WHAT IS THE PRICE OF LOYALTY?

2019 SURVEY

DEEP SECURE

TABLE OF CONTENTS

01 A growing problem

02 Personal use & profit

03 The price of loyalty

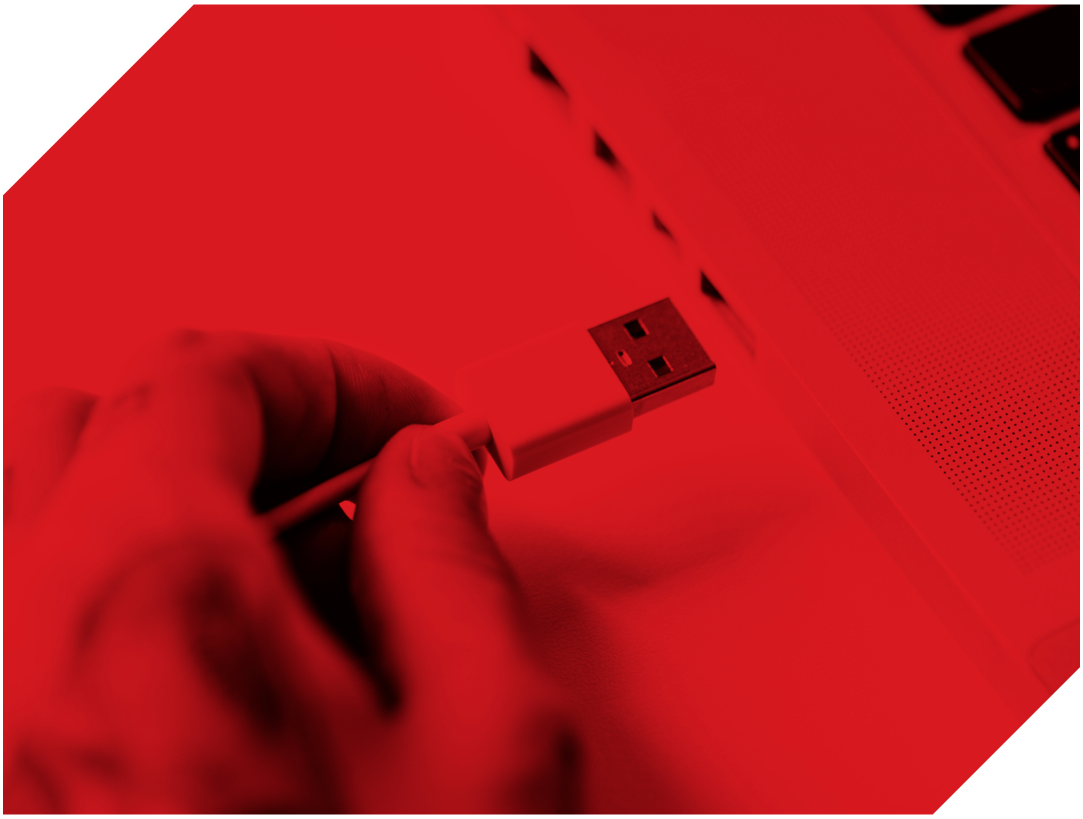
04 Stealing information

05 Mitigating the risk

06 Methodology

06 About Deep Secure

A GROWING PROBLEM



Our research findings aligned with the industry trend, with more than half of respondents (59%) reporting that at some point they have taken company information from a corporate network or devices.

19%
personal work completed

11%
client/customer information

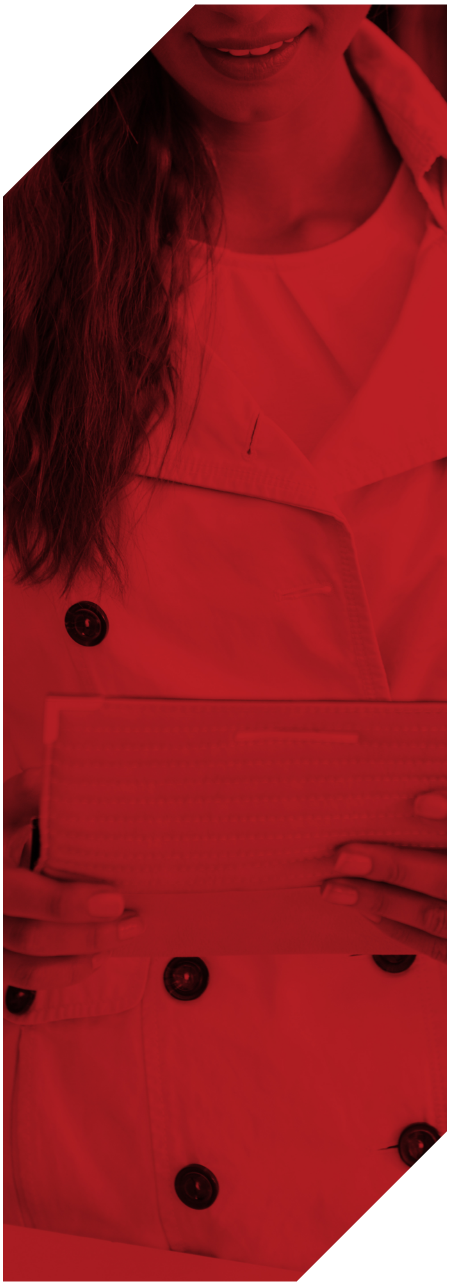
7%
company assets

Insider threats are a real and growing problem. The Verizon DBIR found that, insiders are complicit in 28% of data breaches in 2017 (up from 25% in 2016).

Customer information included contact details of clients (11%), confidential market information about the company or customers' companies (7%) and details of the sales pipeline (6%).

Company Assets included passwords to subscription services (i.e. external databases, content subscriptions, company benefits) (9%), sensitive information relating to colleagues (7%) , company or customer credit card details (6%) and intellectual property (i.e. product specifications, product code, patents) (6%)

PERSONAL USE & PROFIT



A key motivator was the potential value that the information would have to the individuals' career success, with respondents deciding to take information because they thought it would be of value in a new role (12%), they wanted to keep a record of their work (12%) or they thought it would benefit their career (10%). However, the value to third-party organizations (and potential financial compensation) was also a key driver:

47%
given data to a 3rd party

8.5%
paid to do so by a 3rd party

8.5% of respondents took company information because they were paid to do so by a third party outside their organization.

Of these, 19% of these respondents were grads/interns – pointing to potential targeting of these younger, newer to the industry employees.

7% of respondents took company information because they knew it would be of value to a third-party organization; this rose to 12% amongst individuals that were with the company for 3-4 years

In fact, of those who took information off the corporate network, 47% have given it to a third-party – (this rises to 62% amongst male respondents).

THE PRICE OF LOYALTY

45%

of all office employees admitted that they would share corporate information with a third party, if paid

25% information for £1000

15% sales pipeline details for £1000

15% market information for £1000

14% intellectual property for £1000

11% customer information for £1000

10% customer contact details for £250

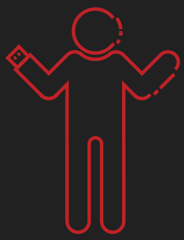
15% information about colleagues for £1000

8%

of respondents admit to using cyber tools to exfiltrate information

11%

of respondents admitted to having emailed company information to a third party outside of their organization



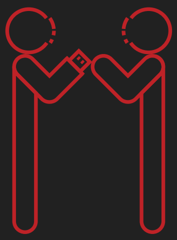
59%

of respondents report that at some point they have taken company information from a corporate network or devices

19% personal work completed

11% client/customer information

7% company assets



47%

of respondents admit to supplying company data to a third party

8.5% paid to do so by a 3rd party

19% of these were grads/interns

STEALING INFORMATION

Individuals are using digital techniques to exfiltrate data to third-parties. Some individuals are using traditional techniques to take information, including printing (11%), hand-writing (9%) and taking a photo (8%).

Others are using digital techniques to exfiltrate data to third-parties. 11% of respondents admitted to having emailed company information to a third-party outside of their organization, saved company information to a personal cloud storage device of a third-party outside of their organization and saved company information on an external storage device that they have then given to a third-party outside of their organization.

A significant number (8%) also reported using cyber tools to hide and exfiltrate company information (such as, steganography or encryption).

The use of cyber tools to steal company information has been democratised by the availability of toolkits on the web. Steganography toolkits that enable cybercriminals to encode information into an image are available FREE and guarantee an undetectable route out of the network.

A significant number (8%) also reported using cyber tools to hide and exfiltrate company information (such as, steganography or encryption).

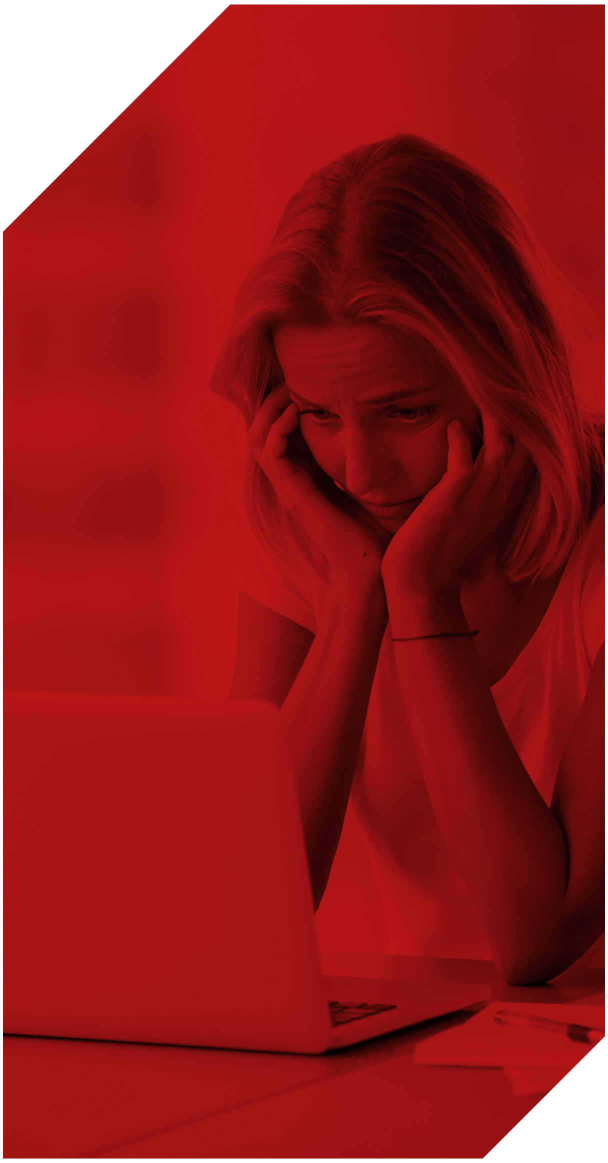
MITIGATING THE RISK

With nearly half (45%) of all office employees willing to be paid to share corporate information with a third party, the risk of the insider threat is significant.

The use of digital tactics to exfiltrate this information is high, so it's critical that businesses invest in a security posture that will help them both detect and prevent company information from leaving the network.

Data breaches have fueled a steep increase in the adoption of Data Loss Prevention technologies (the market is predicted to record a CAGR of 23.59% between 2018-2023)

A mixture of detection and prevention technologies are needed to truly mitigate the risk of malicious insiders using digital tactics to exfiltrate information. Prevention technologies, like Content Threat Removal, are capable of removing 100% of information concealed in images using steganography, no matter whether it's emailed or uploaded to cloud storage. This completely frustrates cybercriminals' efforts when using more sophisticated methods of concealment.



Some cyber tactics such as steganography are completely undetectable and render an organization defenceless.

THE METHODOLOGY

The research was conducted by Censuswide on behalf of Deep Secure.

The research surveyed 1,500 UK office workers and was carried out in April 2019. Censuswide abide by and employ members of the Market Research society which is based on the ESOMAR principles.

ABOUT DEEP SECURE

Deep Secure solves the biggest problem of the information age. By moving cybersecurity beyond detection and eliminating any threat in the attack vector of choice - digital content - we ensure your world is completely digitally pure.

Our technique – content threat removal - eliminates the major inbound attack vector, and by preventing any covert exfiltration of data using image steganography, helps mitigate the insider threat.

www.deep-secure.com
+44 (0) 203 950 5116
info@deep-secure.com