WHITEPAPER

Vulnerability Detection and Remediation

Are IT teams cracking under the extra weight?

LIMA

Contents

Executive summary

The turbulent economic environment of the technology sector in recent years has spun many businesses into turmoil, as we try to find a level footing once again.

Business leaders are faced with slashed budgets and higher targets than ever, as they strive to meet revenue goals while meeting increasingly rigorous regulatory requirements.

It's a juggling act, as leaders tackle the increased costs of retaining employees, maintenance of costly office space in the remote working world and steep price hikes from vendors for software, support and installation services.

2023 was a real turning point for many organisations. The bubble had burst for the technology sector and the ripple effect of redundancies cascaded like a tsunami outwards from Silicon Valley.

The result? Reluctant investors, deep concern in the board room and a renewed focus on retaining customers and talented employees as businesses sought to stay afloat.

While we're no longer in the eye of the storm, some of these challenges ring true, still, in 2024. And as we surge towards 2025, business leaders must continue to review the lessons learnt and the areas to address now for a more secure future. In more ways than one.

Throughout this whitepaper, we will assess the challenges faced by businesses, and notably, IT teams in 2023, with steps to help your team identify and resolve gaps in their security profile and move forward effectively.

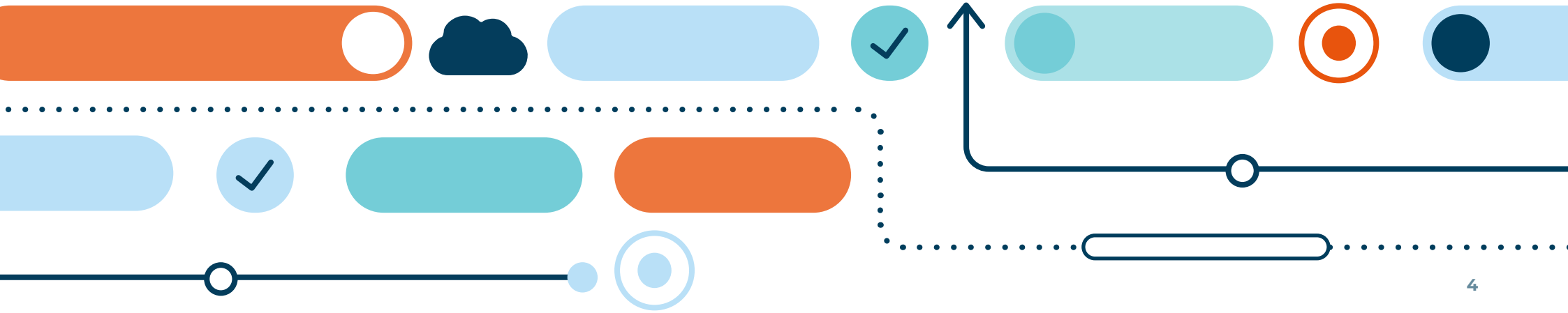
1

The evolution of the IT team

The role of the IT team has changed beyond that of simply an IT helpdesk. It is a business-critical function that if left to flounder, could have serious implications on the overall health and wealth of the organisation.

While once the IT team was responsible for getting new team members hooked up to their desktop, that same team must not only keep that desktop operational but maintain a vast cloud infrastructure and ensure the business is protected against a growing army of cyber-criminals.

Business as usual activity for the IT team has evolved, but has the business noticed?



2

How was the success of the IT team hindered in 2023?

According to a LIMA poll of IT teams, respondents unanimously believe that ‘It’s a bit of a mixed bag’ when it comes to the added responsibility of vulnerability being effectively managed by their team.

A result that speaks to the chaotic nature and juggling of resources, roles and responsibilities amongst IT teams. It’s vital that we now take the time to understand how this environment has come to be, and what we can do to remove the obstacles that hinder success amongst talented IT professionals.

2023 was a tough year for IT leaders

Technology Implementation

Removing legacy or end-of-life equipment from use within the business

Immense importance was placed on moving away from end-of-life equipment, much of which is likely to have been installed pre-pandemic and has come to the end of its useful life span. Renewing is the only option, with businesses seeking to invest capital to reduce spending in the long term and bring inflating costs under control.

IT teams were charged with the lengthy and costly task of removing and replacing legacy equipment within organisations.

Renegotiating contracts or migrating data to new systems

With the removal of legacy technology and transition to Software as a Service (SaaS) systems from physical, on-premise infrastructure, comes the need for negotiating new contracts and outsourcing agreements. All of which can become complex, resource-heavy and time consuming.

Providing self-service IT to teams across the organisation

The pandemic was the catalyst of an unprecedented shift in workplace culture, which has spanned beyond lockdowns as many businesses adopted hybrid or remote working as standard.

IT teams are responsible for enabling hybrid and remote operations and providing employees with the ability to self-serve; right down to actioning password resets without IT intervention.

Hiring and retaining talent

Providing regular one-to-ones

Talented IT pros know their worth, but are you letting them know that you do too?

Retaining talent is a major challenge in every department, more so in IT roles than any others, with the increasing demand for their immensely sought-after-skills and experience. It has become imperative that IT leaders assure their teams of the value they add to the business, a previously – relatively – simple task that has become a challenge without regular in-person one-to-ones.

Ensuring training is provided before it is required

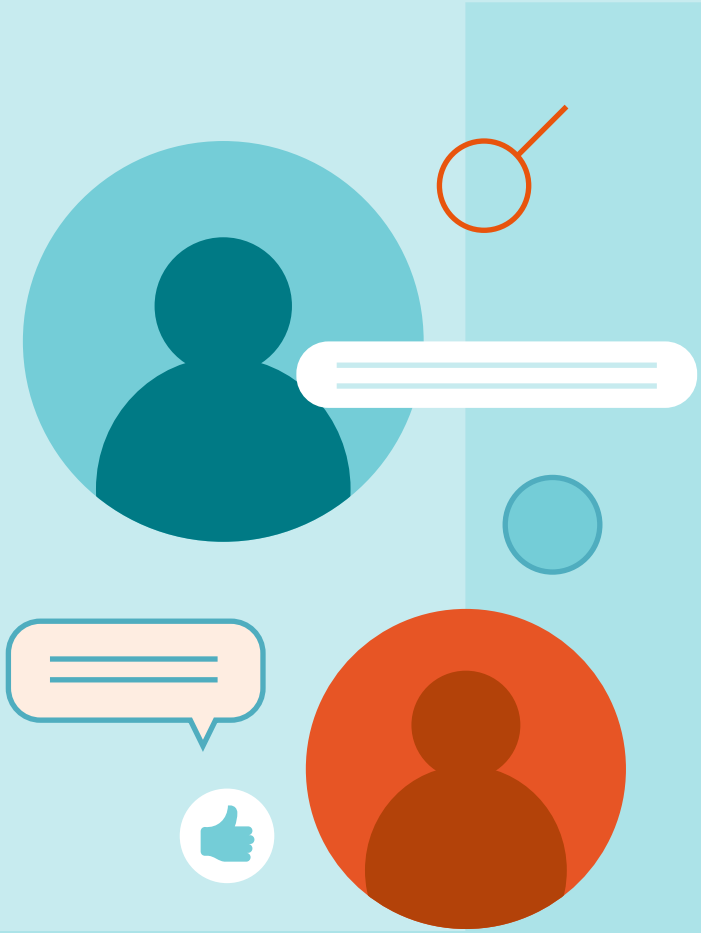
An estimated 70% of employee learning is acquired on the job[1], or via knowledge transfer from adjacent departments and teams. Ensuring integrated, organic learning continues to occur and thrive in the hybrid working environment has been difficult for IT teams; with whom responsibility for facilitating training typically lies.

Driving workplace culture and employee happiness

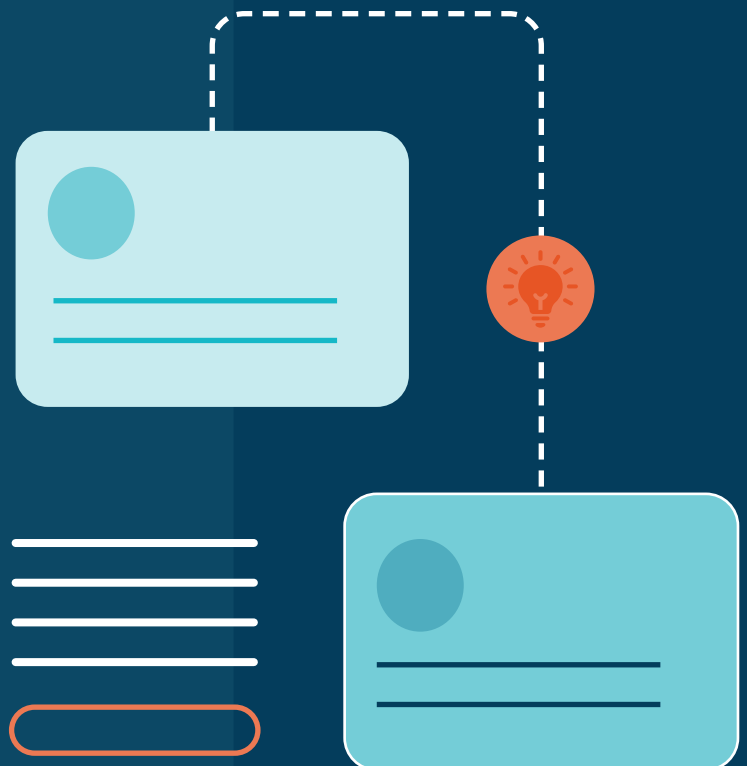
How do you create a thriving company culture, when 50% of the organisation opts for remote working?

The tools a business chooses to use are implemented by IT, who are then responsible for monitoring the efficacy of tools in both the office and home environment.

It's vital that all tools are helping to facilitate remote or hybrid working, and do not become a hindrance to both productivity and employee happiness.



Source: 1. Devlin Peck: Employee Training Statistics, Trends and Data in 2024; 10/01/2024



Cross department collaboration

Alignment on key priorities across teams

How do you make sure that your team's priorities are at the top of the pile?

Managing priorities across teams can be difficult in the most collaborative of environments, with every department tackling the pressures of their own specific challenges. Throw in hybrid and remote working with the lack of regular face-to-face interactions, and it is possible to see how swiftly dysfunctional cross-departmental communication can manifest.

Communicating between virtual and physical worlds

This is certainly not an IT-centric challenge, but one experienced across the board by departments from marketing to finance and HR.

Team leaders continue to tackle the new world order presented by hybrid and remote working, and effective communication between virtual and physical team members.

Providing a standard technology experience to all staff

All team members deserve to receive the same Digital Employee Experience. This is the holistic experience with the digital workplace provided by IT, based on the performance of the team member's device, applications, networks and end-user sentiment.

Employees must be successfully enabled to have a positive impact on the business. This puts pressure on the IT team to ensure employees are not hampered by slowdowns, crashes and disruptions, while juggling their existing workload.

3

Where are IT teams focusing their efforts in 2024?

More than 59% of IT teams spend most of their time providing IT support, and just 16% of their time protecting against security threats[2].

As business leaders strive to move onwards and upwards throughout the decade – growing revenue, acquiring talent and developing footholds in new markets – it is vital that IT teams are given the time and room to drive business critical areas forward.

In 2024, IT teams seek a transition from business-as-usual IT support, and towards activity that will drive progress within their teams and beyond.

Source: 2. Exclaimer: The state of IT – IT's role in fuelling organisational growth

Facilitating new focuses in 2024 and beyond

Streamlining repetitive tasks

- Automating parts of the business and team processes
- Reducing time between key steps and actions
- Ensuring no single members of the team are a point of delay or failure

Adopting AI technologies

- Assessing the right technologies are utilised and widely adopted
- Ensuring AI usage is safe, ethical, secure and productive

Time is of the essence, and IT teams know just how to create more of it.

Streamlining repetitive tasks, that can be automated at the click of a button, is just one way of generating more time across the business. Redundant processes can be removed entirely, while easing the load on team members in admin-heavy roles that cause delays; and often create a single point of failure.

AI may be at the top of the buzzword bingo tree, but it's with good reason. In 2024 we have seen the release of accessible, consumable AI technology such as Microsoft's Co-Pilot, that has the capacity to transform ways of working.

However, as with all emerging technology, it is essential to execute due diligence and ensure that it is safe for widespread use amongst the business, secure and ethical; does it meet green credentials?

Improving security

- Driving awareness of cyber security posture across the business
- Ensuring end users are using systems and data securely
- Monitoring and auditing usage of IT systems to detect early signs of compromise

Cyber security is no longer an optional extra, but a critical component for any and every organisation. The responsibility for maintaining a secure operating environment typically falls to the IT team, and it is no small feat to add to the already hectic mix of day-to-day responsibilities.

It's important to note here that the 2024 areas of focus are not in place of the tasks that presented challenges in 2023, but are additional items added to the ever-expanding list of demands put at the feet of the IT team.

And we haven't even touched on Cyber Essentials yet.

4

What is Cyber Essentials?

Cyber-attacks may vary in size, shape and severity, but they all give organisations cause for sleepless nights. Cyber Essentials is a UK Government-backed scheme that helps businesses guard against the most common cyber threats, and complying with the scheme is a clear, public demonstration of the organisation's commitment to cyber security.

UK organisations have two certification options:

Cyber Essentials – The self-assessment

This option gives businesses protection against a wide range of the most common cyber-attacks. Without which, the business becomes an easy target for basic attacks, that quickly escalate to unwanted attention from sophisticated attackers seeking to exploit known weaknesses.

Cyber Essentials Plus – Technical audit

Cyber Essentials Plus has all the hallmarks of Cyber Essentials – giving businesses the tools to stay secure in the face of the most common cyber attacks – but instead of a self-assessment, the Cyber Essentials team carries out a hands-on technical verification.

Where does Cyber Essentials fit into the scope of the already busy IT team?

Sounds fairly straightforward, quite a simple and common-sense approach to keeping businesses secure and ensuring they and their customers are protected against cyber-attacks. It's certainly not a framework to ignore.

But what toll is this additional requirement taking on the already task-laden IT team?

The scope of Cyber Essentials Plus increases every year, and the security requirements also change.

It's been put on the IT team to manage vulnerabilities, and by that I mean, if there are out of band patches released by the software vendor or the infrastructure vendor, you have 14 days to apply them if they are classed as high or critical by the vendor.

That is a new responsibility that we must deliver day or night, over seasonal holidays, periods of annual leave – it's something that the business is absolutely committed to fulfilling.

My takeaway from this is, is this actually the best use of our time? Given that the challenges in 2024 are more significant in terms of business transformation, is it the right thing to be spending the team's time on these tasks?

Ollie Potts, Head of Product at LIMA

5

Are IT teams cracking under the pressure?

The responsibilities of the IT team are mounting up, particularly as they seek to address the increasing pressures of cyber security compliance.

Now let's address the elephant in the room. For some, larger organisations, with healthy-sized IT teams, this scope of work is manageable, if causing them to feel a little stretched at times. For small-to-medium sized businesses, it's a different story.

Not only are these organisations likely to be hit hardest by budget cuts, but they may also be struggling to retain talent and close the skills gaps required to successfully fulfil some of the more specialist tasks outlined throughout this whitepaper.

Is there a viable solution for small-to-medium sized businesses?

Cyber Essentials is a pass-fail self-audit and then external audit. The CIS top 19 gives you a score of how well you're doing in different areas.

We did a gap analysis and said we don't just want to pass the standard, we want an idea of how well we're doing in different areas and where we should concentrate for the greatest improvement in our cyber security.

We identified that we needed a managed detect and response service and we needed to manage our laptops much better. Neither of these solutions were going to be particularly cheap, but I've got the backing of the board, the board are very invested in cyber security and recognise that it's not a like to have, it's a must have. And if boards tell you that you must do something, they'll make the money available.

This needs a security expert. Someone that's expert in building remediation packages that can be rolled out, and we had decided that we didn't need to employ a new staff member to do that. That option introduces more problems. They go on holiday, they might get ill, they might not have complete knowledge. Instead, we saw that there were a lot of advantages to going with a managed service, from an organisation that's got a lot of people that can help.

James Osborne, Head of IT at Two Rivers Housing

6

Is 2025 the year your business reaches new heights?

Creativity requires time and space to grow. Without it, we're stifled, focused only on completing the task in front of us as quickly as possible, often sacrificing quality work for quick work. In this environment we are not allowing ourselves the scope to think about the bigger picture and what comes next.

The same is true for any specialism. So, what can business leaders do to give their IT teams this creative freedom to grow, and ultimately reach their own goals in 2025?

Give your IT team the gift of time

Throughout this whitepaper we have discussed the responsibilities laden on IT teams. Now let's think about reducing the burden, sharing the load and freeing up your team to achieve more.

For the last 10 years, IT teams have been responsible for the Identity and Protect elements of the NIST Framework* (fig. 1), while a security company will typically handle Detect, Respond and Recover. But that needn't be the case, you can expect more and you can expect better.

These areas aren't normally taken care of by an IT outsourcing company, or a managed service provider like LIMA. Typically, these are the team's responsibilities.

How does that work? And how do you make sure that even if you do outsource, you still have that chance to govern what is going on with the organisation, based on the services that are offered?

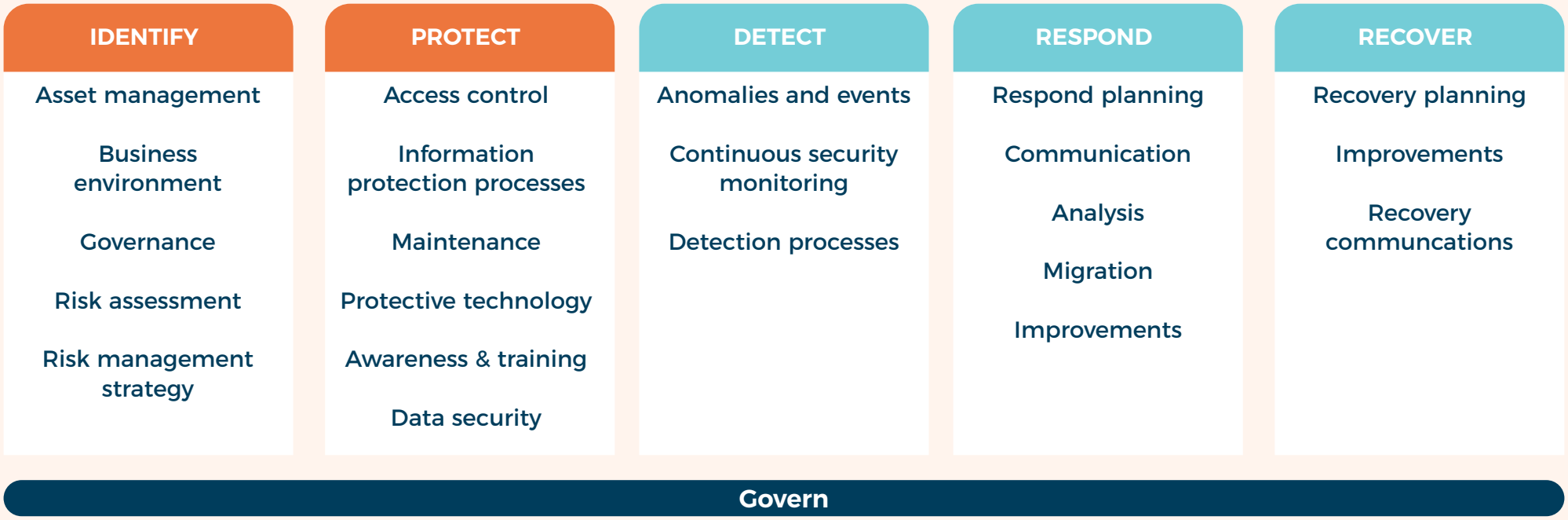
Ollie Potts, Head of Product at LIMA

Security processes managed by the IT team

***Definition**

The NIST Cybersecurity Framework (CSF) 2.0[3] provides guidance to industry, government agencies, and other organisations to manage cyber security risks. It offers a taxonomy of high-level cyber security outcomes that can be used by any organisations – regardless of its size, sector or maturity – to better understand, assess, prioritise and communicate its cybersecurity efforts.

Fig 1



Source: 3. The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology; 26/02/2024

Expect better and do more, with LIMA

Freeing up time for your IT team starts with VDR.

LIMA reviews your entire IT environment to reveal and resolve any vulnerabilities, within a single outstanding SLA.

VDR covers 500+ technologies and is backed by 25 years of specialist experience and expertise. We take care of vulnerability, detect and remediation, so your team can focus on your business.

Keeping you secure – and compliant

In an ever-evolving cybercrime environment, VDR seamlessly maintains your security and compliance, operating within an outstanding SLA to speedily identify and remediate vulnerabilities and risks.

Review

Your IT security is only as strong as its weakest points. VDR shines a light on every aspect of your hardware, software, third parties, systems, networks and applications – and continuously monitors it in depth, across 500+ technologies.

Reveal

Your security may not be as robust as you think. One recent VDR review revealed a remarkable 12,000 weaknesses in a single system. VDR identifies all those hidden vulnerabilities, prioritises them and keeps you informed about your risk profile with tailored monthly reports.

Resolve

We don't just reveal those vulnerabilities. We resolve them, with unprecedented remediation coverage across your IT technologies – meeting and exceeding all regulatory requirements with our outstanding guaranteed SLAs, aligned with Cyber Essentials Plus.

Protect your business effectively and efficiently with VDR

contact LIMA today

0345 345 1110

enquiries@lima.co.uk

LIMA