Securing IP in the pharmaceutical sector

Despite investments in cyber security, pharmaceuticals 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

An increasing share of many businesses' value now comprises of their unique Intellectual Property (IP), insights, trade secrets and other confidential information stored digitally across their organisations.

With formulas for new drugs being the lifeblood of the sector, pharmaceuticals depend more than most on their ability to develop and protect their unique IP. Investment in Research and Development is higher in pharma than any other sector, with the industry investing around 30% of its sales in research. In the UK alone, this amounts to nearly £4bn year.

IP theft can be catastrophic

Given the importance for pharmaceuticals to generate a return on their R&D investments, the impact of their IP falling into the hands of a competitor can be catastrophic..

Not only for the individual company, but the broader economy can be negatively impacted, with Pharma as one of Europe's largest sources of skilled employment;

- Nearly 700,000 people are employed directly across Europe
- An estimated further 3 – 4 times that number are employed indirectly.

Recent research into the causes of data breaches found that 47% involved a malicious or criminal attack, with 25% involving a negligent employee or contractor.[1]

The growing impact of IP theft

A UK government report has estimated that IP theft is the most costly type of cyber-crime for UK businesses, costing £9.2bn a year in total.

The report also identified the pharmaceutical sector as the number 1 target for cyber-criminals intent on stealing IP, estimating the cost of IP theft in the UK pharmaceutical and biotech sectors at £1.8bn per annum – more than any other sector[2].

The potentially high profits, the significant investment in R&D and the large numbers of SMB businesses within the sector, all combine to make pharmaceuticals a particularly attractive target for criminals.

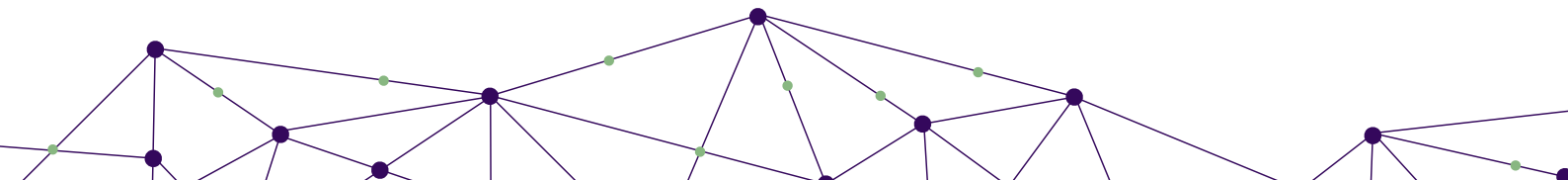
Pharma's increased exposure to IP loss

Pharma tends to employ high numbers of knowledge workers, who typically store and access data on a variety of laptops, tablets and mobile devices. It also relies heavily on collaborative working across extended teams, making the ability to share data crucial.

These two factors increase the sector's exposure to loss of IP. With the majority of data breaches resulting from either malicious attack or human error, pharmaceuticals are at risk from such threats as;

- A contractor copying sensitive files to a portable device
- An employee leaving a laptop on a train

[1] 2015 Cost of Data Breach Study, Ponemon Institute/ IBM [2] The Cost of Cyber Crime, UK Government/Detica, 2013



The risks that must be addressed

The most common data protection failures that leave pharmaceutical companies exposed to the loss of critically important IP can be summarised as;

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, formulas and innovation are the key drivers of value, protecting IP has never been more critical for pharmaceuticals.

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