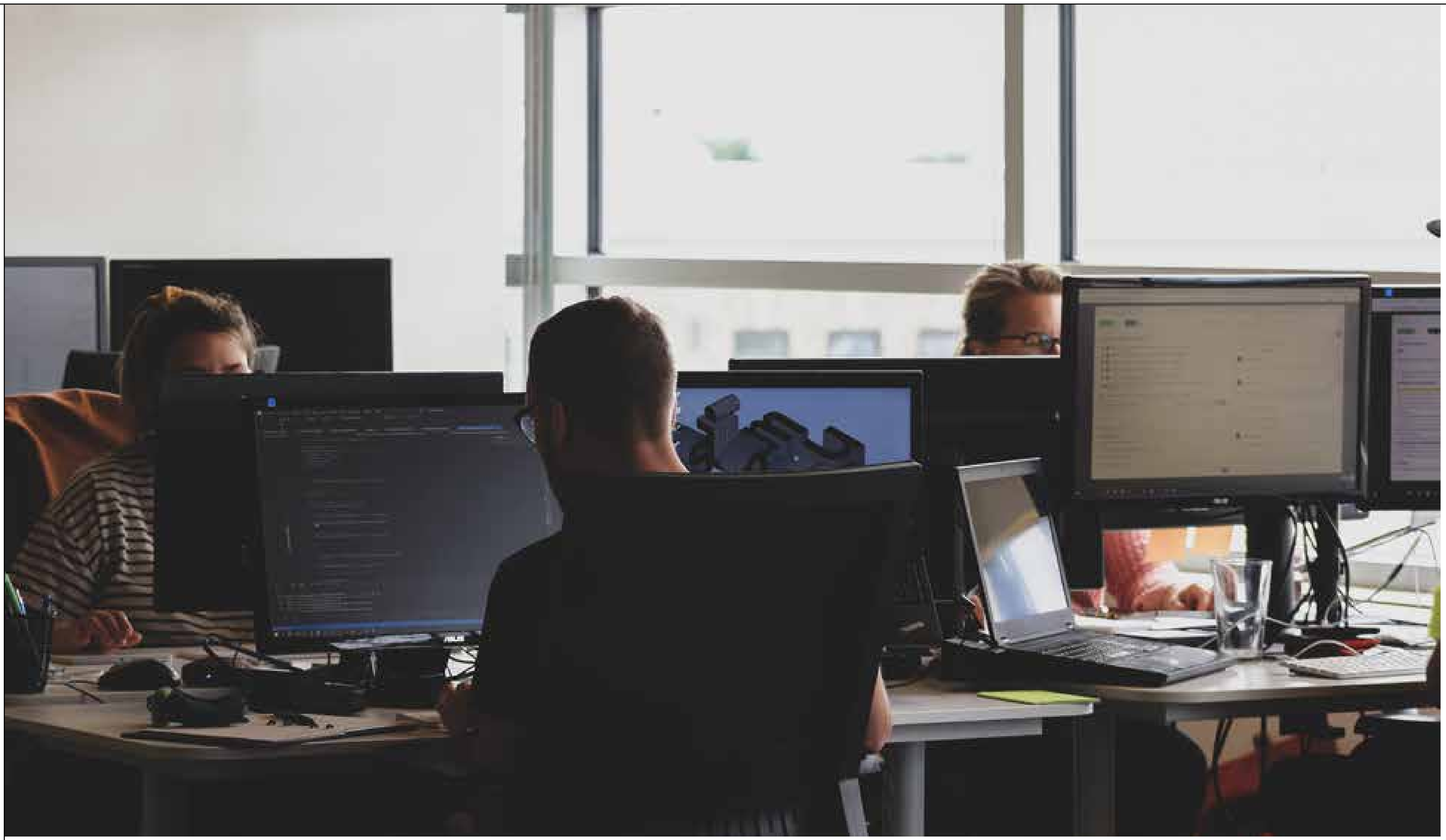

Picture credit: Unsplash

DETECT AND RESPONSE

Richard Ford *reveals how businesses can beat budget constraints by investing in managed security*

The ongoing economic crisis is taking a profound toll on societies across the world. In its World Economic Outlook series, the International Monetary Fund has been hitting home some hard truths. While inflation has declined as central banks have raised interest rates, underlying price pressures are proving sticky, with labour markets remaining tight in several economies.

Much has been said of the cost-of-living crisis that continues to rage on in face of these adverse economic conditions. However, for enterprises, the rising cost of doing business has become an equally critical concern dictating major strategic decisions.

According to the 2023 Global Business Monitor, which surveyed key decision makers from SMEs across nine countries, inflation (55 percent), energy costs (49 percent) and uncertain economic environments (28 percent) are the three major factors stifling business growth at present.

In an effort to navigate a multitude of cost-related issues, cash-strapped businesses are responding by scrutinising every expense, leaving no stone unturned as they cut budgets and streamline operations. For security leaders, this creates yet another tricky situation. Indeed, it's perhaps the worst possible time for enterprises to take their feet off the digital protection pedal.

If an incident occurs, organisations need to be able to respond at speed

Part of the reason for this can be attributed to skills shortages. According the (ISC)2 2022 Cyber security Workforce Study, the current shortage of security professionals sits at around 3.4-million globally.

Competition for talent is high, with seasoned professionals able to command ever greater salaries, pricing those making budget cuts out of securing the in-house security expertise that they need. Further, subscriptions and solutions deemed to be low value are being scrapped, weakening the arsenals of potentially understaffed, under qualified security departments.

It is nothing short of an uphill battle. Owing to financial concerns and constraints, organisations are often unwillingly dropping their guard at a time when criminal activity is ramping up, leaving gaping holes in their defences that are increasingly likely to be exploited. And if that happens, the costs can be immense.

Looking at Fortinet's 2022 Cyber security Skills Gap Research Report, it's estimated that four in five enterprises may have avoided breaches if they had better cyber security skills. Further, for those that did suffer from breaches, 38 percent had to spend more than a million dollars to remediate them.

It may look like a hopeless task: companies don't have the funds to properly protect themselves in the current economic climate, while the volume and sophistication of attacks continues to grow at speed. However, several steps can be taken to beat budget constraints and turn the tide.

Part of the problem lies in poorly optimised spend. According to a 2023 Interity360 Twitter poll, 31 percent of the 2,000-plus respondents said that 30 percent of their cyber security budget is allocated to tools and solutions which aren't being used to their full potential.

Here, organisations may need to have a rethink in terms of strategy. At present, many businesses continue to primarily focus on stopping the efforts of threat actors attacking critical systems and data in the first instance. This emphasis on prevention is undoubtedly important. However, it is also necessary to recognise that this is just one piece of an increasingly complex cyber security puzzle. Consider the way in which we manage fire safety.

It's not enough to hope that the measures you have in place prevent a fire from occurring. You equally need to ensure that if such a scenario arises, you have the fire extinguishers, fire alarms, fire exits and fire service on speed dial to ensure internal occupants are kept safe, the property damages are limited, and plans are in place to ensure a speedy return to normal service.

In a cyber security context, balancing the entire cyber value chain beyond prevention is critical for this very same reason. If an incident occurs, organisations need to be able to respond at speed. And if they can't, the impacts can be significant.

Concerningly, IBM's 2022 data security report suggests that it took an average of 277 days (over nine months) for businesses to identify and report a data breach. This is more than enough time for attackers to reap untold damage, as is no better demonstrated than by the infamous SolarWinds Breach uncovered in December 2020.

Here, attackers successfully broke into the systems of the US networks security provider, thereafter, injecting malicious code into its Orion software – a solution that was used by 33,000 customers at the time. When the organisation then sent out its next regular software update, the tampered code unknowingly created back doors that enabled the threat actors to infiltrate SolarWinds customers and deploy more malware. In total, it's estimated that 18,000 organisations including Fortune 500 companies and US government agencies installed the malicious update that went undetected for months on end.

Promisingly, organisations are aware they need to improve in several security departments. According to the Integrity360 Twitter poll, 33 percent of respondents feel threat detection is lacking most when it comes to cyber security and incident detection and response. This was closely followed by training and testing (27 percent), slow response times (26 percent) and lack of visibility (18 percent). To address these shortcomings, organisations should consider acquiring a more comprehensive selection of security solutions capable of not just helping to prevent, but also detect, analyse and respond to threats in real-time.

40 PERCENT FEEL THAT CYBER SECURITY TESTING IS BETTER HANDLED BY EXTERNAL PARTIES

Of course, this is easier said than done, particularly given many enterprises lack the skilled professionals needed to orchestrate security optimisation and improvement programmes. So, what's the solution? How can organisations wriggle out of being stuck between the skills shortage rock and budgetary-constrained hard place?

Enter Managed Detection and Response (MDR) – an effective means of accessing the market leading expertise and solutions needed to achieve enhanced protection without breaking the bank.

Critically, MDR offers protection across the whole value chain, delivering everything from real-time threat detection, proactive threat hunting, and incident containment and response to security incident analysis and threat intelligence, compliance reporting, and 24/7 monitoring for businesses.

It is a carefully curated selection of security solutions that leaps beyond traditional security methods, enabling firms to rapidly respond to and contain threats that have overcome the first line of defence – be it on networks, endpoints or the cloud.

Here, there is further reason for optimism. Critically, the Integrity360 poll shows that 29 percent of firms agree that MDR should be prioritised, indicating that they will begin to allocate most of their cyber security budgets to managed security moving forward. This is no coincidence, the study also revealing that those enterprises already utilising MDR services have seen a 62 percent reduction in the average number of security incidents per year.

While the extensive toolset that MDR offers can dramatically enhance the prevention, detection and response capabilities of any organisation, the key

▶

often lies in the fact that service users gain access to on-demand and proactive support from the seasoned security professionals that they crave.

In the current economic climate, enterprises are visibly assessing the value and efficiency of their current security setups, with many recognising the merits of investing money and trust in service providers. The Twitter poll again highlights that 40 percent feel cyber security testing is better handled by external parties than in-house professionals, while 35 percent believe a service provider is better placed to manage cloud computing security.

IT TOOK AN AVERAGE OF 277 DAYS FOR BUSINESSES TO IDENTIFY AND REPORT A DATA BREACH

Outsourcing can be both a flexible and cost-effective approach. By embracing MDR services, enterprises themselves aren't required to spend significant sums either developing or outright purchasing expensive tools or software. Not only that, but MDRs are able to continually invest in developing and enhancing their security offerings, guided by cutting-edge threat intelligence, and financed by the economies of scale they achieve from delivering services to many customers.

It's clear that firms themselves recognise these merits, with many leaning more actively towards a collaborative security stance. Indeed, over a third (36 percent) view increased defences as the most significant benefit of cyber security collaboration, with the same number (36 percent) highlighting faster response times as the key benefit of embracing managed detection and response services.

As we move through 2023 and beyond, it's important to acknowledge that the increasing volatility we see in the threat landscape isn't a phase. Current threats are only likely to get worse. Looking at IBM's latest analysis, the global average cost of a data breach in 2023 was $4.45-million, marking a 15 percent increase in the space of just three years.

Further, come 2025, it is estimated that the total global cost of cyber crime will reach $10.5-trillion – a figure that exceeds the current GDP of every country barring the USA ($25.03-trillion) and China ($18.32-trillion).

Any notion that this is a temporary wave of increasing activity which can be ridden out must be avoided. If organisations don't react, adapt and evolve to the increasing sophistication of cyber criminals, they will leave themselves open to potentially catastrophic damages.

It's clear that organisations fear these impacts, the Integrity360 poll suggesting that financial loss (4 6 percent), loss of trust (28 percent), and reputational damage (20 percent) are all significant consequences of data breaches. Of course, it is easy to sympathise with firms fearing that budgets and effectiveness go hand in hand when it comes to security. However, even in a cash-strapped economic environment, there are ways to make every penny go further.

By embracing MDR, organisations can ensure their security strategies are moving in tandem with a changing threat landscape, tapping into transformative expertise, tools and technologies for fraction of the in-house equivalent cost ●

Richard Ford is CTO at Integrity360.

It is estimated that the total global cost of cyber crime will reach $10.5-trillion by 2025

Picture credit: Unsplash