# Protecting IP in the Oil, Gas & Minerals sector

**Despite investments in cyber security, Oil, Gas and Minerals companies risk potentially crippling losses if they fail to adequately protect the data stored on laptops, PCs, portable devices and removable media.**

## The critical value of IP

**Whether it's exploration data, proprietary processes, or unique know-how, IP is at the heart of many Oil, Gas and Minerals companies' competitiveness and profitability.**

Driven by depletion of existing resources, geopolitical uncertainties, pressure to reduce carbon emissions and price volatility, companies across the sector need to access new resources and improve their ability to exploit existing ones. From developing new production techniques to creating more efficient fuels and processes, the Oil & Gas sector is one of the highest investors in R&D, investing £5.7b in the UK alone in 2009.

### IP theft can be catastrophic

Clearly, protecting the IP that results from this huge investment is critical, as evidenced by the fact that the sector accounted for 20% of all patent protection cases globally in 2013.[1]

The impact of IP and trade secrets falling into the hands of a competitor can be devastating. So protecting IP needs to be a priority for all players in the value chain, including producers and the wide range of service companies that the sector relies upon.

59% of companies within the Oil & Gas sector now have a dedicated IP team.[1]

## The growing impact of IP theft

**A UK government report identified the Oil & Gas and Mining sectors as amongst the most vulnerable to the loss of IP from cyber-crime.**

IP theft is the most expensive type of cyber-crime for UK businesses, costing £9.2bn a year in total, with industrial espionage not far behind at £7.6bn a year.[2]

In a 2012 speech, the Director General of MI5 talked of the CEO of a major oil company who had disclosed privately that the loss of oilfield exploration data – due to hacking – had cost the company hundreds of millions of dollars.[3] While losses from industrial espionage in the mining sector have been estimated at £1.6b per annum in the UK.

While the causes of data breaches are varied, the majority are a result of either malicious attack or human error. Recent research found that 47% of breaches involved a malicious or criminal attack and 25% involved a negligent employee or contractor.[4]

Unsecured devices are often a source of vulnerability. With the sector employing high numbers of mobile workers carrying around sensitive data on laptops, tablets and mobile devices, and needing to collaborate across extended teams, the Oil, Gas & Minerals sector is particularly exposed to data breaches from unsecured devices.

[1] *Intellectual Property 2015*: The Oil & Gas Perspective, Oil & Gas iQ [2] The Cost of Cyber Crime, Cabinet Office/ Detica, 2011

[3] https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html 2015 [4] Cost of Data Breach Study, Ponemon Institute/ IBM

## The risks that must be addressed

**Common data protection failures are leaving Oil, Gas & Minerals companies exposed to the loss of critically important IP;**

### Policy black holes

Companies lack policies governing how data is managed and protected on portable devices – often accompanied by limited employee awareness of what *they* can do to reduce risk.

### Failure to protect data at rest

Businesses fail to adequately protect data stored on desktops, laptops and portable media because they mistakenly assume that password protection or Endpoint Protection technologies adequately protect the data from a determined cyber criminal.

### Data leakage via portable devices

Businesses fail to prevent data being easily copied onto unencrypted portable media (such as USB drives and smartphones) – one of the most common sources of IP theft.

### Over-restrictive or complex security

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

### Limited visability & control

Businesses are often unclear about what data needs protecting, what devices are being used to store that data and how the data is being used and copied.

In a market where ideas, innovation and data are key drivers of value, protecting IP has never been more critical.

## Simple solutions for IP protection

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

### Secure your data at rest

Approved by the UK government to secure classified data (up to TOP SECRET), Becrypt's *Disk Protect* provides highly secure, full disk encryption for Windows laptops, PCs, tablets and servers – keeping data secure in the event of the theft or loss of a device.

### Prevent data leakage

With full event reporting and audit trails, Becrypt's Port Control, *Connect Protect*, defends companies from 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, unique device ID or a signed device process.

### Flexible sharing

Supporting multiple users on a single device, *Disk Protect* gives flexibility without risk by eliminating password sharing. Becrypt's Media Encryption, mShare, encrypts data on external storage devices such as USBs.

### Easy implementation

Saving time and minimising the need for end-user involvement, Becrypt's *Enterprise Management* (BEM) enables quick and easy roll-out of our data protection products across thousands of devices. Active Directory integration allows easy importing of users, organisational units and security groups.

### Fully manage, control & audit

*BEM's* centralised management system ensures full visibility and control of user activity, enabling the creation, application and updating of policies to end-points, users or groups. It also allows fast risk assessment in the event of a lost or stolen device.

To find out more about protecting device estates from IP theft, contact the experts.

✉ dataprotection@becrypt.com ☎ 0845 838 2080 #becrypt.com