fell into the wrong hands

In the 2015 Cost of Data Breach Study, extensive use of encryption was the second most important thing companies could do to limit the impact of any breach – second only to the use of an Incident Response Team[8]

6. Keep it simple and seamless for the user

The more complex your security procedures are for your users, the greater the likelihood of breaches as a result of their actions. For example, if your users have to remember separate passwords to authenticate themselves with your encryption solution, and then to log on to their Windows domain, they're more likely to start writing down their passwords on post-it notes stuck to their device. Enabling single sign-on to any device limits the impact on your users and reduces your risks.

7. Don't get in the way of people being able to do their jobs

If your security policies and technologies prevent people doing their jobs, they'll inevitably find a way to bypass those controls – creating a bigger problem than you started with. When implementing technology solutions, ensure they're flexible enough to meet the needs of your business and your users.

Blanket restrictions on being able to copy data to a removable media, for example, are clearly impractical. Sometimes people will have very valid reasons for needing to share data via a USB drive or copy something to a mobile phone. You need to be able to set policy at a granular level, based on users, domains or devices. And you need to ensure that the data you allow to be copied to removable media is always encrypted.

8. Ensure you have effective management control and auditability

Having the right technology on your endpoints is of limited value if you can't easily manage that technology and you don't have visibility of what your users are doing on their devices.

You need to ensure you have the tools that allow you to roll out new technologies centrally – such as disk encryption or port control – without relying on users to do anything or requiring your IT staff to physically touch the device. You also need monitoring and reporting on which devices have been encrypted and what data users are copying to removable media. This ensures that you can easily identify potential problems. And you need to be able to carry out a rapid risk assessment – accessing a full audit trail – if there is a problem. If you can't prove to regulators that you've taken all reasonable measures to protect your data, you're more liable to receive a substantial penalty.

9. Limit administrative complexity

The more tools that your administrators have to interface with to manage your devices, the greater the likelihood that mistakes will be made or things will fall between the cracks. You should look for tools that offer a 'single pane of glass' to manage your estate.

10. Take time to educate your users

Although having the right technology is important, ensuring the right user behaviours is equally critical in reducing your risks. It's vital that your people understand the value of the data they're storing, sharing and using – and the implications of their actions. In one recent survey, 43% somewhat or completely agreed that they have "no idea of the value of business data." Your people need to understand what your policies are and why they exist – particularly where these policies place restrictions on what they can do.

For more information on the Becrypt suite of data and endpoint protection solutions, visit **becrypt.com »**

[1] World Intellectual Property Report 2011, WIPO
[2] Big & Fast Data: The Rise of Insight-Driven Business, Cap Gemini/EMC, 2015
[3] http://www.securitymagazine.com/articles/print/85702-questions-to-determine-your-enterprises-cyber-attack-defenses
[4] Identity Theft Resource Center, 2015
[5] The 2015 Cost of Data Breach Study, Global Analysis Benchmark, 2015, Ponemon Institute
[6] www.breachlevelindex.com
[7] The 2015 Cost of Data Breach Study, Global Analysis Benchmark, 2015, Ponemon Institute
[8] The 2015 Cost of Data Breach Study, Global Analysis Benchmark, 2015, Ponemon Institute

How can Becrypt help?

Preventing your valuable IP and data from being stolen from laptops, PCs and portable devices, Becrypt's suite of data protection solutions safeguards the value of your business and reduces your risk of compliance failures.

Our disk encryption, port control and secure media solutions enable you to keep your important data secure. They ensure you don't have to compromise user productivity, while giving you full management control and auditability.

Securing your data at rest

Underpinned by strong user authentication, **Becrypt Disk Protect** provides highly secure, full disk encryption for laptops, PCs and Windows tablets – keeping your data secure in the event of the theft or loss of a device.

Preventing data leakage

Equipping you with full event reporting and audit trails, **Becrypt Connect Protect** defends you against data leakage and malware by preventing unauthorised access to, and use of, externally connected devices.

Flexible sharing without the risk

Supporting multiple users on a single device, **Becrypt Disk Protect** gives flexibility without the risks. The addition of **Becrypt mShare** allows your users to encrypt data on external storage devices such as USBs – giving them flexibility and portability while still protecting your data.

Easy implementation

Saving time and minimising the need for end-user involvement, **Becrypt Enterprise Management (BEM)** enables quick and easy roll-out of our data protection products across thousands of devices.

Full management control and auditability

The **Becrypt Enterprise Management's** centralised console gives you full visibility and control of user activity, enabling you to:

- easily create and apply policies
- carry out fast risk assessment in the event of a lost or stolen device
- deal simply with issues such as forgotten passwords

For quick, straightforward data protection across your device estate, contact:

dataprotection@becrypt.com
0845 838 2080

#becrypt.com/endpoint