Pierre Audoin Consultants

Gold study sponsor:

CGI

Experience the commitment®

Is cyber security now too hard for enterprises?

Cyber security trends in the UK

Executive Summary

Core statements

I. Cyber security is now too hard for enterprises

- The threat is increasing
- Board level concern is increasing
- Yet budget are static

II. Enterprises would prefer to:

- Hire more staff and retrain existing internal staff
- Use external resources on a project basis only
- And yet, 70% of enterprises outsource at least some of their security

III. Enterprises are more willing to consider outsourced security

- There's an inherent reluctance to outsource
- But it fixes some immediate issues, such as skills and compliance

IV. BDMs are:

- Less likely to support Cloud-based security
- More concerned at the prospect of outsourcing Governance and Security Management

Introduction

Enterprises today are faced with three key challenges:

- Implementing new SMAC technologies to support the business, as part of their digital transformation programs, but while keeping it secure;
- Responding to the increasing and changing threat landscape of targeted attacks;
- Achieving and retaining compliance with an increasing number of rules and regulations.

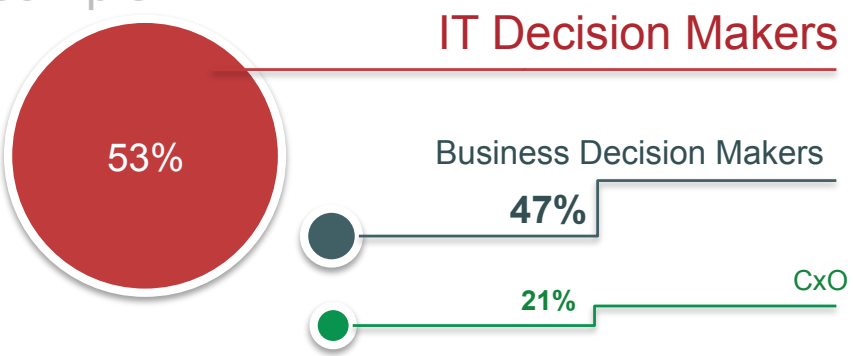
Our hypothesis for this study was that enterprises are struggling to cope with the increase in workload, and are increasingly offloading (some of) their security provision to outsourcing providers as Managed Security Services (MSS).

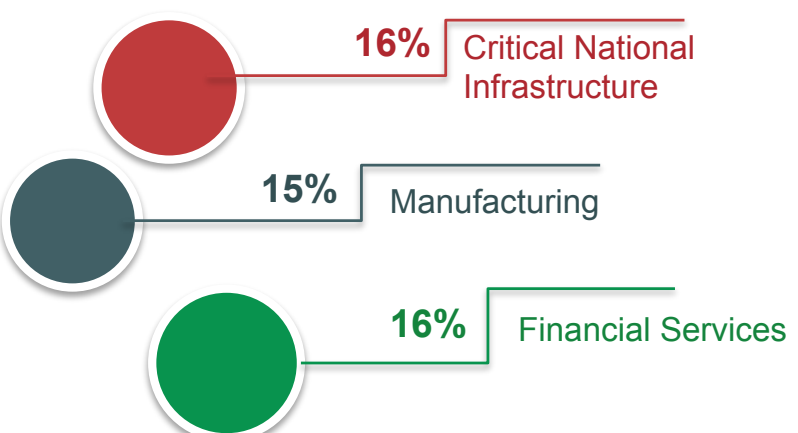
We surveyed **230** decision makers in **large companies** in the UK, to understand their **motivations** and **drivers** with regard to cyber security provision.

This study deals with the following questions:

- What do companies understand about the growing cyber threat landscape?
- How are companies meeting their resource challenges in cyber security?
- How are they using external providers to meet resource challenges?
- What are the drivers and inhibitors for using external cyber security providers?
- What alternative approaches to external cyber security provision being considered?
- Which services do companies expect from a cyber security provider?
- What are the capabilities and attributes of a credible cyber security provider?

Sample





Executive summary I

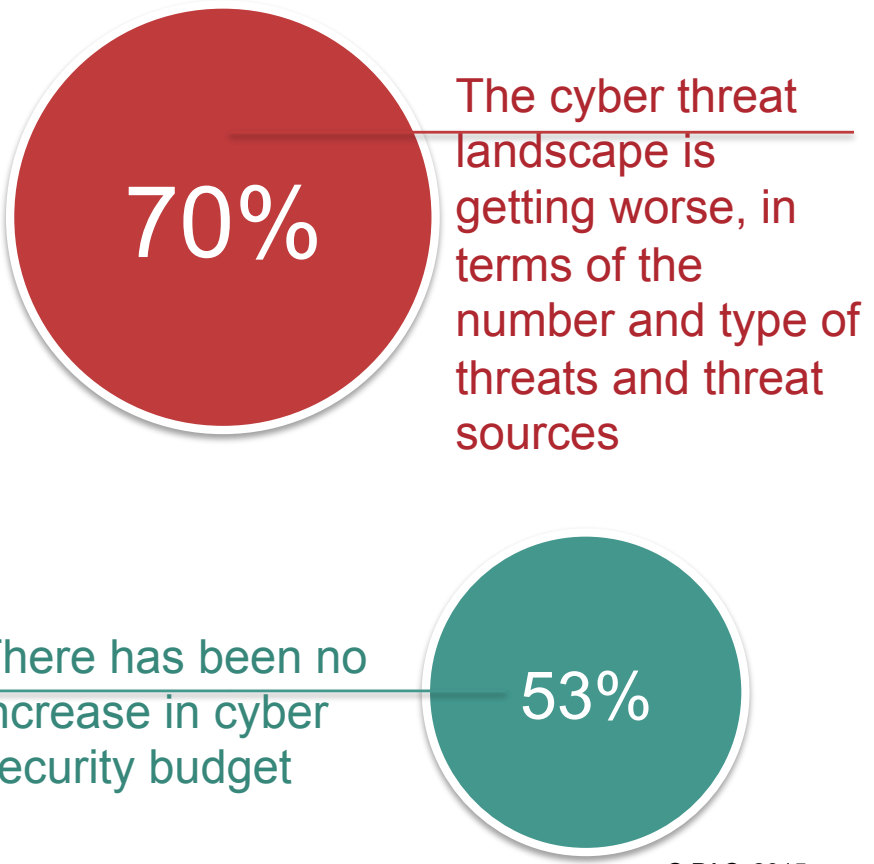
Cyber security is increasing in importance as the threat landscape worsens. But budgets are not rising in line.

The overall picture of cyber security provision in large organisations is that the threat landscape is getting worse, board attention and focus is increasing, but there is a funding shortfall in many organisations.

An overwhelming majority of enterprises see the cyber threat getting worse. This is not a surprise, but it does enable us to quantify the scale and extent of enterprises' perception regarding the cyber landscape. As our figure shows, 70% of respondents believe that the situation is getting worse. We believe that this is caused in part by respondents' own experience within their firms and partly by the greater exposure to cyber security breaches in the national and trade press.

Firms' preferred approach to this is to increase the amount of security automation, followed by training of internal staff. There is a clear reluctance (or inability) to hire external staff and a tangible antipathy towards outsourcing.

However, organisational reluctance to outsourcing does not necessarily translate into practice, with more organisations admitting to using external resources than would prefer to do so.



Executive summary II

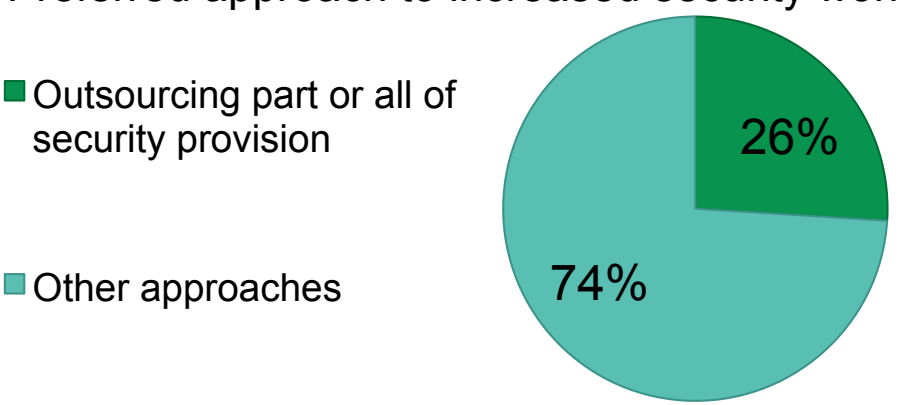
Firms are suspicious of outsourcing as they dislike loss of visibility & control. But they do use 3rd parties selectively.

Our research shows that organisations have an innate reluctance to outsource, and this even extends to admitting that outsourcing goes on. But by drilling down into actual practice we discover that there is a high degree of use of external provision, including outsourcing. The prevalent method of using external provision is by buying in expertise on a project-by-project basis.

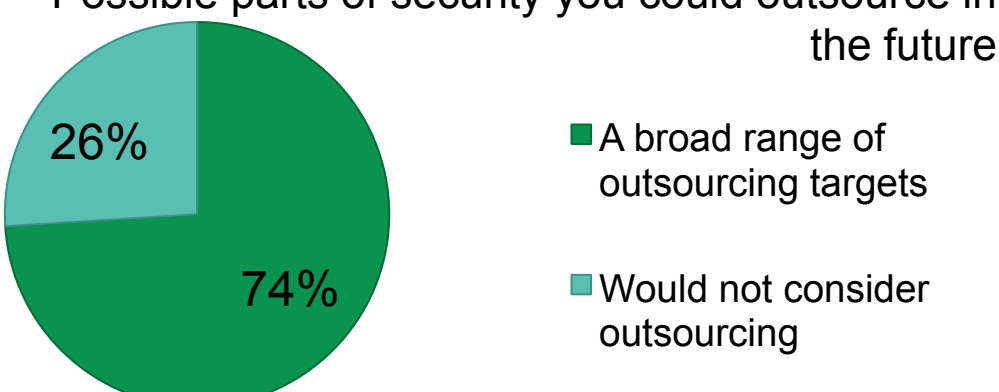
The overall motivation for using external provision, including outsourcing, is a combination of a lack of funds and expertise, echoing our earlier findings which identified a funding gap. The double whammy of insufficient funds and a scarcity of skills appears to be driving organisations towards external resources, including outsourcing, even though there is a clear reluctance to do this.

This represents an entirely pragmatic approach, according to PAC. Organisations dislike losing visibility and control of processes, especially those that have a high risk profile such as cyber security. But the pressures on budgets and expertise are such that companies have little option but to use external providers.

Preferred approach to increased security workload



Possible parts of security you could outsource in the future



Executive summary III

The importance of cyber security to enterprises drives a detailed examination of suppliers' credentials & experience

Cyber security is critical to organisations. And although they currently use external providers, they are clear that when they do such providers must come with robust credentials.

Of those organisations that currently outsource or use external support for security provision, a majority target risk management (combined 75%) and audit & penetration tests (76%). 68% of firms that use some external provision do so in the management of security solutions, a oft-reported headache for CISOs.

Enterprises are clear when asked to report the key attributes of a potential cyber security services provider. They value evidence, in the form of a strong track record and security expertise and skills. Industry knowledge is also important, as is a trusted and well-known brand.

Cyber security is too important to businesses for them to adopt additional risks with their suppliers. It is important then for suppliers to communicate their track records, and strong industry knowledge is also extremely useful.

Gold Sponsor – Profile

Experience the commitment®

Company profile: CGI

About CGI

Founded in 1976, CGI Group Inc. is the fifth largest independent information technology and business process services firm in the world. Approximately 68,000 professionals serve thousands of global clients from offices and delivery centres across the Americas, Europe and Asia Pacific, leveraging a comprehensive portfolio of services including high-end business and IT consulting, systems integration, application development and maintenance, infrastructure management as well as a wide range of proprietary solutions.

Cyber security is part of everything we do and for over 35 years, our government and commercial clients have regarded us as their cyber security expert of choice. Cyber-attacks are becoming more sophisticated and can cause financial loss, reputational damage, theft of business critical information or regulatory fines. We have helped our clients build cyber security into their corporate strategy so they can conduct business in a digital age with confidence, openly and globally, driving competitive advantage, efficiency and growth.

We have invested heavily in establishing our credentials by working closely with international security associations and standards bodies and we have built a CGI UK Cyber Centre. Many of our experts are recognised as leaders in the industry, contributing to the development of standards such as ISO/IEC 27002. They are part of CGI's 1,400 strong global cyber security team and they bring this shared expertise, research, knowledge and solutions to our client projects. We have received many accolades for our work and have supported our clients to achieve a 100% success rate when undertaking ISO 27001 accreditation. We provide the deep sector and cyber expertise needed to keep ahead of the attackers and protect an organisation.

Experience the commitment®

Company profile: CGI

About CGI (continued)

Our cyber security technical experts have helped our clients design, develop and deliver some of the world's most complex, secure technology projects and services. We have also been trusted by hundreds of government and commercial clients to help them operate securely. CGI has ten Security Operating Centres (including one in the UK) providing Protective Monitoring and Advanced Threat Investigation services - handling more than 74 million cyber events every day. For 27 years we have operated a commercial evaluation facility and regularly test the products and services of over 25 global technology suppliers.

We offer the full range of cyber security services needed by clients to:

- assess their cyber security risk including risk and vulnerability assessments, governance, awareness, supply chain review and compliance
- protect their business including new technologies such as mobile and cloud, secure systems engineering, identity and access management, testing, certification
- operate with confidence including protective monitoring, advanced threat investigation, penetration testing and incident response

Our deep and broad experience helps our clients be agile, adopt new technologies and ways of working, develop a global supply chain and open new channels to their customers – whilst remaining confident that they are secure. We believe that if you want your organisation to be considered as a top employer, one that customers love, that suppliers want to be working with and which takes advantage of the latest technologies - cyber security should be part of that vision.

Find our more at cgi-group.co.uk/cybersecurity or contact us on cybersecurity@cgi.com

Disclaimer, usage rights, independence and data protection

This study was compiled in multi-client mode under the sponsorship of CGI, cybX and Fujitsu/Symantec.

For further information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in January 2015 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

This study was produced solely by Pierre Audoin Consultants (PAC). The sponsors had no influence over the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies, and no individual survey data was passed to the sponsors or other third parties. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and the sponsors of this study.

About us

From strategy to execution, PAC delivers focused and objective responses to the growth challenges of Information and Communication Technology (ICT) players.

PAC helps ICT vendors to optimize their strategies by providing quantitative and qualitative market analysis as well as operational and strategic consulting. We advise CIOs and financial investors in evaluating ICT vendors and solutions and support their investment decisions. Public institutions and organizations also rely on our key analyses to develop and shape their ICT policies.

Founded in 1976 and headquartered in Paris, France, PAC is part of the CXP Group, the leading European research & advisory firm in the field of software and IT services.

For more information, please visit: www.pac-online.com

PAC's latest news: www.pac-online.com/blog

Duncan Brown
Research Director,
Cyber Security

+44 (0) 20 7553 3966

d.brown@pac-online.com