DigitalXRAID

Why outsourcing security operations is a SMART investment:

Hackers don’t sleep....why should your SOC?

Why outsourcing security operations is a SMART investment: Hackers don't sleep....why should your SOC?

The workplace has changed a great deal over the past year. But one thing that has not is the omnipresent risk of a serious security breach. In fact, the risks have multiplied recently thanks to mass remote working, stretched IT resources and resourceful attackers. The truth is that cybercriminals have always worked from home, so it should be no surprise that they were quickest to adapt to the new reality of life during a pandemic. They are also highly distributed, flexible workers who will target your organisation 24-hours a day.

What does this all mean?

It means the 24/7/365 Security Operations Centre (SOC) has never been a more critical part of your cybersecurity posture. But few enterprises have the resources to support the high upfront and ongoing staffing and technical costs. The case for outsourcing has never been stronger.

A year of change

The threat landscape is continually evolving. And its latest iteration over the past 12 months has seen a rebranding of phishing campaigns with COVID-19 lures, and a targeting of remote workers and infrastructure. **Google claimed to be blocking as many as 18 million malware and phishing emails related to the pandemic daily by April 2020**. Phishing has always been a preferred tactic for deploying malware and stealing data and log-ins, but the advent of distracted home workers on insecure personal devices and networks has played right into the hands of cybercriminals.

It doesn't help that many of these employees have been straying dangerously far from corporate security policy. Remote workers are now their own compliance officers, and that's not an optimal situation for CISOs. **A recent survey found that ensuring employees can work securely is the most challenging aspect of remote working for businesses**. If remote working is to become commonplace after the pandemic recedes, businesses need to deploy the right combination of technology, process and training to mitigate risk here.

The bad guys have also been excelling at finding weaknesses in the tools and networks organisations are using to support this newly distributed workforce. **Exposed RDP endpoints and vulnerable gateway appliances and VPNs have been easily hijacked in sophisticated ransomware attacks**. While digital transformation has accelerated by years in the space of just months to support new business processes, it has also exposed organisations to more threats targeting web applications, cloud infrastructure and more.

What were the more challenging aspects for the company in terms of remote/home working?

1. Ensuring employees could work securely and remotely and in compliance with industry requirements
2. Providing equipment (mobile devices, laptops, headsets, etc) for employees
3. Providing adequate technical support
4. Providing access to the apps, data, and services employees need

Source: Omdia Future of Work Survey 2020

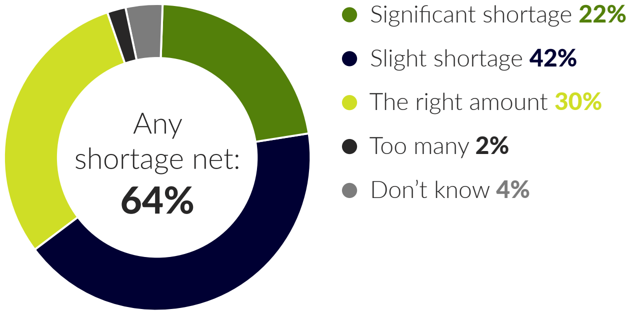
Why SOC matters

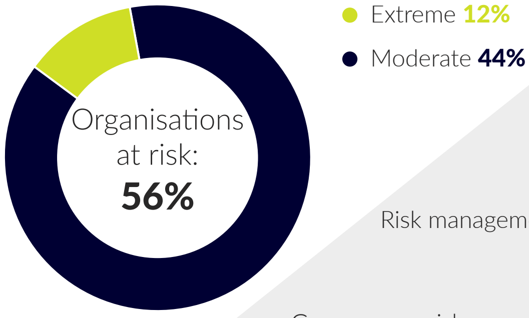
A SOC should be an essential part of a company's cybersecurity strategy as it can provide round the clock threat detection and response. Given the current threat landscape, and the ever-expanding corporate attack surface, it has never been more important for businesses to invest in their cybersecurity posture.

Yet as strategically important as the SOC is, there are major challenges facing CISOs and their peers. Skills shortages remain endemic in cybersecurity. Although it fell slightly last year, **the current global shortfall is estimated at over three million globally**. In-house security analysts may be a valuable commodity, but they are being wasted in many organisations because of inadequate technology. Too many competing security alerts from too many tools threaten to overwhelm teams, leaving them unable to prioritise or focus on higher value tasks. In fact, **a study from the Ponemon Institute found that global organisations use on average 45 security tools**. The result is too many false positives, causing staff to chase dead-ends, and too many false negatives, leading to critical alerts being ignored.

The outcome is that it **takes an estimated 280 days to identify and contain a breach today**. The longer attackers are allowed to dwell inside victim networks, the more financial and reputational damage will usually result.

Cybersecurity professionals report staff shortages at their organisations, and security risks that spring directly from those shortages.





Top cybersecurity skills needed

Cloud computing security	**40%**
Risk management, analysis and management	**28%**
Security analysis	**28%**
Governance, risk management and compliance (GRC)	**26%**
Threat intelligence analysis	**26%**
Application security	**25%**
Security engineering	**24%**
Security administration	**23%**
Data management protection	**22%**
Penetration testing	**22%**

Cybersecurity professionals plan to develop their skills across multiple areas over the next two years, with **40%** specifically naming cloud computing security as an area of focus.

Source: (ISC)² Cybersecurity Workforce Study

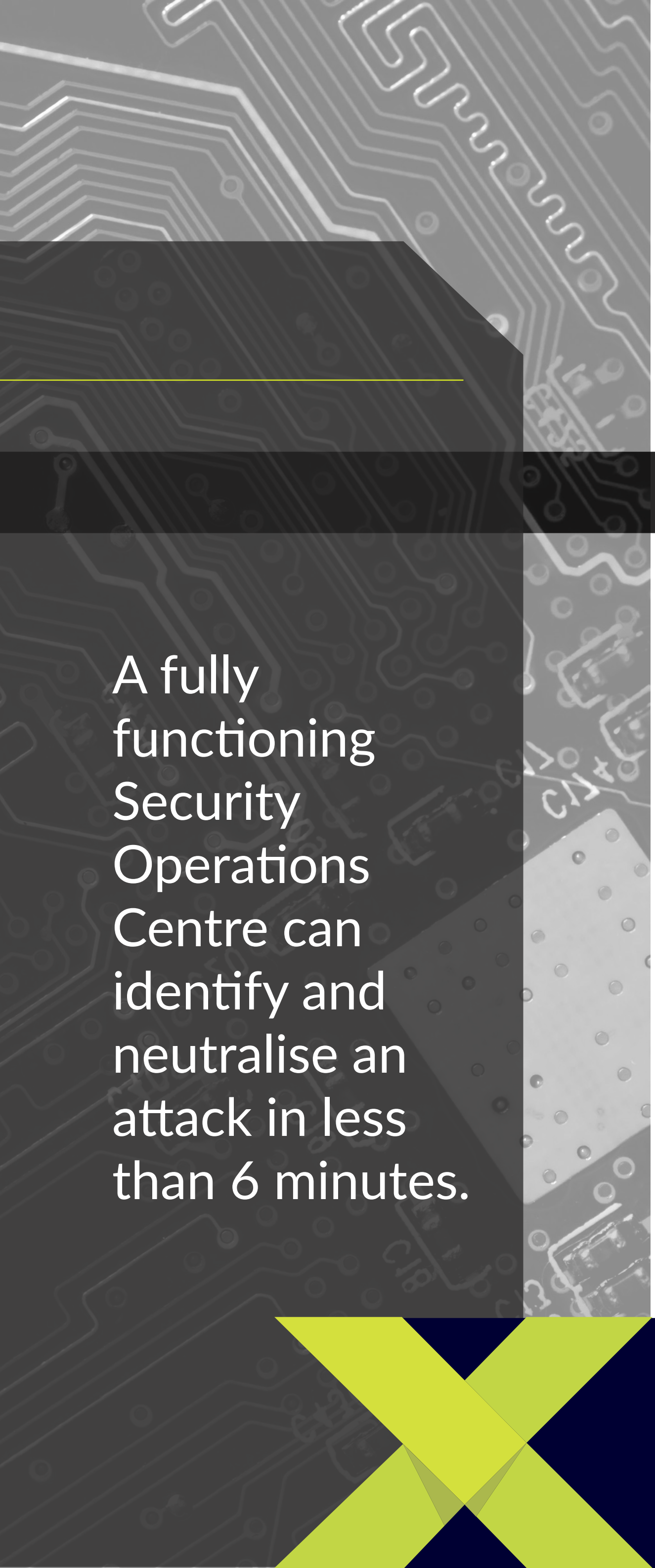
Making budget count

Although **more than half of UK business and tech execs said they were planning to increase cybersecurity budgets** this year, where the money is spent is almost as important as the fact that more funds are being allocated. Unfortunately, just 38% are very confident their cyber budget is allocated to the most significant cyber risks, versus 44% globally. And just 36% are very confident they're getting the best return on their cyber spend compared to 42% globally.

In times of global financial crisis, it's doubly important that budgets are allocated effectively to maximise ROI. For those that still view security as a cost centre, it's worth remembering that **the average cost of a data breach today stands at $3.9 million (£2.8m)**. But in some cases, the impact of a serious outage can hit 10 or 20 times that. The latest big-name to suffer was **healthcare giant UHS, which reported $67 million (£48m) in losses due a ransomware incident** which forced patients to competitors and incurred major IT overtime costs.

only **36%** of UK organisations are very confident they are getting the best return on their cyber spend versus **42%** globally.

Source: PWC Cyber security strategy 2021



Time to outsource

In this context, SOC spending should be non-negotiable today. An effective security operations team will detect, respond to and prevent threats to minimise the financial and reputational impact of cyber risk. But before deciding what kind of model to run, IT and security leaders should think carefully about their existing resources.

Can your internal security team operate 24/7/365?

After all, hackers don't sleep, so neither should your defences. Do you have the budget to staff a SOC, and ensure they have all the automated, AI-powered tooling they need to prioritise and investigate alerts efficiently? It can take half a million pounds even for relatively basic capabilities, which won't give you 24-hours-a-day visibility.

This is where outsourcing can provide the best of both worlds. With a trusted provider your outsourced SOC becomes an extension of your own security team, working seamlessly to provide world-class threat detection and response. Most importantly, you can do this without a high upfront cost or the stress of hiring, training and retaining talented analysts. In effect, you benefit from the economies of scale your provider offers, as well as the extra insight they gain into the threat landscape across their customer base.

This leaves your in-house security team freed-up to focus on what matters: providing strategic support for business growth and digital transformation initiatives. It could be the difference between success and failure as enterprises scramble for differentiation in a post-pandemic world.

A fully functioning Security Operations Centre can identify and neutralise an attack in less than 6 minutes.

Find out more about DigitalXRAID's Security Operations Centre here

01302 639 470 | info@digitalxraid.com | digitalxraid.com