ADEPT4

IT AS A SERVICE

Now We're Talking:
Buy-in or build-out? IT security for the mid-market

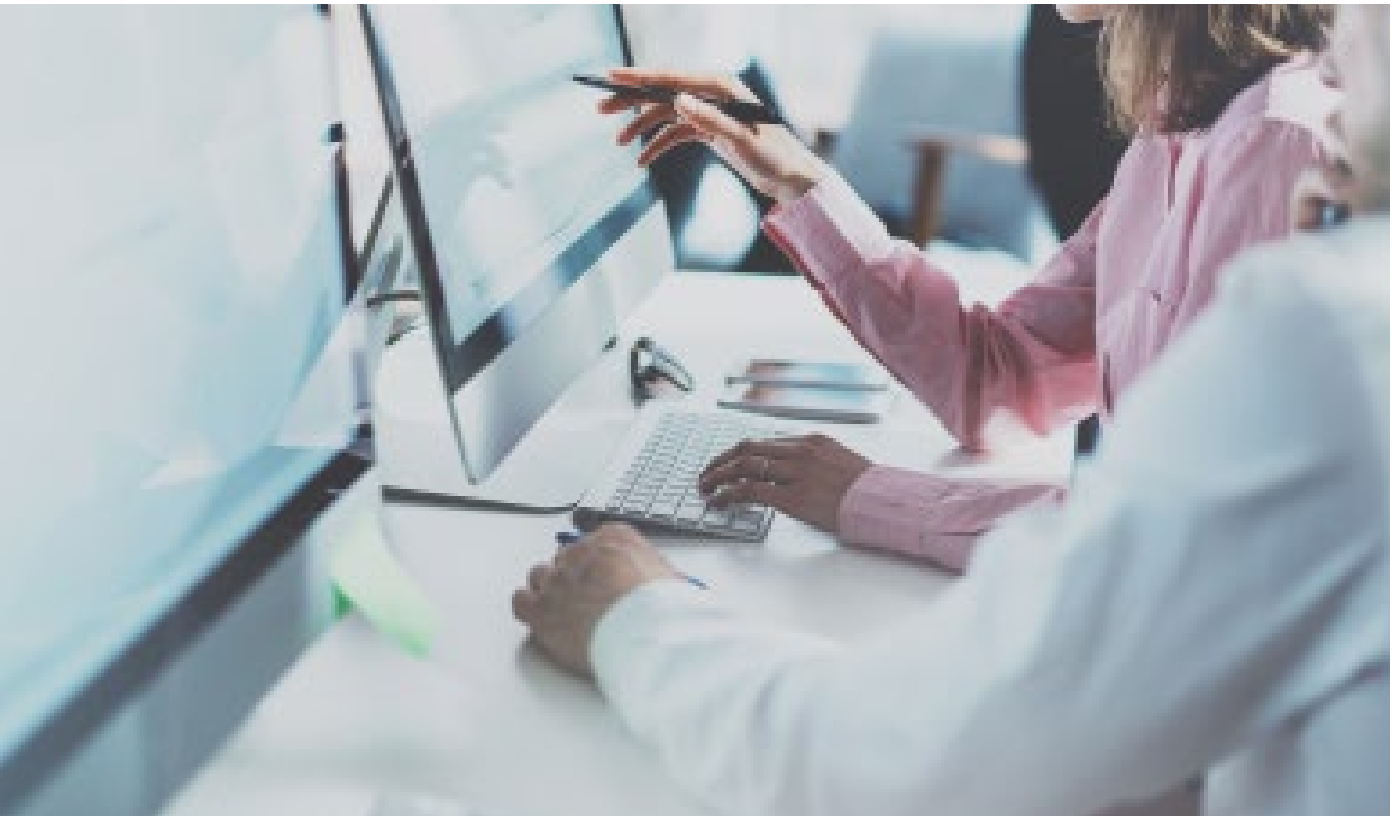
www.adept4.co.uk

Introduction

The distinction between ‘buy-in’ and ‘build-out’ is one of the starkest ways of modelling organisational Security Operations Centres (SOCs). From tiny start-ups to multi-national enterprises, the choice is the same: ‘buy-in’ a security solution or package of solutions from a third party, or ‘build-out’ an entirely in-house security facility, managing everything from technology to staff internally.

It’s an age-old dilemma. Each of the two carries with it its own advantages and disadvantages, benefits and challenges.

In this insight guide we’ll work through them.



From nice-to-have to business essential: why security matters for every business

There are at least three core reasons as to why IT security has moved from vague concern for businesses in certain sectors or with a particularly complex IT infrastructure, to a centralised issue for all organisations.

First, the cyber threat landscape has evolved – and continues to evolve – dramatically and dynamically. The scope and scale of tools and techniques deployed by everyone from digital vandals to highly sophisticated cybercriminals are ever-growing, and organisations of all sizes and across all sectors are at risk. Organisations may simply be ‘drive by’ victims of indiscriminate campaigns, where infected links or attachments are sent out en masse to thousands of email addresses.

Or they may be the targets of highly planned attacks, where criminals seek to extract specific data from within their systems over weeks or months. All it takes is a single employee opening the wrong attachment or clicking on the wrong hyperlink and ransomware can freeze critical business applications, steal valuable data or bring operations grinding to a halt. And because human error can never be totally mitigated, nor too can the risk of such cyber threats infiltrating any organisation.

‘All it takes is a single employee opening the wrong attachment… and ransomware… steal valuable data or bring operations grinding to a halt.’

Second, even the smallest organisations are operating increasingly complex IT infrastructures, with large numbers of applications and endpoint devices to protect, and new users and devices continually being added. As the Internet of Things (IoT) continues to proliferate, and employees become more likely to work across a number of different mobile devices, so businesses have a larger number of endpoints to keep track of and protect with enterprise-grade security. For fast-growth organisations, those with multiple sites and those that employ a large number of temporary or freelance staff, the challenges are even greater.

Third, the wider regulatory and legal landscapes governing organisations' IT security are increasingly demanding. The EU General Data Protection Regulation (GDPR), due to come into force in May 2018, is one of the best-recognised, demanding a range of measures designed to protect individuals' personal data and ensure that cyber incidents are rapidly and comprehensively reported. However, there is a massive range of other regulatory frameworks, depending on the jurisdictions in which an organisation operates and the sectors and activities it participates in. Typically, the requirements of such regulations are twofold: they require specific security standards and protocols to be implemented; and they require accurate audit trails demonstrating those standards and protocols. Both requirements demand an organised and often partly automated security operation.

With all these demands in mind, SOCs are no longer the realm of international businesses or those operating in particularly restrictive sectors. Any organisation with any IT function at all needs to take its IT security seriously, and that means running a SOC.

But which kind?

The two models: comparisons and considerations

Clearly, different organisations have different security needs depending on the precise array of applications and data they are seeking to protect.

Nevertheless, all SOCs, whether build-out or buy-in, must deliver the same basic functions: they need to continually monitor the organisation's IT systems for any signs of malicious or accidental interference; when such incidents occur they need to rapidly isolate, assess and if necessary repair them; and they need to keep a record of all activity for the purposes of regulatory audits and overall IT strategy. All this is achieved through bespoke packages of monitoring, assessment and repair tools and technologies – and, of course, highly skilled IT security personnel to operate them.

A build-out SOC may be created on an existing site or sites belonging to the organisation in question, or it may be created at brand-new premises, but regardless it is fully owned and operated by the business. By contrast, a buy-in SOC exists remotely, managed by a third-party provider and with the majority of monitoring and even maintenance carried out remotely too. Essentially, it's a cloud-based model, with the SOC delivered as-a-service.

This underlines one of the major differences between build-out and buy-in SOCs – their payment models. Build-out SOCs require a hefty upfront investment in technology and potentially new premises and staff. Buy-in SOCs work on an OpEx basis, where services are paid for month-by-month, according to use and the scale of the organisation. Build-out SOCs do have ongoing expenses as well however, since employees are required to staff them.

Indeed, staffing is another major difference between the two models. Build-out SOCs are manned entirely by members of the organisation, essentially meaning that it is necessary to hire, train and support a SOC team or department. Buy-in SOCs can be staffed entirely at the third-party provider side, with as little as a single manager at the client side. This manager can be an IT professional, or from an entirely different specialism. With a buy-in SOC, there may be no need to hire any internal IT security staff at all.

Decisions, decisions

For many organisations, the allure of a build-out SOC is great.

It seems to offer the greatest level of visibility and control, with everything from the software and hardware deployed to the schedules for routine scans and checks absolutely down to the discretion of the organisation. However, some crucial questions should be asked before taking the plunge.

- Do you have enough security staff to create a 24x7 in-house SOC?
- Do those staff have an appropriate spread of knowledge and skills between them to look after all aspects of your infrastructure?
- Who will design the SOC, both in terms of its physical site and the technologies deployed?
- Who will document all the policies and processes within your SOC?
- Who will ensure that your SOC stays on top of the latest cyber threats?
- Who will ensure that your SOC stays on top of the latest legal and regulatory requirements?
- Who will interpret the threat intelligence data your SOC generates?
- How will you prove that your SOC is offering real value to senior leaders?

As you can see, every one of these questions relates in some way to the human resource you have available to create and manage your SOC.

Superior skills

The IT skills gap is hardly a new concept, but it is particularly stark in the security sector..

Because organisational IT security encompasses such a broad range of functions, and because the wider threat and regulatory landscape is so dynamic, even small organisations typically require a number of different experts to manage a comprehensive SOC function. And that quickly becomes unmanageable.

This is the great advantage of buy-in SOCs for mid-market organisations. They are quickest, most cost-effective and most-efficient of getting 24x7 access to all of the diverse skills and expertise required to keep an organisation's IT infrastructure protected – without paying hefty recruitment and salary costs every month. What's more, because those experts are working across a number of different client organisations, threat intelligence from other businesses is used to develop a far richer picture of the threats facing your business.

Mid-market organisations: a clear choice

Build-out SOCs, fully owned and operated by the organisation in question, certainly have their place.

For the largest businesses, with the ability to run an extensive and multi-skilled IT security team in-house, they offer supreme visibility, control and flexibility, and may end up being more cost-effective in the long run.

However, for mid-market and smaller organisations, they are an unnecessarily costly and complex option. They are unlikely to be able to innovate and develop at the same pace as either the attacks they are defending against, or the technological and regulatory landscapes they need to meet – at least without prohibitive recruitment and technology deployment costs. What's more, they are completely unnecessary.

> ‘For mid-market… they are an unnecessarily costly and complex option.’

Cloud computing has enabled smaller organisations to benefit from a shift to OpEx models and borrow resource from much larger organisations in a wide range of applications – security is no different. A buy-in SOC, delivered via the cloud from a specialist managed services provider is the ideal means of staying competitive and protected in a dynamic world.

About Adept4

Adept4 is a managed services provider.
It enables organisations to become operationally and culturally agile through smart, adaptive cloud based technology strategies that respond effectively to everyday challenges.

Adept4 is a northern based power house delivering hybrid IT, Microsoft cloud and managed services that enable organisations to securely transition, flex and integrate between on premise and cloud-based services.

Adept4 is a market–leader in developing solutions that enable mid-market sized organisations to make faster decisions, improve operational efficiency and gain competitive advantage.

If you're ready to start your journey to the Cloud then book in for a free free Cloud Readiness Assessment with one of our consultants.

Book Assessment

ADEPT4

IT AS A SERVICE

Head Office

Adept4 Managed IT Ltd
7750 Daresbury Business Park
Daresbury Office Village
Warrington, Cheshire
WA4 4BS

t. 0808 252 4444
e. info@adept4.co.uk

Aberdeen

3 Merkland Road East
Aberdeen
AB24 5PS

t. 0808 252 4444
e. info@adept4.co.uk

Leeds

Adept4 Managed IT Ltd
Victoria Spring Business Park
Liversedge
West Yorkshire
WF15 6BE

t. 0808 252 4444
e. info@adept4.co.uk

www.adept4.co.uk