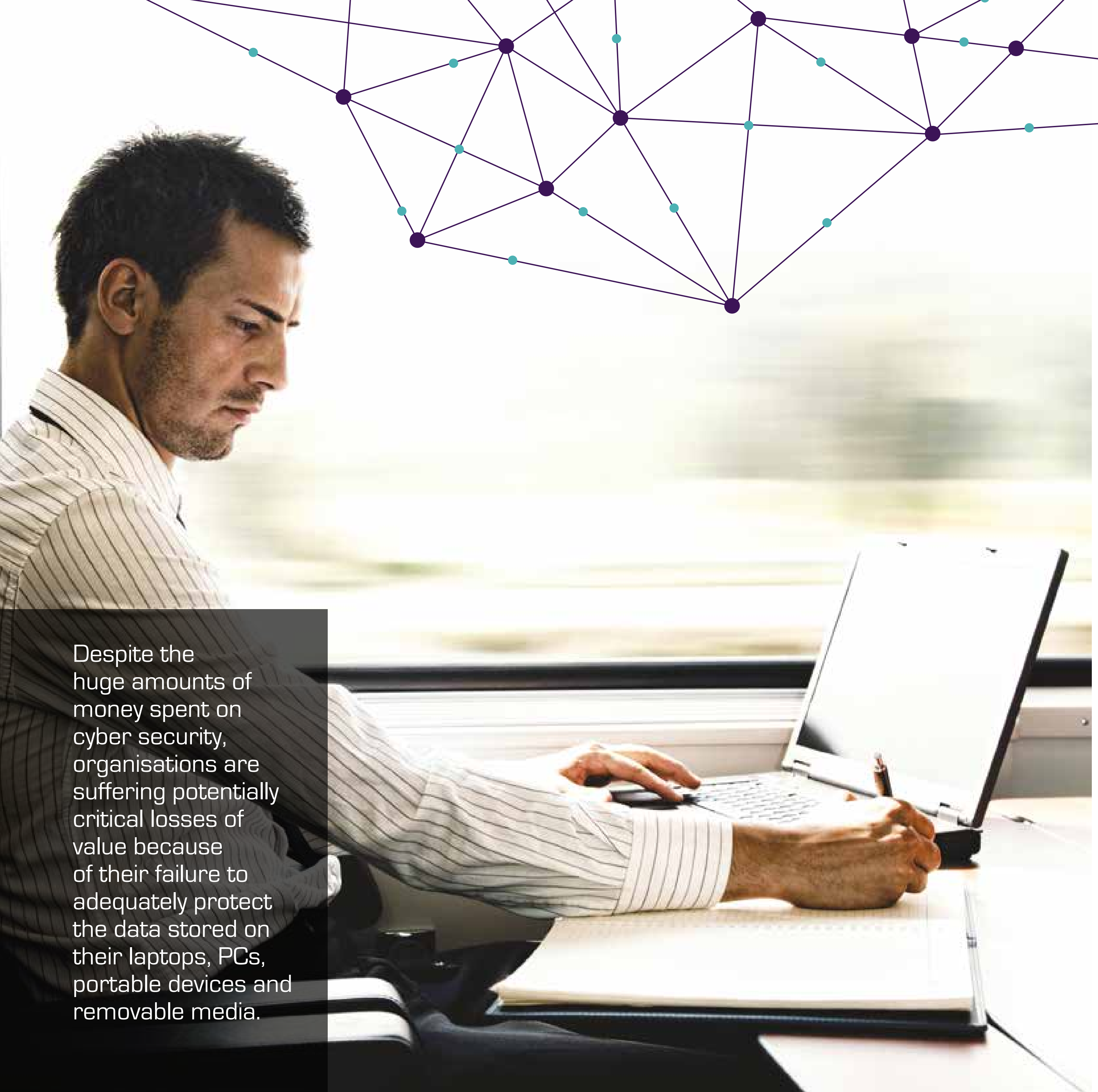
#becrypt.com

Are you protecting the value of your organisation?

How to safeguard your laptops, PCs and portable devices from data theft

GovernmentSector



Despite the huge amounts of money spent on cyber security, organisations are suffering potentially critical losses of value because of their failure to adequately protect the data stored on their laptops, PCs, portable devices and removable media.

Why risk the viability of your organisation?

For many departments, an increasing share of their value comprises of unique Intellectual Property (IP), insights, trade secrets and other confidential information that's held digitally within their organisation. Without effective safeguards in place, the loss or theft of the data stored across your laptops, PCs, tablets, smartphones and removable media such as USBs – your data at rest – can threaten your department's viability.

The cost of losing your organisation-critical IP and data

Theft of Intellectual Property – whether extracted from stolen devices or copied from poorly protected machines – is costing UK businesses billions of pounds every year.

The damage caused by an unauthorised party gaining access to your IP and confidential information – from designs and business plans to details of commercial negotiations and lists of existing clients – can be huge. The impact of stolen IP includes;

- **Lost sales and lost customers**
- **Lower profit margins**
- **Reduced ROI on R&D**
- **Loss of jobs**

Protection is vital – and easily implemented

While the negative impact of IP and data loss can be critical, safeguarding your business with effective protection is actually straightforward. With Becrypt's suite of data at rest protection solutions, you can quickly and easily ensure the data on your entire mobile device estate is safe in the event of loss or theft. What's more, you can do so without compromising the mobility and productivity of your people.

New European General Data Protection Regulation is introducing severe penalties for data protection compliance failures, with potential fines of up to 5% of worldwide turnover.

With Becrypt's suite of solutions, you can quickly and easily ensure the data on your entire mobile device estate is safe.

Why the threats to your IP are real and on the rise

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

Breaches from cyber attacks are common and increasing. A UK government report highlighted IP theft as the most damaging cyber crime for UK businesses, resulting in a loss of £9.2bn a year.[1]

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.[2]

And when breaches do occur, the costs are significant and rising. The same report found that the average cost of a data breach was $3.79m in 2014, up 23% from 2013.

Three common categories of data breaches

The losses arising from data breaches typically fall into three categories;

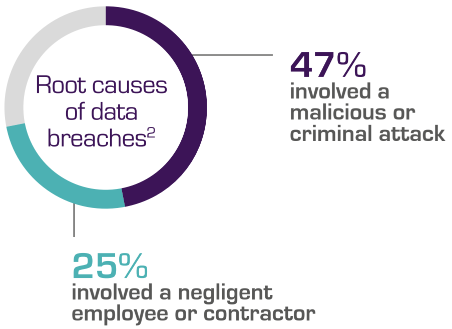
- The value of the data stored on the device itself – this could range from thousands of pounds to millions of pounds, depending on the nature of the data
- The increased risk of a targeted attack on the department's people and systems – the typical corporate laptop contains a wealth of information that could help a cyber criminal further penetrate an individual or an organisation's defences
- Fines levied by regulatory authorities, particularly if the breach involves a loss of personal information – last year, for example, the ICO issued a £180,000 fine to The Money Shop credit provider in response to the loss of computer equipment containing a significant amount of customer details.

IP theft is the most damaging cyber crime for UK businesses, resulting in a loss of £9.2bn a year.[1]

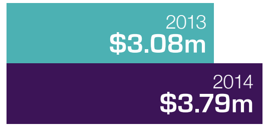
Four common categories of protection failure

The most common data protection failures can be summarised as;

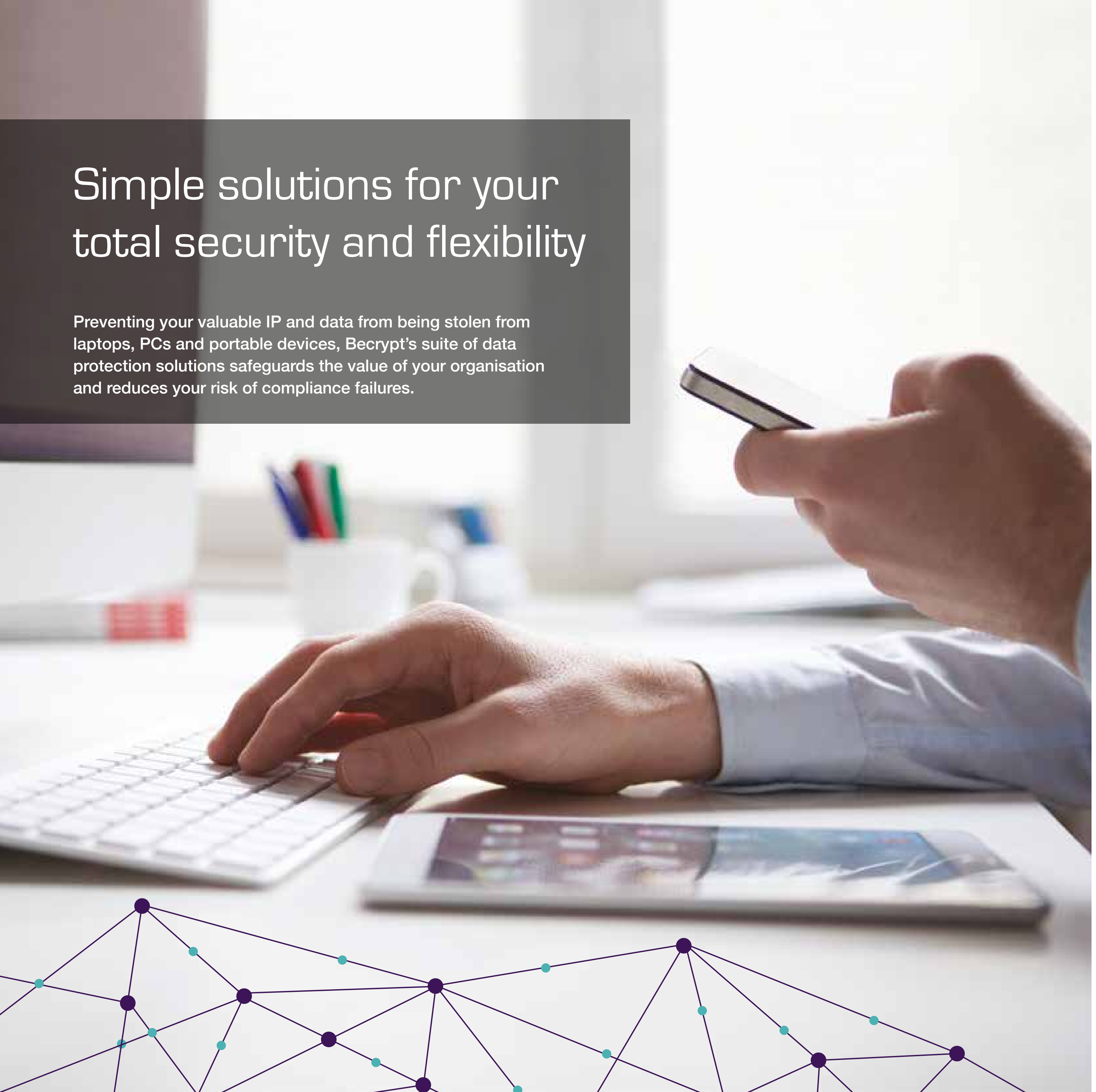
- **Policy black holes** – too often, organisations simply lack policies governing how data is managed and protected on portable devices
- **Failure to protect data at rest** – frequently, organisations fail to adequately protect data stored on desktops, laptops and portable media as a result of widespread misconceptions;
  - The assumption that, because users need to enter a password to log on to their Windows domain, their data is protected. It's not.
  - The assumption that Endpoint Protection products – safeguarding devices from malware and targeted attacks – provides adequate protection for their data. It doesn't.
  - The assumption that full disk encryption is enough. If data can be easily copied onto unencrypted portable media (such as USB drives and smartphones), it isn't.
- **Over-restrictive or complex security** – if security prevents people doing their jobs effectively, employees are likely to find ways to bypass it
- **Limited visibility and control** – even organisations that are aware of the issues are often unclear about what data actually exists, what devices are being used to store that data and how the data is being used and copied.



Average cost of a data breach has increased by 23% in 12 months:[2]



If security prevents people doing their jobs effectively, employees are likely to find ways to bypass it.



Simple solutions for your total security and flexibility

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 organisation and reduces your risk of compliance failures.

Secure your data at rest

Underpinned by strong user authentication, Becrypt's Disk Encryption, *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. Approved by the UK government to secure classified data (up to TOP SECRET), it is available in a number of approved variants to meet different levels of security. Encryption is applied transparently with no impact on user performance.

Prevent data leakage

Equipping you with full event reporting and audit trails, Becrypt's Port Control, *Connect Protect,* defends you against data leakage and malware by preventing unauthorised access to, and use of, externally connected devices. Policy can be applied at device, user or group level, and devices can be white-listed by make/model, individual unique device ID or by a signed device process.

Flexible sharing

Supporting multiple users on a single device, *Disk Protect* gives flexibility without the risks, providing multi-user support at pre-boot and so eliminating the need for password sharing. The addition of Becrypt's Media Encryption, *mShare,* allows your users to encrypt data on external storage devices such as USBs – giving them flexibility and portability while still protecting your data. It enables users to convert any standard external USB connected storage device into a secure portable file store.

Easy implementation

Saving time and minimising the need for end-user involvement, Becrypt's *Enterprise Management (BEM)* enables quick and easy roll-out of the data protection products across thousands of devices. Active Directory integration enables easy importing of users, organisational units and security groups, while self-registration enables individuals to add themselves as Disk Protect users on a device.

Fully manage, control & audit

BEM's centralised management system gives you full visibility and control of user activity, enabling you to;

- easily create, apply and update policies to end-points, users or groups
- carry out fast risk assessment in the event of a lost or stolen device with detailed audits of events, warnings or errors that are recorded, reportable and searchable
- easily manage issues such as forgotten passwords

> Becrypt mShare enables users to convert any standard external USB connected storage device into a secure portable file store.

Achieving peace of mind with Becrypt

With Becrypt, you can safeguard the value of your organisation and reduce your risk of compliance failures by preventing your valuable IP and data being stolen from laptops, PCs and portable devices.

Our disk encryption, port control and secure media solutions enable you to keep your important data secure without compromising user productivity, while also giving you full management control and auditability.

Secure your data at rest

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

- Approved by UK government to secure classified data (up to TOP SECRET)
- Available in a number of approved variants to meet different levels of security
- Encryption applied transparently with no impact on user performance
- Generates its own keys eliminating the reliance on external agencies
- Unique pre-boot authentication for tablets (no external keyboard required)

Prevent data leakage

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

- Uses filter drivers to allow or deny access to devices
- Devices can be white-listed by make/model, individual unique device ID or by a signed device process
- Policy can be applied at device, user or group level
- Comprehensive centralised management system providing full event reporting, audit trails and analysis

Includes a comprehensive centralised management console providing full event reporting, audit trails and analysis.

Flexible sharing

Becrypt Disk Protect reduces risks by supporting multiple users on a single device, while Becrypt mShare allows users to encrypt data on external storage devices (such as USBs), giving them flexibility and portability while still protecting your data.

- Disk Protect provides multi-user support at pre-boot, eliminating the need for password sharing
- mShare enables users to convert any standard external USB connected storage device into a secure portable file store
- All files copied to and from the mShare secure vault can be fully audited

Easy implementation

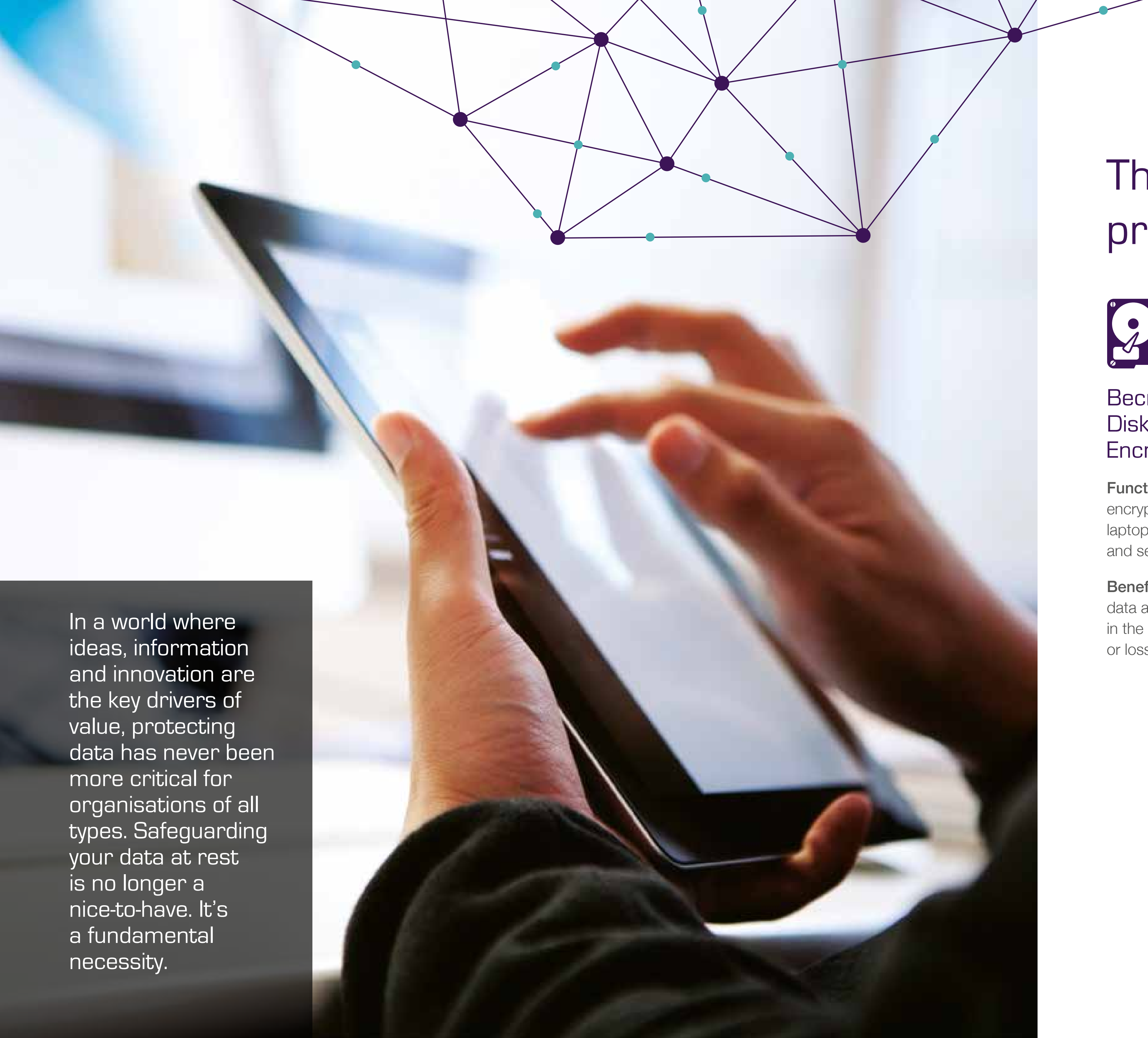
Becrypt Enterprise Management (BEM) enables quick and easy roll-out of Becrypt data protection products across thousands of devices, saving time and minimising the need for end-user involvement.

- Active Directory integration enables easy importing of users, organisational units and security groups
- Self-registration enables individuals to add themselves as Disk Protect users on a device

Fully manage, control & audit

The Becrypt Enterprise Management (BEM) centralised system 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, or easily address problems such as forgotten passwords.

- Detailed audits of events, warnings or errors are recorded, reportable and searchable in the management console
- Policies can be created, applied and updated to end-points, users or groups from the central console



In a world where ideas, information and innovation are the key drivers of value, protecting data has never been more critical for organisations of all types. Safeguarding your data at rest is no longer a nice-to-have. It's a fundamental necessity.

The Becrypt total protection suite

Becrypt Disk Encryption

Function: Full disk encryption for Windows laptops, PCs, tablets and servers

Benefits: Keeps your data at rest secure in the event of theft or loss of a device

Becrypt Port Control

Function: Peripheral device control to protect from unauthorised access

Benefits: Defends you against data leakage and malware ingress while providing full event reporting and audit trails

Becrypt Media Encryption

Function: Full encryption for data on external storage devices such as USBs

Benefits: Protects your data while supporting your users' productivity with full flexibility and portability

Becrypt Enterprise Management

Function: Centralised management system for full visibility and control of Becrypt estate

Benefits: Maximises the efficiency of your IT department and the management of your Becrypt estate

Becrypt's suite of data protection solutions safeguards the value of your business and reduces your risk of compliance failures.

About Becrypt

With over 15 years' experience of helping governments and businesses secure their valuable data, Becrypt has a long heritage of providing enterprise data protection solutions to the most security conscious organisations.

Innovating to provide the highest levels of product assurance, our data protection solutions allow diverse platforms to be adopted within the enterprise with confidence. Working with device manufacturers, we deliver comprehensive mobile security as a seamless user experience that supports productivity without compromising protection.

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

✉ dataprotection@becrypt.com

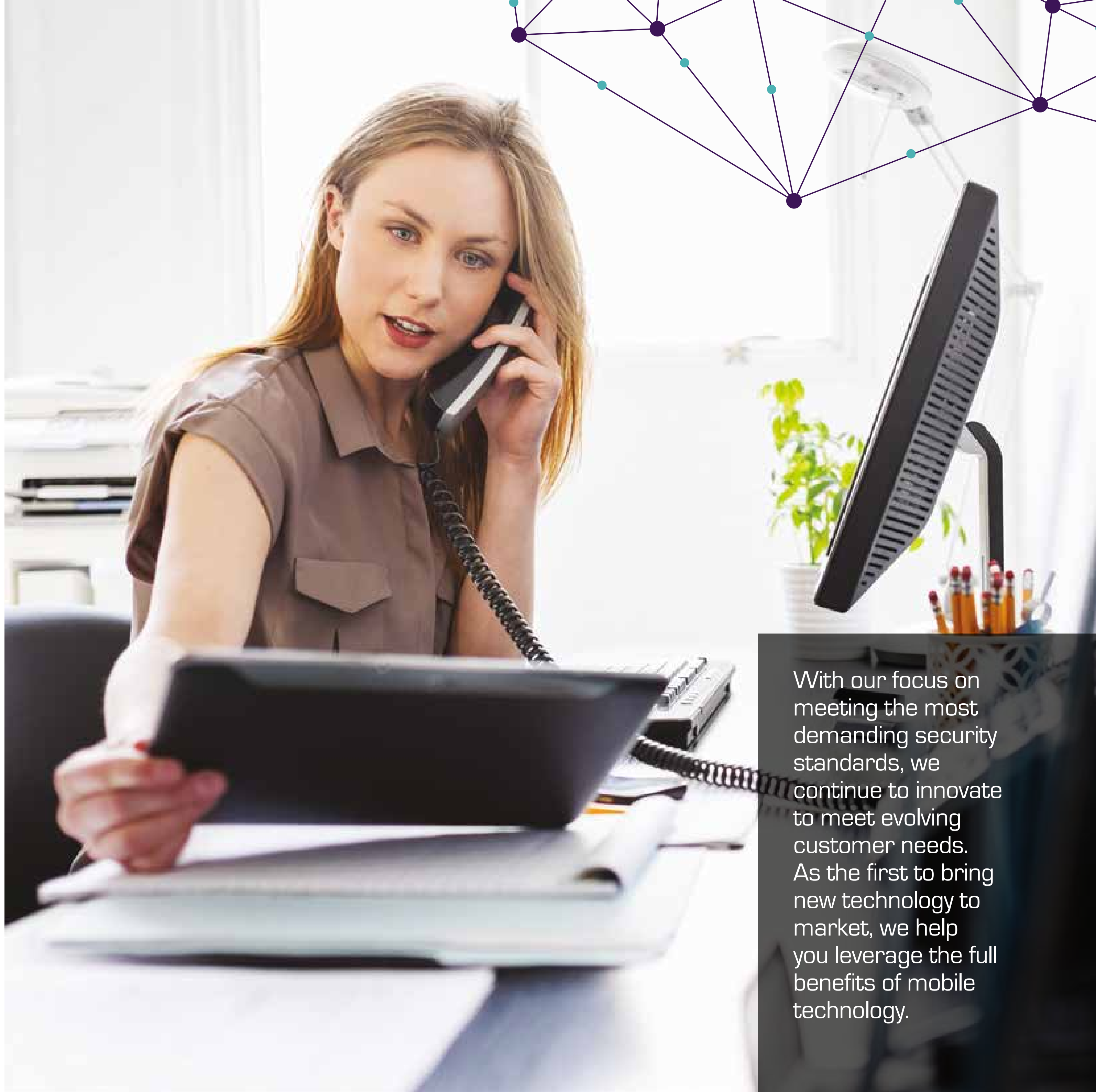
☎ 0845 838 2080

#becrypt.com/endpoint

References:

[1] The Cost of Cyber Crime, Detica/ Cabinet Office, 2011

[2] 2015 Cost of Data Breach Study, Ponemon Institute/ IBM



With our focus on meeting the most demanding security standards, we continue to innovate to meet evolving customer needs. As the first to bring new technology to market, we help you leverage the full benefits of mobile technology.

Becrypt Headquarters:

Becrypt Limited, Artillery House,
11-19 Artillery Row, London, SW1P 1RT
United Kingdom

☎ 0845 838 2080

✉ dataprotection@becrypt.com

twitter.com/becrypt

#becrypt.com