SecureLink 2017 Security Maturity Insight Report

www.securelink.net/sma

TABLE OF CONTENTS

FOREWORD

Organisations of all types, and especially those which have a digitally-focused business strategy, require cybersecurity programmes and capabilities. The requirement for these capabilities is driven by the ever-growing likelihood of cyber attacks and an increasingly complex threat landscape. However, implementing appropriate technical and organisational safeguards to protect digital assets can be a challenge, largely as a result of deep-rooted behaviours, complex interdependent systems and an explosion of digital-first strategies.

SecureLink has seen first-hand how personal and professional reliance on technology has dramatically changed. Just a decade ago, an IT department controlled what users had access to and how they connected; now, however, users demand access to applications of their choosing at a time they specify, and on a device and platform they prefer.

Cybersecurity has changed dramatically, not only in name [information security, IT security, cybersecurity] but also as a business function. Historically seen as an expensive and retrospective checkbox exercise, it is now a critically important business unit that enables business innovation and transformation. Furthermore, the challenges facing IT leaders almost always differ between organisations.

Since 2016 cybersecurity teams across Europe have been utilising the SecureLink Cybersecurity Maturity Assessment platform, which provides a structured and quantitative approach to the measurement of security maturity. The unique dataset that results from these assessments provides real insights into the strengths, weaknesses and challenges of a growing number of cybersecurity teams.

This actionable intelligence is a natural bi-product of measuring cybersecurity maturity. Expressing maturity indicators in terms of risk informs IT leaders where to make interventions in their security programme – and it's here we share with you some key insights into the strengths and challenges currently facing organisations across Europe.

The assessment data presented here has been analysed across two main datasets. The first of these focuses on people, process and technology: the three critical elements of a cybersecurity programme. The second focuses on prevention, detection and response actions. From these datasets, the strengths and challenges presented can be considered and appropriate paths to improved security maturity can be determined.

CONTRIBUTORS

Insights and data contained in this Report are based on assessments performed between October 2016 and October 2017.

Acknowledgements and thanks go to the following contributors:

Richard Jones, Chief Information Security Officer, SecureLink Group
Eward Driehuis, Chief Research Officer, SecureLink Group
Ade Taylor, UK CTO, SecureLink UK
Maikel Roolvink, Cybersecurity Advisor, SecureLink NL
Konrad Pawelec, Assessment Services Manager, SecureLink UK
Grant Paling, Head of Managed Services, SecureLink UK

THE NEED TO MATURE

Frequent and repeated cyber attacks demonstrate the need for improved cyber-security in organisations of all sizes and types. Unlike traditional organisational and operational risks, however, the cyberthreat is continually changing, and organisations must constantly identify new methods to face this challenge. cybersecurity maturity is a series of indicators that identify capability within a given area of a comprehensive cybersecurity programme. An organisation needs to establish and maintain these capabilities along with a set of behaviours, practices and patterns designed to protect against evolving cyberthreats.

Traditional approaches to cyberthreats utilise a risk-based approach which is largely dependent upon the organisation: budgets, attitudes, resource and knowledge (of threats). The organisation would then focus its defence strategy on risks with high probability and moderate impact. Low probability, but high impact, risks would be categorised as 'theoretically unlikely'.

However, the threat landscape is changing at an unprecedented pace, and those once 'theoretically-unlikely' risks have started to materialise frequently and repeatedly. Today, this new group of very-high-impact-risks grab the attention and focus of executive leadership teams, and has firmly arrived on their agenda as cyber risk. Consequently, the efforts invested in addressing cyber risk (preventing and detecting criminal and unauthorised use of data) are now known as cybersecurity. We now accept cybersecurity to consist of the framework of people, process and technology designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

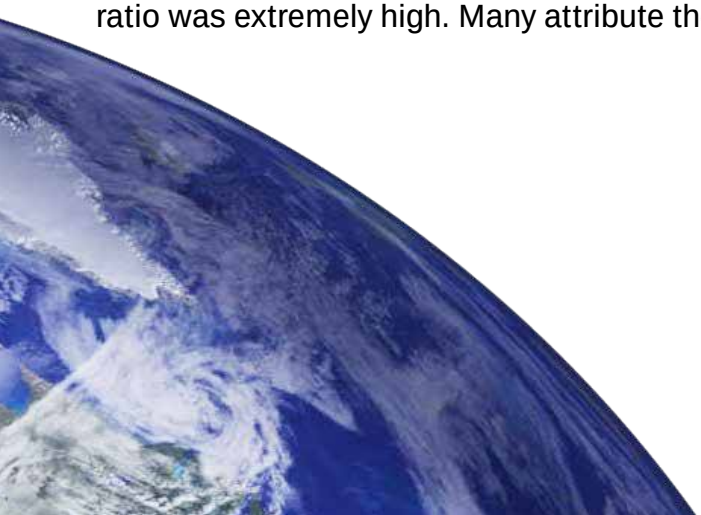
Businesses should note that the shift in the risk-lens represents an ongoing trend. Very-high-impact risks will become increasingly frequent, forcing us to become better at protecting assets and devising creative solutions to mitigate these risks.

THE GLOBAL THREAT LANDSCAPE

2017 has hailed more disruptions than the entire decade before it. At SecureLink we identify three key trends in the threat landscape impacting the complexity of today's infosec management:

1. Organised cybercrime targeting enterprise
Ten years ago organised cybercrime targeted finance exclusively. Over the years, (online) retail was added, then criminals branched out to healthcare, law firms, hospitality, and in the recent years manufacturing, logistics and supply chains. In 2016, the largest criminal moneymaker was business e-mail compromise (CEO Fraud). Criminals are investing more time in manual campaigns. Ransomware is not as popular as people think, but due to the enormous collateral damage it's the number two cyber risk. Fraud and bespoke campaigns is something to watch out for, with lateral movement (espionage techniques) now being used by criminals in their attacks.

2. Weaponisation of malware.
With Wannacry and Notpetya, two global attacks, with hundreds of millions to billions worth of damage, we entered a new era in cyber threats. Due to the absence of (automated) cash out processes in these attacks, many believe the purpose of the attacks was not to "make money", but rather to "destroy". As both attacks made only a few hundred thousand dollars in bitcoin, the collateral-to-ransom ratio was extremely high. Many attribute the attacks to nation states, with North Korea and Russia being the top mentioned. Whomever is behind this, and whether or not the nation state narrative is true, these attacks hail the weaponisation of malware – regular enterprises can get caught in the crossfire.



3. Activists and Nation State actors.
In 2017 the geopolitical landscape has seen a considerable amount of high impact events, including the US government tone change, Brexit, elections in Europe, and tensions in the middle east, southern Asia and other parts of the world. Nation states are expanding their cyber capabilities, and press and opinions makers voice their opinions online, activists (motivated individuals and organized groups alike) join online campaigns to spread information and propaganda. Ten years ago threats were straightforward: there were spies stealing IP, and criminals stealing money. Now, with these new adversaries, enterprises can be targeted, they can experience collateral damage, and they can get caught in the cross fire.

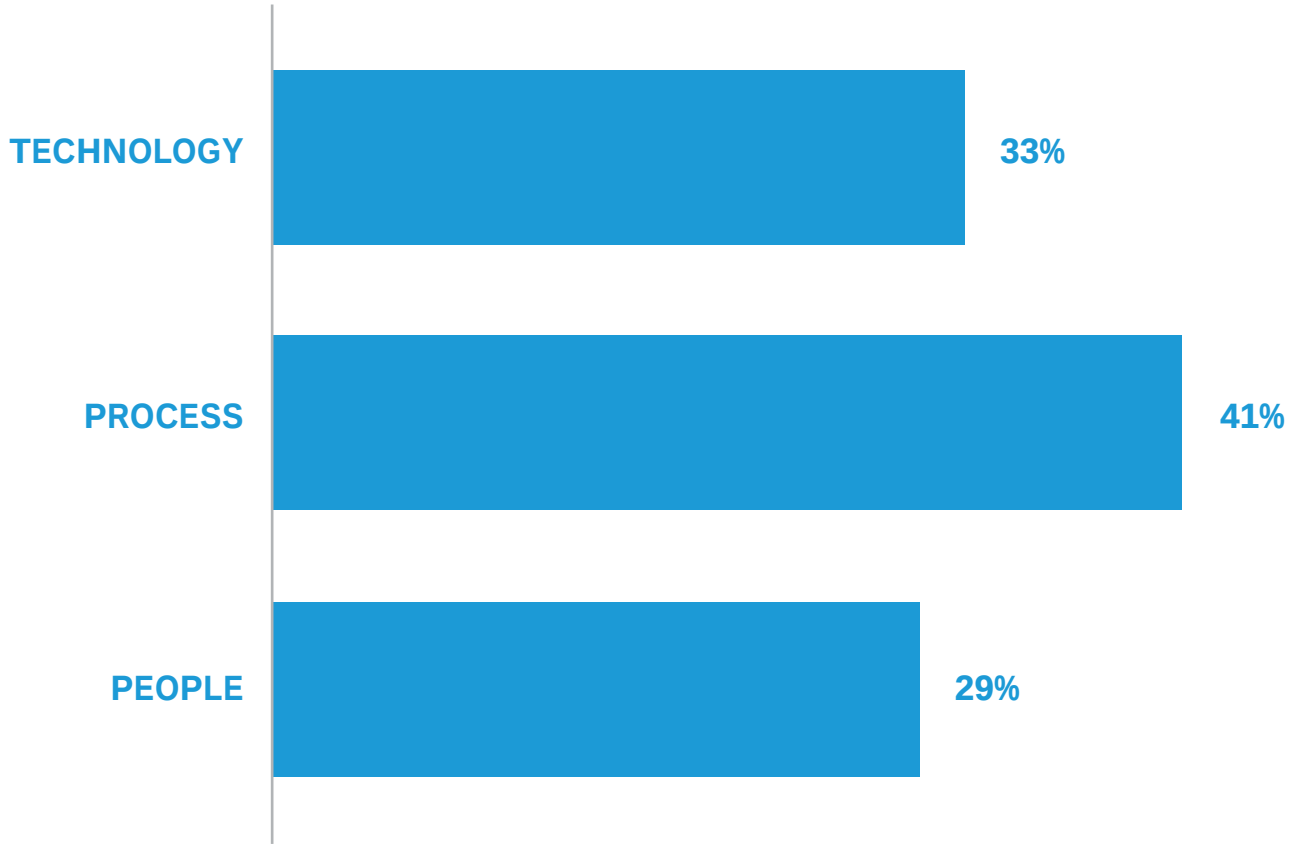
These changes to the global threat landscape indicate infosec is getting more complicated, and the CISO's responsibilities span a much broader attack surface. When designing your infosec processes, these trends need to be taken into consideration. Lawmakers in many countries are pulling their weight: Europe is pushing GDPR and PSD2, while NIST is getting more traction internationally. While these are valiant efforts to build resilience across geopolitical regions, there is little global response to threats increasing. Activism, cybercrime, espionage and geopolitics blurring. Knowing one's specific risk profile and which attack vectors and regulations are relevant is more important than ever.

PEOPLE PROCESS & TECHNOLOGY

INTRODUCTION

Establishing and maintaining cybersecurity capabilities requires people (the experts), processes (that guide the experts), and technology (that automate what the experts design). This report explores the challenges and effectiveness of each of these aspects of cybersecurity, and shows how you could improve your own cybersecurity maturity.

Average Score Across Industry



PEOPLE

PEOPLE OVERVIEW

A cybersecurity programme must begin with a sponsor – that is, a member of the senior leadership team. This sponsor should be a respected executive, widely acknowledged by the organisation as **being in charge of** cybersecurity and responsible for its outcomes. There is no one-size-fits-all approach to sponsorship. However, as with cyber risk, it is recognised that the sponsor must have specialist understanding of cyber risk and be competent to deliver a cybersecurity programme dynamically adaptable to protect business outcomes.

While cybersecurity has evolved from an afterthought to a key item on the boardroom agenda, solutions to new threats continue to be approached with traditional IT methods, either through newer or more tools, or by expanding established processes to include security operations.

This trend of addressing new threats with existing capabilities has continued in the context of people. Cybersecurity executive leadership has been achieved through additional responsibilities placed on existing roles - roles such as IT Director, Head of IT or, in some cases, CFO. This approach is usually a temporary solution, and one that rarely considers the (often already extreme) workloads that accompany such roles.

At the same time, operational security capabilities have grown incrementally; firewall engineers transition into security analyst roles, while support teams become incident response teams. In some cases, technical IT teams recognise the need for security and it is here that basic security roles are born. This is a classic bottom-up approach and certainly not the kind of top-down leadership which should characterise companies looking to achieve even a basic level of security maturity.

This leads us to the obvious question: what are the specific people-challenges identified in our multiple-industry-data?

PEOPLE CHALLENGES

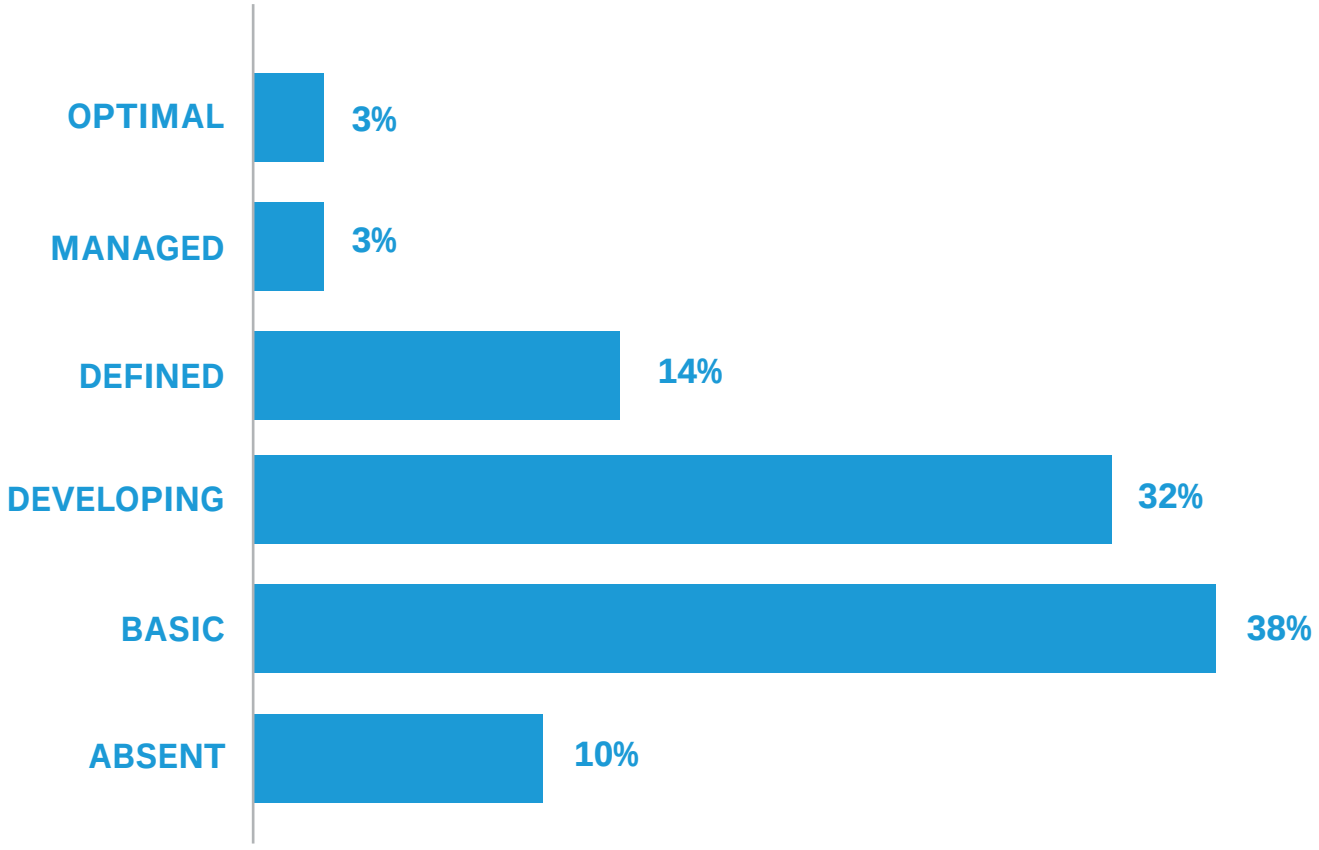
Within all Security Maturity Assessments performed, the area of People is the one that most noticeably scores below an average of 30% (in terms of security maturity).

The assessment data shows that all organisations have highlighted resourcing issues as a major concern for fulfilling requirements in the ‘People’ area of cybersecurity operations. While business-as-usual will - and should - always be prioritised over major changes to operations, lack of suitably

qualified staff can limit any company's capability to prevent, detect, and respond to threats.

The solution to this issue is, typically, to assign a 'new task' to an administrator's list of duties. This invariably means the additional task is sidelined and cannot be given full attention.

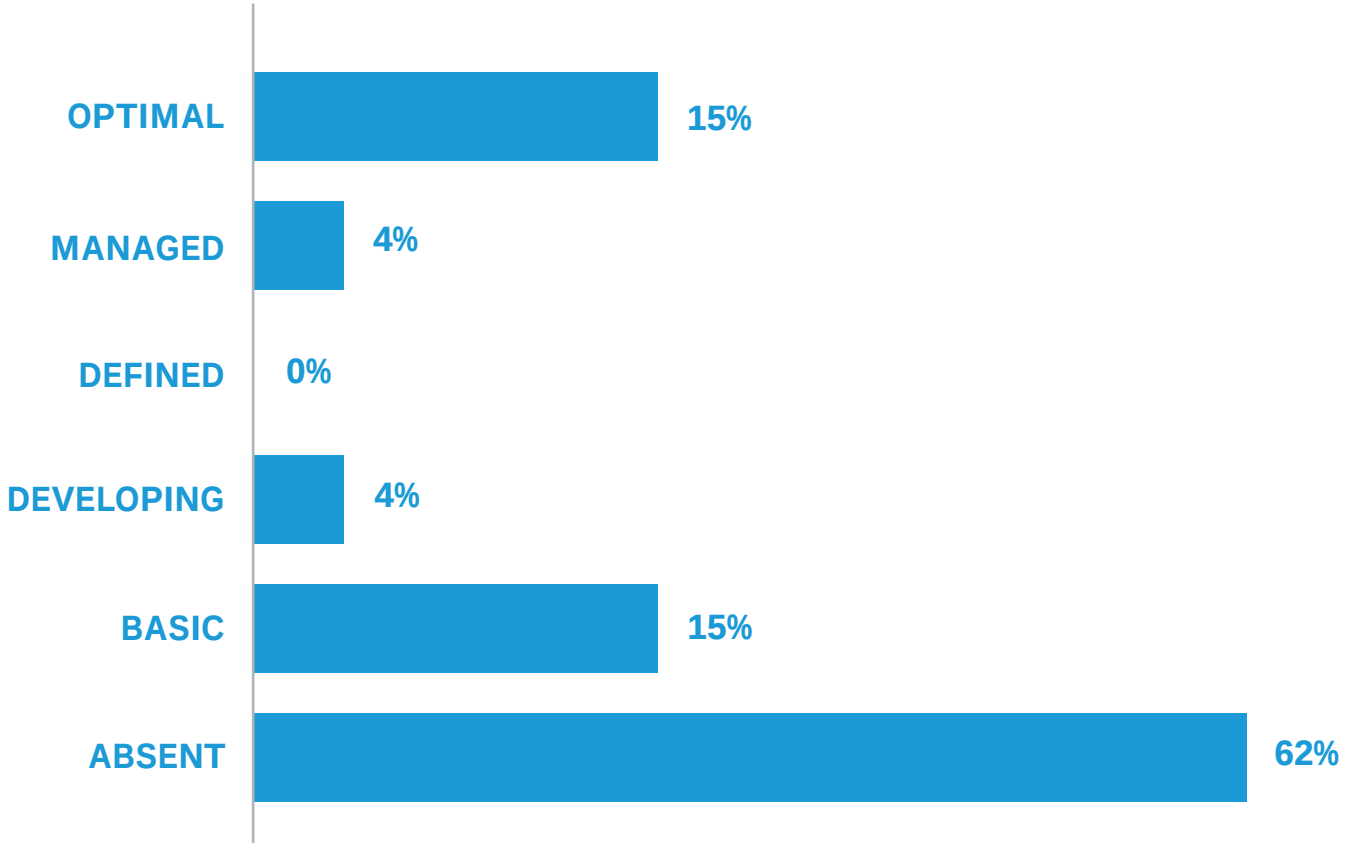
Do You Have Staff With IT Security Tasks Explicitly Stated In Their Job Descriptions?



By way of example, consider an improvement project, intended to mandate the quarantine of high-risk emails. When the quarantine process begins for high-risk inbound emails, the under-resourced administrators often don't have the time to respond to service requests for the release of urgent emails, or - more importantly – determine whether the email is a legitimate threat. As a result, the decision is taken to switch off the quarantine capability, as the administrators see it as a distraction.

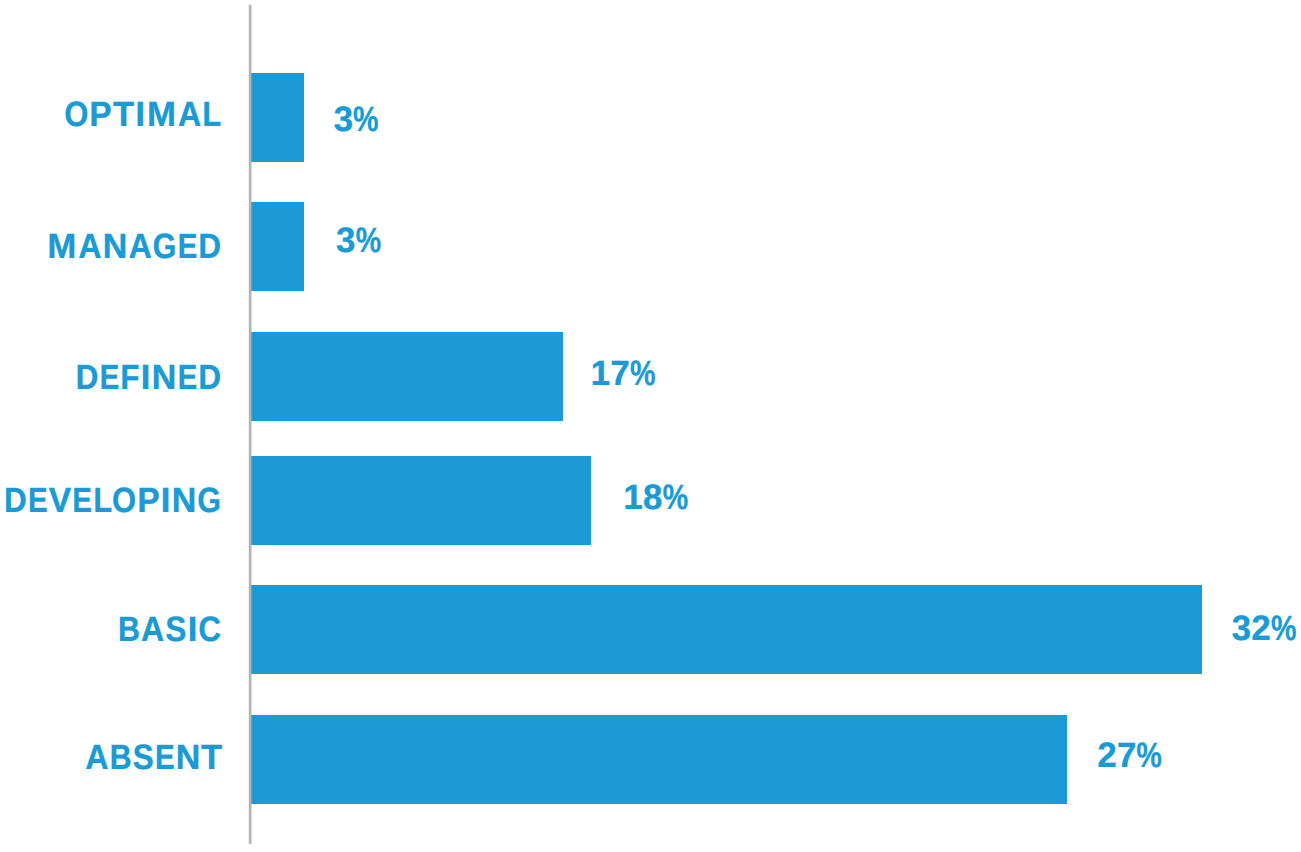
The assessment's Security Operations capability focuses on the centralised collection of logs from critical systems and network components. Capabilities are then established to build a security picture and act on anomalies. However, analysis shows that 62% of organisations have no security operations capability whatsoever (they are recorded as "absent"). This results in logs being collected, but wasted, as there is no-one with the time or expertise to interpret the output.

Do You Maintain A Fully Operational SOC Team?



Most organisations also lack senior management with explicit cybersecurity oversight and accountability. Indeed, at executive management level, it is still uncommon for the Information Security role to exist. This role usually supports the creation of policy and works together with the business to establish the best solutions for the maintenance of safeguarding controls. This enables the business to grow, while ensuring that cybersecurity incidents are handled and communicated effectively.

Do You Have Senior Management With Explicit Cybersecurity Oversight And Accountability?



This crucial role is often shared between the operational teams responsible for the day-to-day activities of passive security defences. These teams will then periodically provide basic cybersecurity reports to IT Directors.

PEOPLE STRENGTHS

Data shows security operations as a challenging area. However, where is does exist, it appears to be well implemented. Although the data doesn't demonstrate clearly how these organisations achieve this level of maturity, it's reasonable to suppose that they have selected a managed security services partner and are operating either a hybrid or fully outsourced model.

There are several key indicators of the need to do better at cybersecurity. These include the regulator's demand for change (with additional guidelines set out by the General Data Protection Regulation), the need to have a bulletproof corporate communications capability, and the elevation of cyber risk to the executive leadership table. Data shows that businesses are improving, though it's clear that some need to do more, and do it quickly.

PEOPLE INSIGHTS

Strengthening your cybersecurity team can be achieved in many ways. The quickest and simplest means of delivering a step change in maturity is the addition of managed security services. Before taking this route, however, organisations should first review their internal resource to identify and retain individuals who have both the ability to realise an effective cybersecurity strategy, and intimate knowledge of the inner-workings of their organisation's IT. Educating and empowering these colleagues to make interventions in the security architecture and passive defence capabilities will deliver effective cybersecurity maturity at an appropriate pace and cadence for any particular organisation.

A more common approach is a hybrid of both retained and outsourced capabilities. This allows an organisation to balance any policy of outsourcing with the simultaneous delivery of significant risk reduction.

Where organisations choose to leverage managed security service providers, they should change their approach to monitoring their security programme. Transitioning to a service-focused architecture demands better understanding of supplier and dependency risk - in particular, a smarter approach to contract and service management. If executed well, the rewards will be high.

University graduate schemes are also a resource stream that organisations should consider tapping. Cybersecurity-degree qualified individuals are a proven method of growing and sustaining a cybersecurity team. While the Chief Information Security Officer (CISO) is still an evolving role in the UK, the need for such a role is increasingly evident. An executive-level manager who directs strategy, operations and budget for the protection of enterprise information is crucial to the success of an organisation's cybersecurity programme.

PROCESS

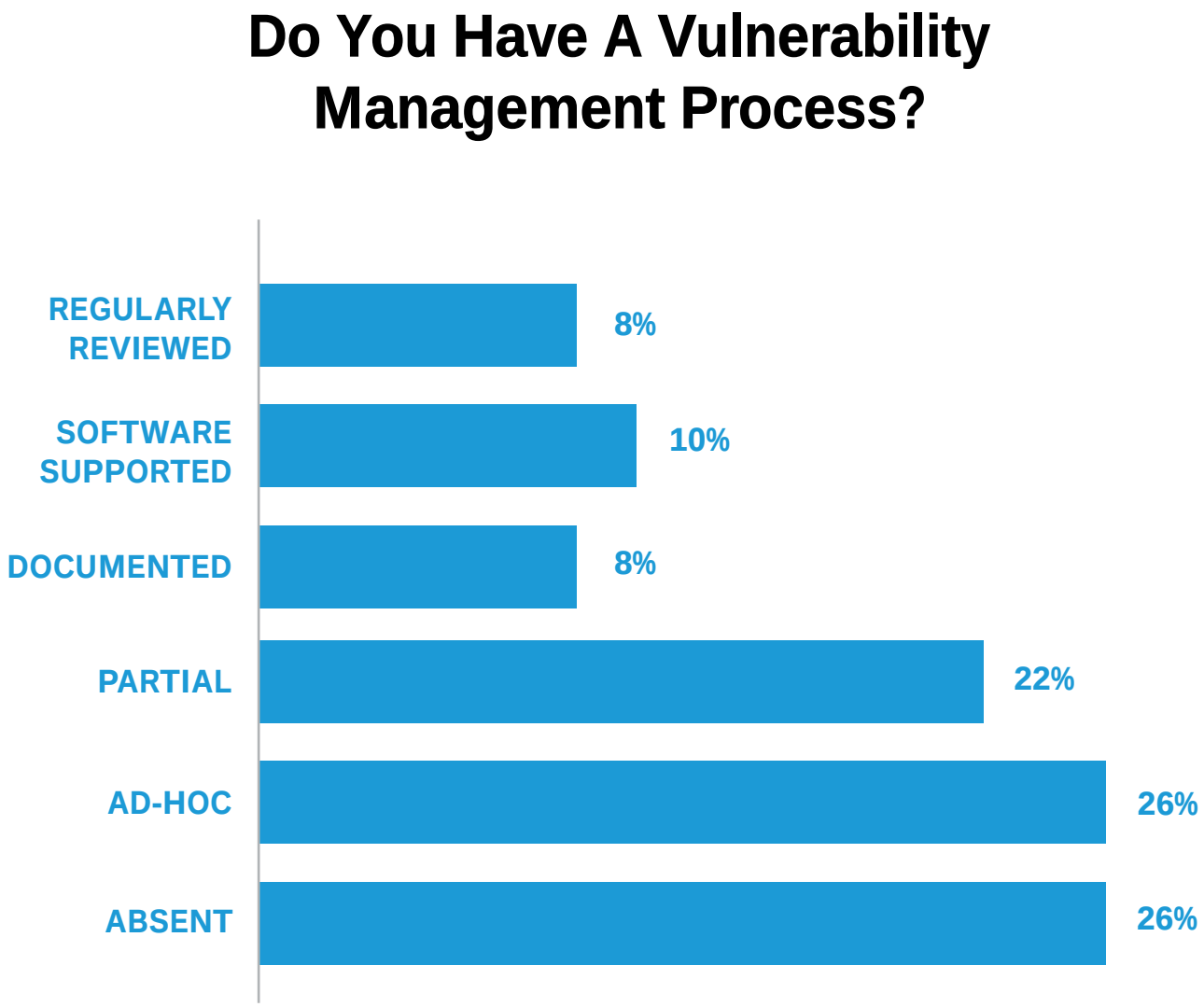
PROCESS OVERVIEW

After carefully analysing the data from the process element we can already determine a few basics points. We may not realise it, but, even within processes, we can speak of preventive, detective and response elements. For example, change management is a clear preventative process, while incident response could be classified as responsive. But what of detective processes such as security monitoring, vulnerability management and processes around security awareness? And how well do each of these processes perform across organisations?

PROCESS CHALLENGES

How do organisations score with their detection capabilities? Let's start with a look at vulnerability management: a defined process which identifies weaknesses and threats that could have a negative impact on the organisation.

Data shows that only 10% of organisations use technology to support the vulnerability management process. And - staggeringly - only 8% regularly review it. That means that, at best, 82% of organisations have a vulnerability management process on paper only, and - at worst - 82% of organisations have nothing at all. Either way, this is worrying and leaves the vast majority of organisations vulnerable.



When we look at processes to ensure adequate skill levels, it is clear that organisations find it much harder than expected to recruit, train, and retain personnel with the necessary skillsets - particularly personnel with cybersecurity education and experience. When we consider this alongside the varying passive defence technology that organisations implement to protect their assets, it is questionable whether organisations really possess the expertise they need to maintain their desired security posture. Organisations should identify what resources they have, and be confident that they have an adequate backup strategy should they need to recover from a major security incident.

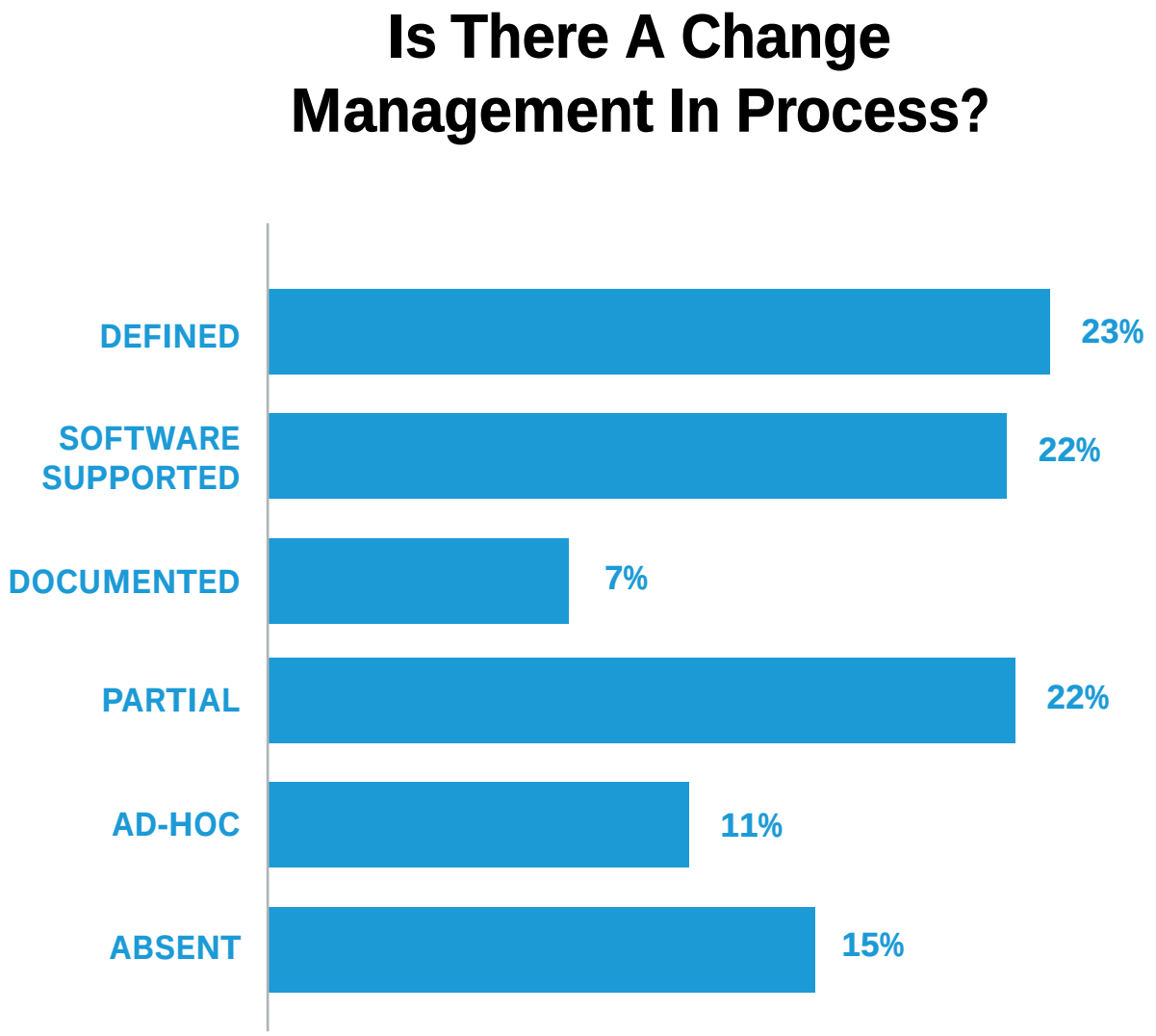
The assessment data shows that 85% of organisations do not have this element of their cybersecurity programme sufficiently covered.

Is this a surprise, or a case of predictable prioritisation? Ensuring cybersecurity teams possess just the right amount of resource is a real challenge – a challenge which is made substantially harder by the need to align the knowledge base of that resource with the pace of cybersecurity change.

Controlling the cybersecurity skills life cycle also includes personnel vetting (such as background security checks) and assigning risk ratings to positions with access to mission-critical systems and applications. An example of this is system administrators whose role requires the ability to change configuration settings, create new accounts, and change passwords on critical systems. Such individuals should be given a higher risk rating, and specific measures should be taken to minimise any risk that they may harm services, either accidentally or maliciously.

PROCESS STRENGTHS

The data shows change management as the 'strongest performing' element of process. Despite change management being one of the IT fundamentals, only 22% of all organisations assessed supported change management with software, and only 23% regularly reviewed their change management processes.



55% of the organisations assessed could therefore improve change management maturity. This would play a significant role in reducing the risks that can – and often do - lead to business disruption, misconfigurations and security incidents.

PROCESS INSIGHT

Building effective security processes is essential to improving an organisations maturity. For those organisations aspiring to establish and maintain documented processes, this opportunity is best leveraged during IT project delivery.

As an example, organisations often establish projects to deliver improvements to technology (such as firewalls), yet fail to identify and document (process map) requirements for maintaining this technology in line with security best practices. Process mapping prevents technology from falling into disrepair while driving other elements of the security programme. Building on the firewall example further, organisations should consider a process for the creation of new rules and the removal of old ones, along with a periodic review to ensure that unused rules, risky-protocols and overly permissive rules are regularly removed or reviewed.

TECHNOLOGY

TECHNOLOGY OVERVIEW

Today, the technology infrastructure involved in securing the enterprise has become incidental in the industry-wide conversation around people, process and technology.

For example, it is now unfashionable to talk about firewalls, switches and intrusion prevention systems. Yet without a strong passive defence architecture, everything else which creates a well-managed, process driven security approach is meaningless.

Major developments over recent years in the use of artificial intelligence and machine learning is driving an industry-wide push toward behavioural analysis of users and traffic. This gives cybersecurity teams a holistic view of their perimeter and internal networks, as well as their overall security posture.

Software defined networks and security, together with virtualisation and cloud adoption, has changed the way technology is designed and implemented. However, firewalls, routers, switches, remote access systems and intrusion prevention appliances (virtual or physical) still need to be in place. Further, they need to be current, well-maintained, and proactively monitored and operated. Without these technology fundamentals, even with insight, process, visibility and analysis, it becomes impossible to achieve a secure environment. The development of “traditional” security technology has slowed as manufacturers’ priorities for research and development (R&D) investment changes. The days of having two new firewall appliances coming to market every month are long gone. Instead, what we are seeing today is security vendors refining and improving existing product ranges and, crucially, integrating them with newer approaches. Despite this, though the term “commodity” is widely used to describe plain old technology infrastructure, such infrastructure is no less relevant or critical.

Most modern firewalls, for example, are fast, reliable and easy to operate, with similar performance and functionality, regardless of manufacturer. This doesn’t mean, however, that vendor and model selection should receive any less attention than any other element of security development and provision

Organisations must also remember that even when security services are moved to the cloud, and onsite devices are relegated to performing largely connectivity duties, that they are still ultimately relying on security appliances – even though they can no longer see them.

There are many security challenges that cannot

be solved by technology alone anymore. Data leakage cannot be “fixed” with a box, and URL filtering will never be so accurate that user training is no longer required. However, all technology implemented should be as good as it can be, and act as the fundamental on which everything else is built. Cybersecurity leaders must research products in-depth, rather than relying on manufacturer claims, and must choose products against a set of criteria designed to ensure purchases are made inline with security strategy.

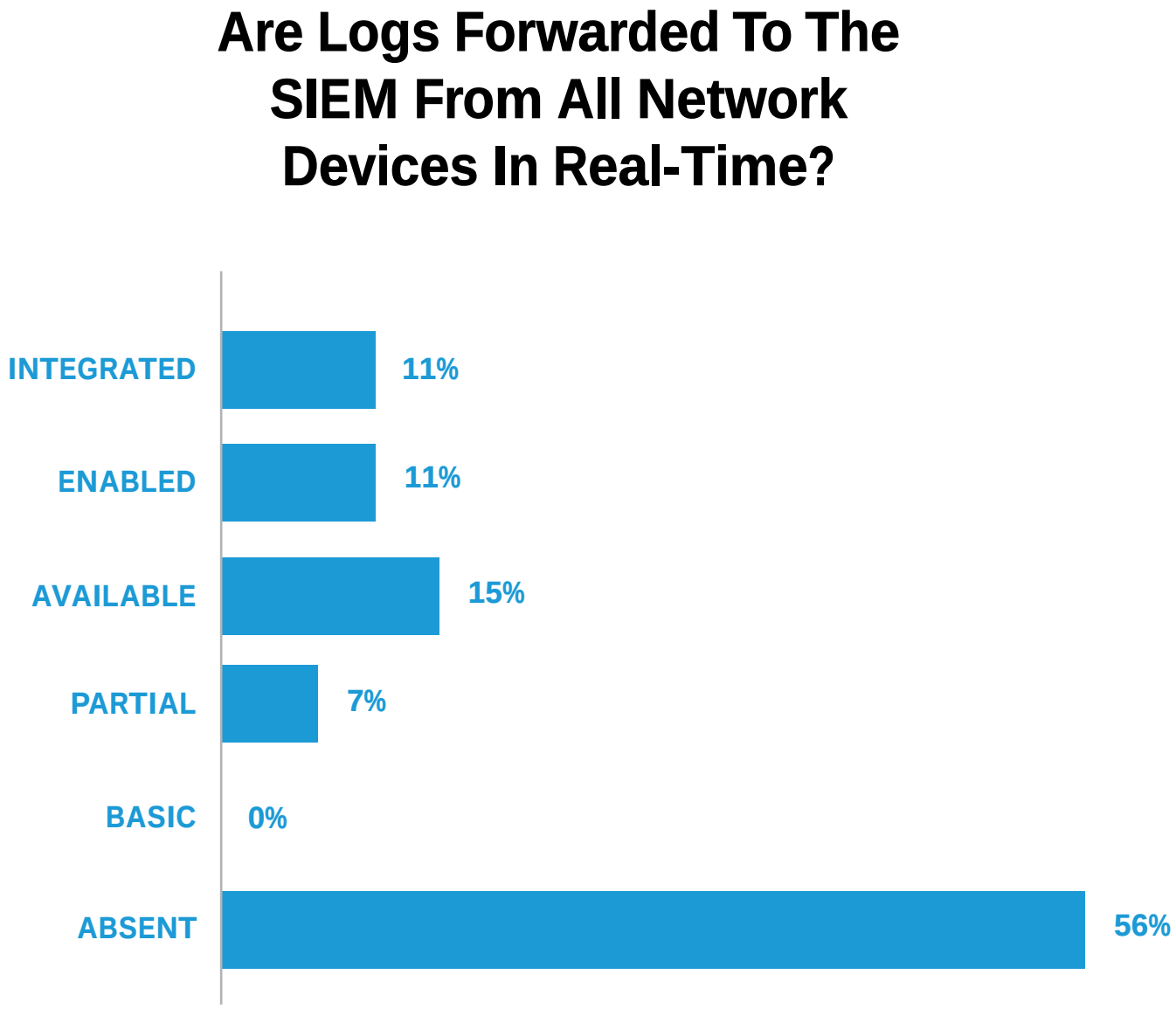
Security maturity is a journey, and that journey typically starts with technology. This point is underscored by the fact that many of the recent high-profile attacks have ultimately been tracked to an unpatched server, or a misconfigured router or firewall, representing a worrying tendency for organisations to take their eye off the technology ball. While it may be impossible to prevent all attacks through the use of technology, the implementation of best practice can ensure that it is much harder for attackers to be successful.

Research and experience shows that many organisations fail to fully utilise their existing investment in passive-defence security technology. Often, devices are bought and implemented to solve a specific requirement, and are rarely reviewed when that requirement has been met. The answer to a new security challenge may lie with an existing technology asset, such as a firewall that may also run application-aware IPS that could be an enforcement point for integrating endpoint protection. Security technology is a big investment - hence the importance of proactively operating and understanding it.

TECHNOLOGY CHALLENGES

SIEM & MONITORING

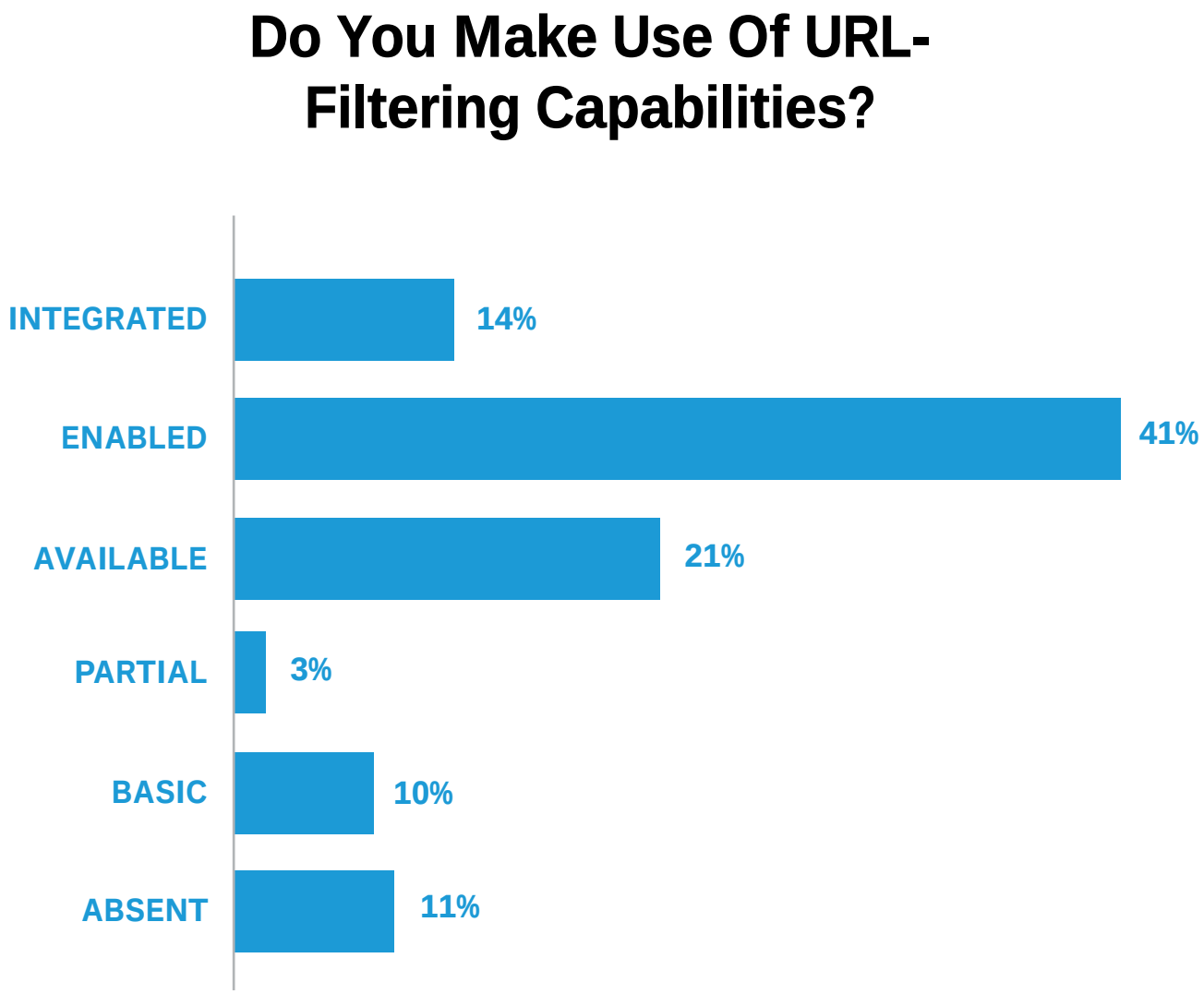
The data reveals that only 11% of organisations have deployed a fully mature, SIEM based infrastructure monitoring system, while more than 55% have no capability in this area whatsoever. This means that events and notifications from the myriad sources on the network are either not being correlated with other events in any way, or are being completely discarded.



It is true that SIEM solutions have these days become a little “old hat”. However, if organisations are not even collecting data, there can be no hope of implementing a process to analyse it. The challenge of SIEM systems has always been managing the data and making it meaningful, but the willingness to invest in the relevant people and processes can only makes sense with the fundamentals in place. Teams and processes will fail if they don’t have the visibility they need. Organisations should collect everything, rather than nothing, and put processes in place as part of a maturity journey, working with the data as it becomes viable. Remediation and root cause analysis, not to mention post-breach forensic investigation, is impossible when relying on manual correlation of data from multiple enterprise management tools - hence the need for reliable real-time and historic data.

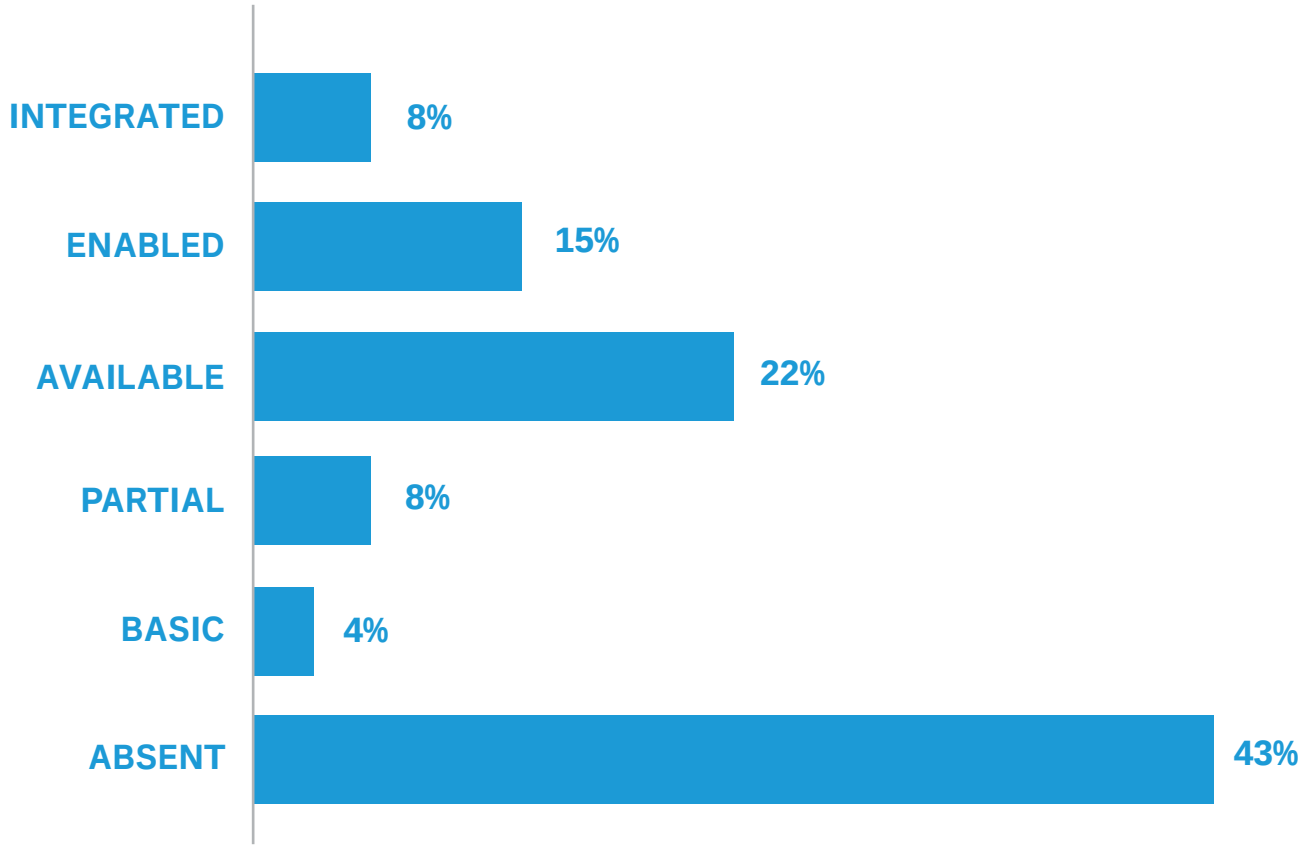
MALWARE PREVENTION

Many system outages and data breaches in recent years can be traced to malware entering the network and infecting endpoints. Much of this malware passes through perimeter security in email attachments or encrypted URLs. There are three places where technical solutions have an opportunity to help protect against these types of attack: at the perimeter, at the application (mail or proxy) and at the endpoint. The data shows that there is no consistency of approach to this challenge. While over 55% of organisations have URL filtering systems in place at a mature level, only 22% have protection against “zero day” malware. This is a missed opportunity to leverage existing technology investments and secure one of the most common modes of entry for malware by inspecting active content loaded by web users.



URL filtering is often implemented as a business tool for HR departments, yet it is also a powerful security touch point. The data shows that 51% of organisations have either limited or no capability to inspect SSL/TLS encrypted web traffic entering or leaving their network. It is clear that organisations are missing opportunities at the application and perimeter to greatly reduce the likelihood of malware entering their networks via users' web browsers.

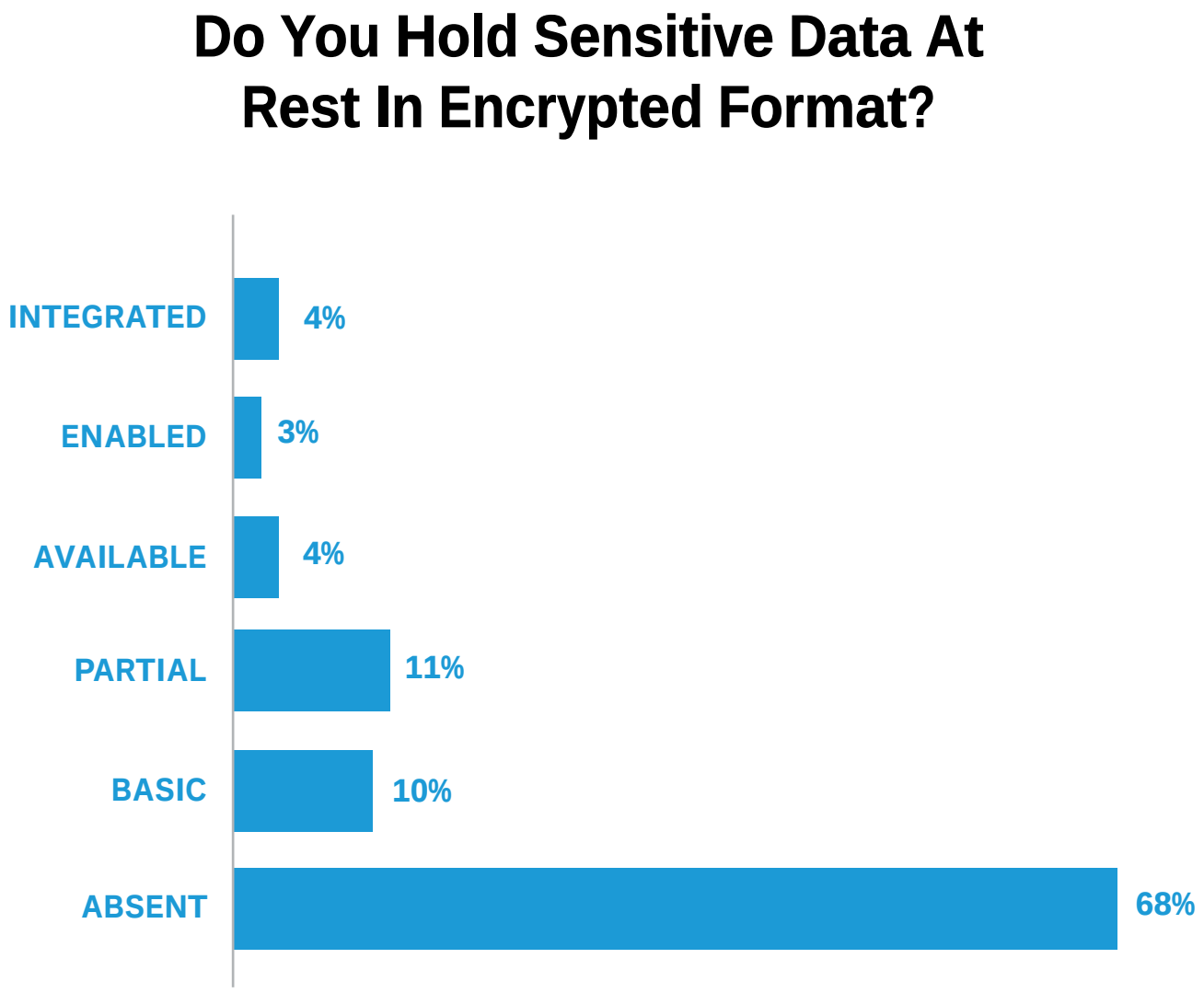
Do You Have The Capability To Inspect Encrypted Traffic?



"Zero day" malware protection remains difficult to manage. No system is entirely secure and all measures can, at least theoretically, be defeated. Endpoint and gateway systems which rely on signatures and heuristics to identify malware are particularly unsuited to identifying new threats or threats which are exploiting a window of opportunity between the release of the malware and the creation of a signature. The need to have a layered approach to security technology, and a holistic, correlated view of its behaviour and status is never starker than when dealing with zero day threats. If well-implemented and managed security technology exists at the perimeter, as well as at the application and the endpoint, then our chances of catching malware of any kind are greatly enhanced. Only one method of protection needs to identify the threat for it to be mitigated or eliminated.

DATA LOSS PREVENTION

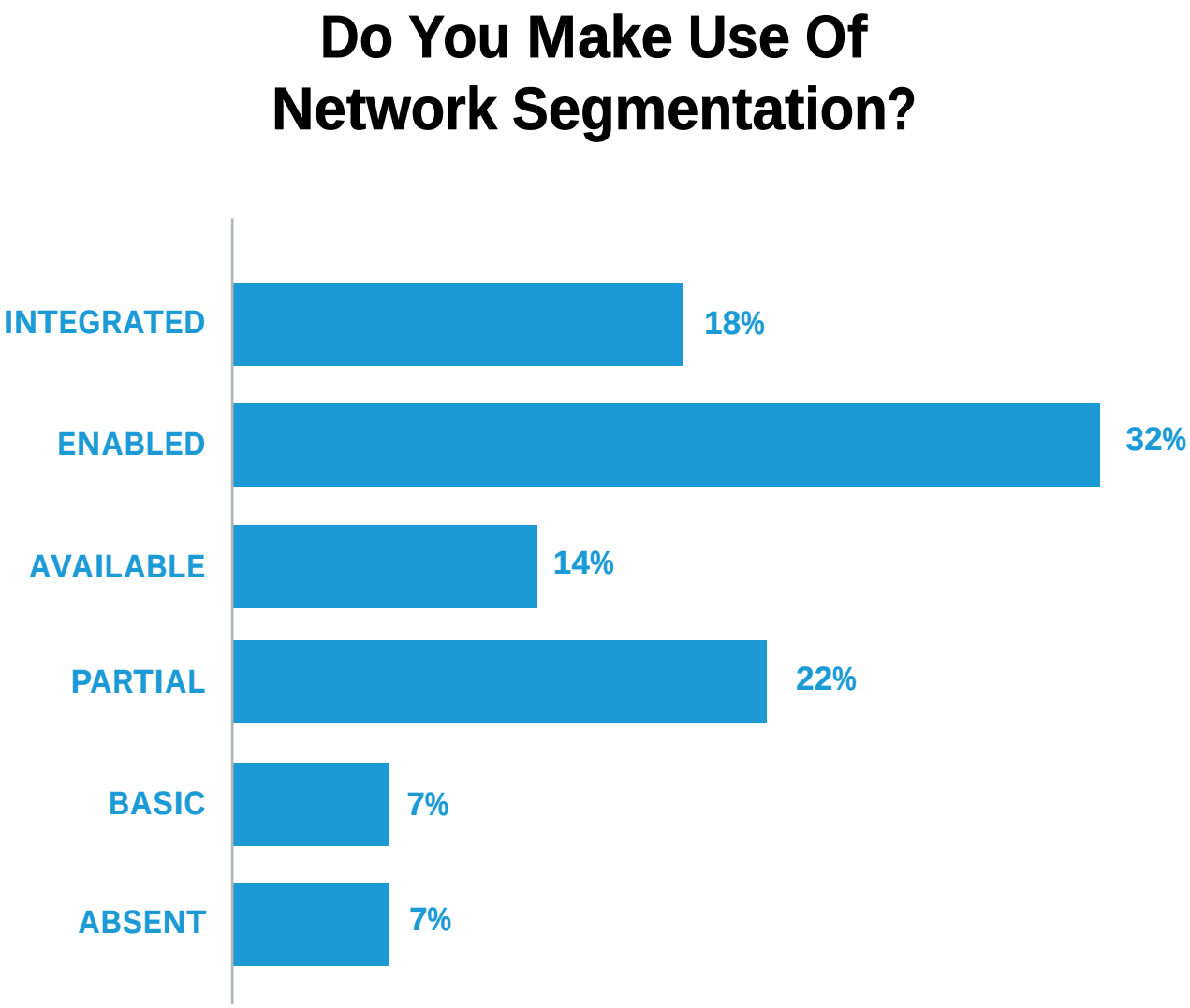
One of the most concerning results in the data shows that as many as 68% of organisations do not encrypt sensitive data, despite the fact that access to this capability is now widely available.



Given that one of the biggest concerns organisations have is the protection of intellectual property or regulated customer data, this is an incredible statistic. Encryption at rest is a great example of a challenge which can often be solved through *in situ* technology. Furthermore, any investment in technology for the purpose of protecting confidential data (which, according to the data, applies at varying levels of maturity to nearly 60% of organisations), is surely wasted if the data itself is not encrypted.

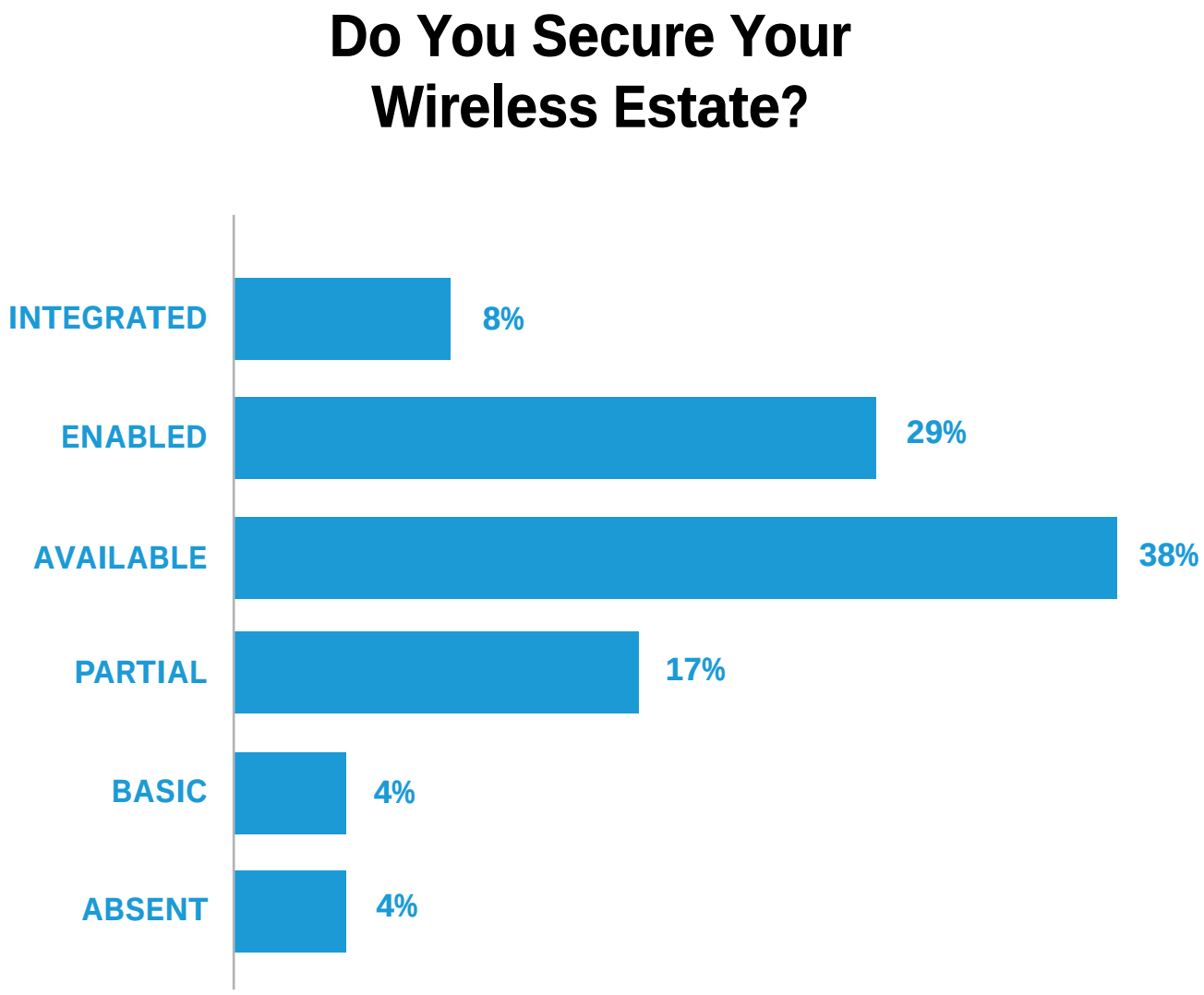
TECHNOLOGY STRENGTHS

Over 85% of us maintain segmented networks, a long-standing rule of network design best practise.



This is likely to be because traffic control and broadcast management has driven the adoption of sensibly-sized and role-related VLANs for many years, with the added benefit of controlling malware outbreaks. An inherent virtue of VLANs is that they provide multiple control points at which organisations can apply policy, or prevent the spread of malicious software.

When it comes to securing wireless networks, more than 88% of organisations have mature models in place – something which has been critical in the support of BYOD, and guest and mobile working.



Finally, organisations still keep physical data under lock and key, with the vast majority of servers housed in secure areas with the appropriate physical access controls.

TECHNOLOGY INSIGHT

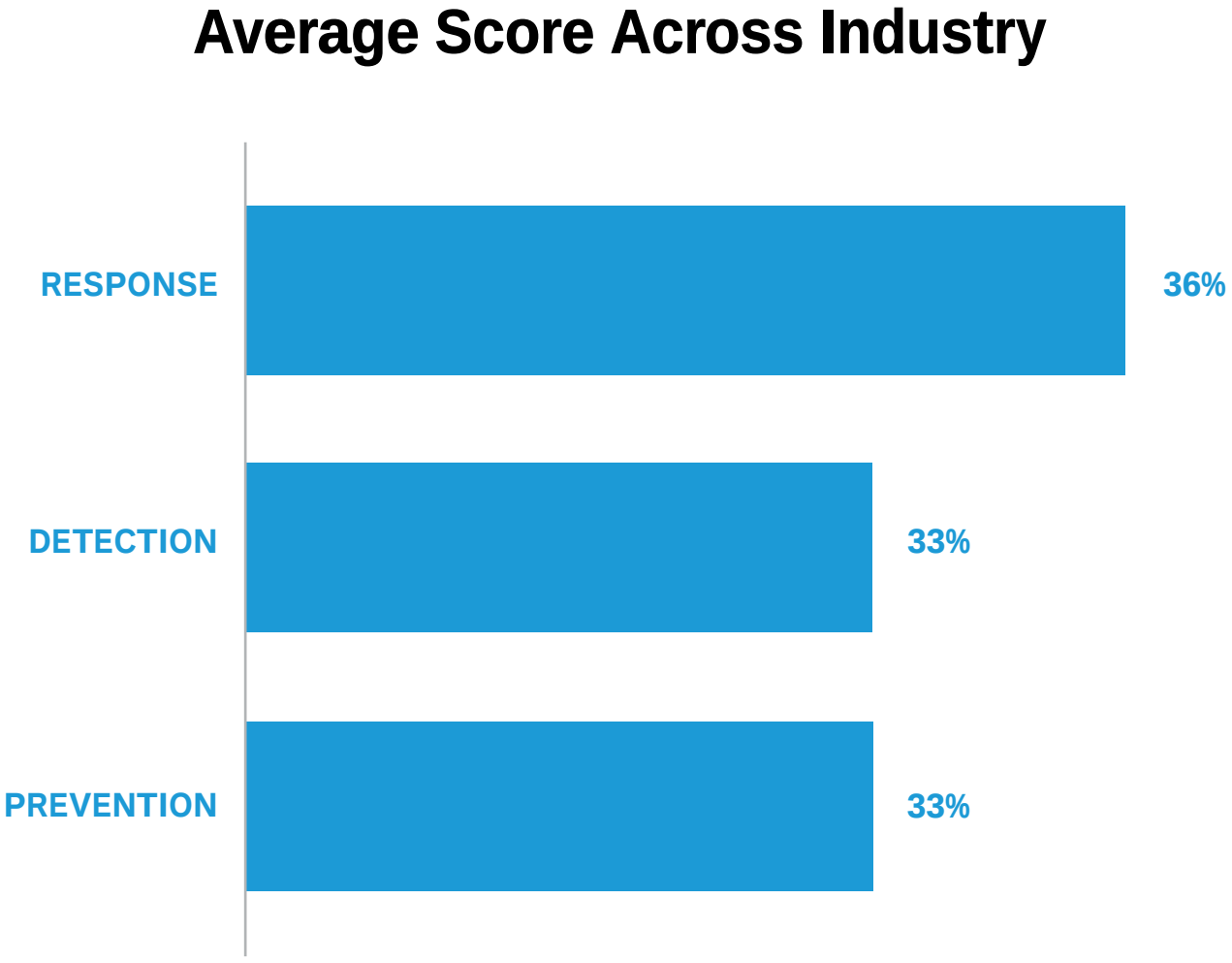
In conclusion, the picture is one of slow adoption. If we look at cybersecurity strengths (networking design and operation, URL filtering, wireless security) and weaknesses (zero day threat prevention, encryption and data loss prevention), this shows a clear *"old world vs new world"* divide. Whilst security maturity is a journey, and takes time, security leaders are taking too long and, as a result, missing opportunities to improve the chances of preventing breaches through technology that already exists in the organisation.

Employers, holders and processors of data need to become more agile, more aware of the challenges and more cognizant of the speed at which malware authors and hackers develop. There is an abundance of "low hanging fruit" for malicious actors, whether via social engineering of poorly-trained users, slipping attachments past perimeter gateways or simply not having to even bother to decrypt stolen data. These issues must be addressed quickly. And many big steps forward are simple to take. After all, paradoxically, what is easiest for a hacker to steal is often that which is easiest to protect. A well configured and monitored technology-context environment provides a good starting point to any security strategy, and is relatively easy to put in place.

PREVENTION DETECTION & RESPONSE

INTRODUCTION

Prevention, Detection and Response have long been the principal actions that define a successful cybersecurity programme. If proper attention is paid to each, an organisation can establish capabilities that safely enable business outcomes.



For many years, organisations focused on prevention, and rightly so. However, an acceptance of “when not if” is still not palatable to most organisations, which is why cybersecurity strategies have traditionally failed to include elements of detection and response. Given this, it is perhaps surprising that the most mature action which surfaced from the data is response.

Despite this, we see an average maturity score of 33%. Why should this be the case? Are organisations investing in technology to solve issues that the out-going technology could solve, but still failing to identify the real issue? Maximising the value of any investment should be a priority for the project sponsor - are they not measured on this crucial metric, or is the issue papered over?

One real surprise in our data is that detection is hiding among prevention and response in the “average score across industry chart”. Again, drawing parallels with response, is this the use of averages? We explore this further and demonstrate that those organisations which have nailed detection have truly nailed it. Conversely, a large proportion of organisations have yet to think about it!

PREVENTION

PREVENTION OVERVIEW

It is an often repeated mantra that all organisations will suffer a breach or data loss at some point, even if they haven't already done so. The ubiquitous reliance on data to run businesses, and the ever-increasing value of that data, will inevitably mean that risks are only ever going to increase. This doesn't necessarily mean that attacks are becoming more sophisticated. For every well-funded or state sponsored targeted attack, there are millions of speculative "drive-by" attacks, using phishing techniques and clumsy social engineering methods. The technology and methodology behind such attacks have barely changed for a decade.

It could be assumed, therefore, that mature prevention technologies should be effective at blocking the vast majority of common attacks. And, for the most part, they are. However, the drive to make sure that websites use strong encryption has meant that, over time, a vast amount of information-rich data has become invisible to traditional detection technologies. Encryption of traffic in flight and the adoption of TLS by the vast majority of web service providers is a very good thing, but it has certainly limited the effectiveness of perimeter inspection by defenses such as firewalls, IPS and even "next-gen" behavioural analysis platforms.

SSL, of course, can be intercepted, decrypted, proxied and re-encrypted – "man in the middle" attacks can be instigated for the greater good and used to run pattern and signature matching systems, before re-encrypting and sending the data on its way. But this is, and always has been, far from ideal. End-to-end encryption techniques were never designed to support inspection of traffic en-route, authorised or otherwise, and the implementation can be not merely clumsy, but brings its own issues with certificate management.

Encryption is chief among several reasons why advanced, or "next-gen", endpoint technology has been developed, and why its adoption has been so rapid. To inspect everything as the user and their Operating System sees it, you need to be looking on the machine on which the code is operating, where the data and user actions can be seen without obfuscation.

As advanced Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) systems develop and merge into powerful insight and prevention systems, the visibility lost at the perimeter is regained. Even more powerful are the recent improvements in integrating EPP systems and more traditional devices at the perimeter – if an EPP tells a firewall to block some traffic, the firewall itself doesn't need to know why, or have any visibility of what it's blocking, and the rest of the estate can quickly be protected from a

threat which was previously passing, encrypted and undetected, through the network edge. CASB (Cloud Access Security Brokers) are also becoming a much more attractive option, as the adoption of SaaS and online storage increase exponentially. CASBs provide visibility into the online activity of users, allow tracking of data and provide the ability to re-apply permissions and access controls that may have been lost during a move to a cloud offering. In both cases, data can be inspected with authorised credentials, so that data can be viewed during the normal process of encryption and decryption, without having to clumsily break into the traffic stream, or come up with a solution which doesn't meet the original RFCs. Where, then, should you be investing your prevention budget? And is it still worth the ROI? The short answer is "yes". Just because perimeter and traditional prevention technologies may be less effective at new and emerging threats, they're no less vital for protection against the vast majority (99% or more) of well-known and easily detected attacks that organisations are likely to suffer from. They are also crucial as enforcement points: if a firewall can't "see" the relevant data then the option exists to implement something which can, and get it to tell the firewall what to do.

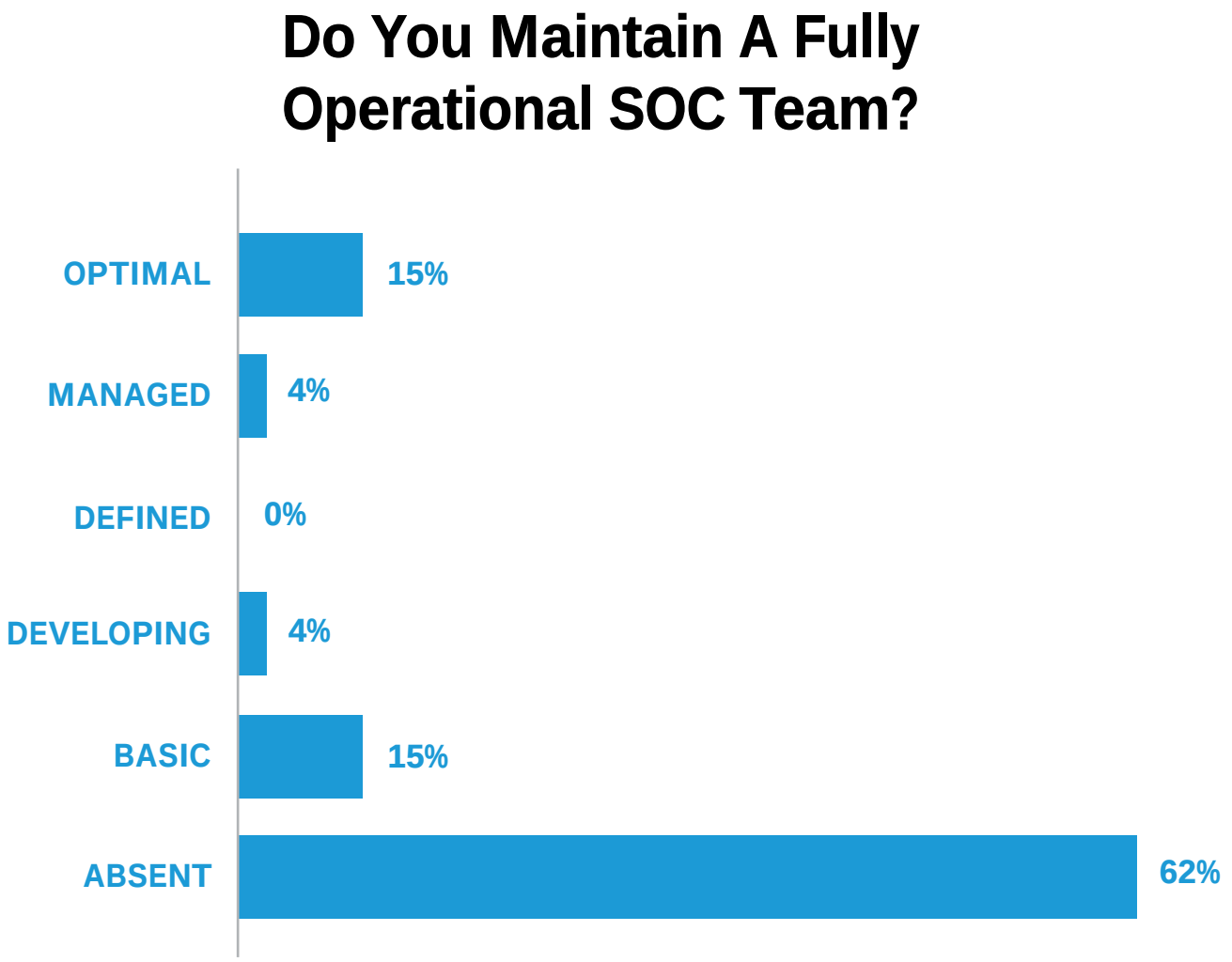
Lastly, the more that is prevented, the less security teams have to detect and respond to. And prevention, if not actually better than cure, is certainly far less expensive.

PREVENTION CHALLENGES

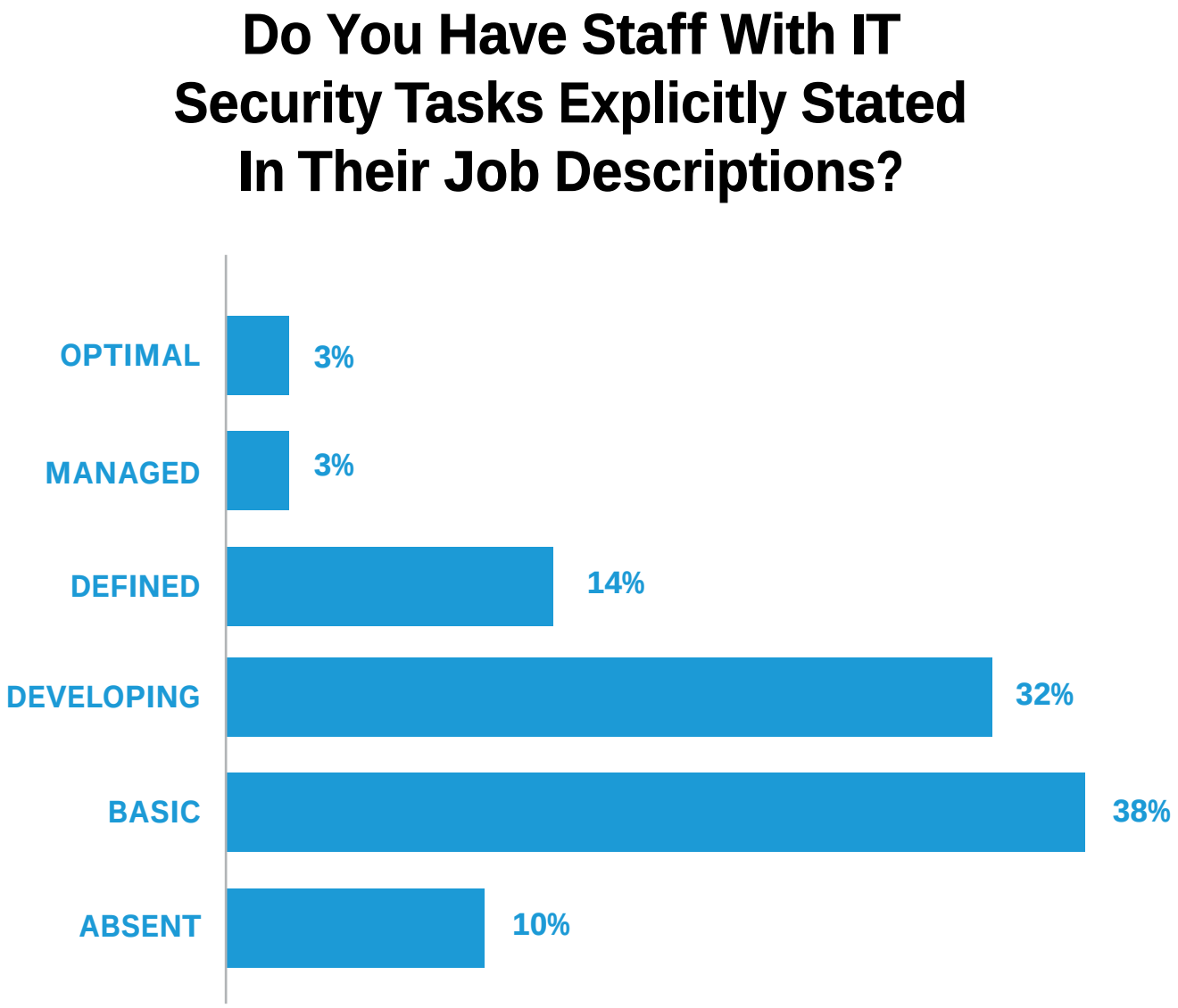
PREVENTION & PROACTIVE MANAGEMENT

Security Operations teams are more commonly associated with detection and response, but without a continuous cycle of feedback, and a clear view of what they are *not* preventing, it's impossible to manage effective prevention systems or policies. Indeed, there is a good argument to be made that organisations shouldn't even care about what they are preventing, as - by definition - it didn't happen, so why waste time collecting logs and running reports about what the system has stopped? Prevention technologies need constant maintenance and tuning, aligned with an awareness of the background threat level defined in the context of the business. In short, staff should be trained, and specialists in security should supervise them.

According to the data, nearly 63% of organisations do not have trained security teams in place, and are therefore either relying on traditional IT infrastructure management teams and processes, or are not proactively managing them at all.



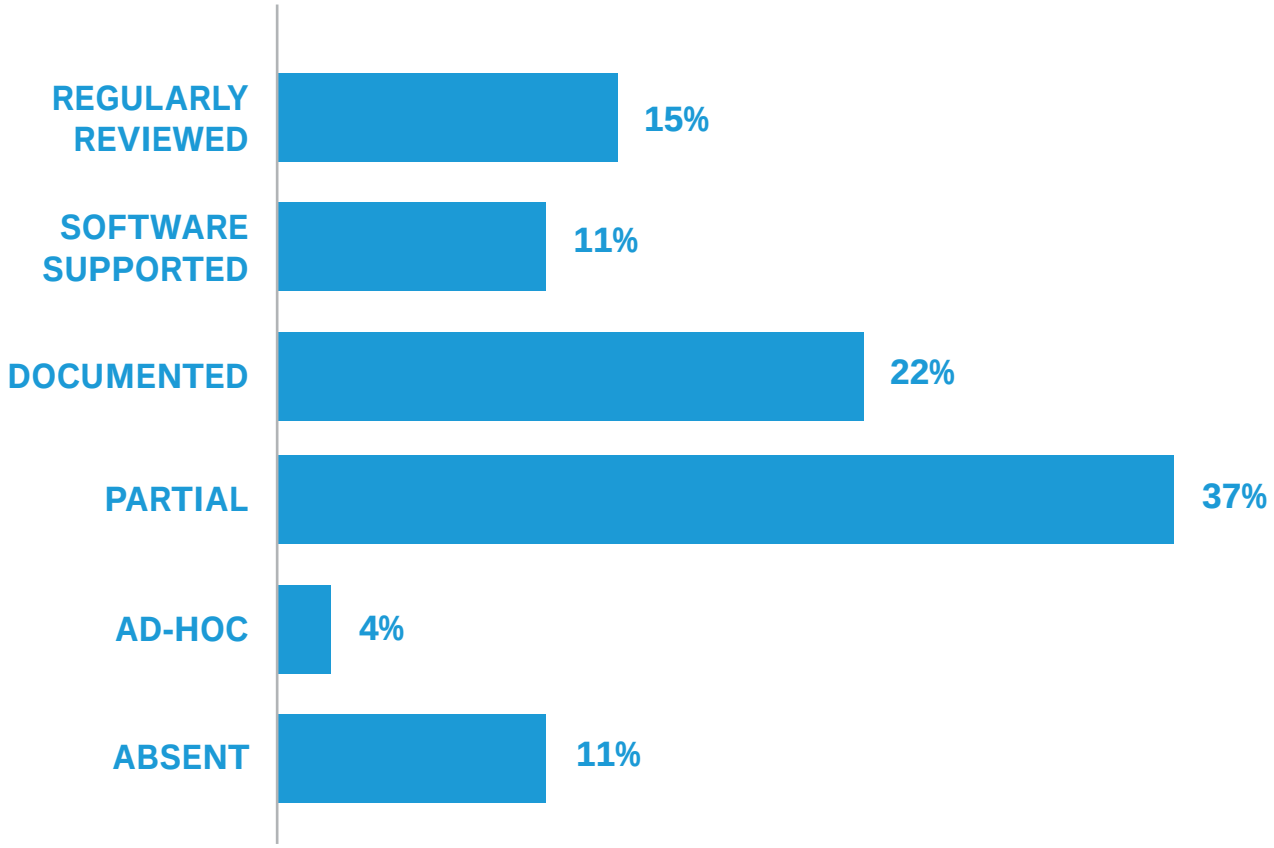
48% do not have access to staff with relevant cybersecurity skills appropriate to their business size and type.



PROCESS & PROCEDURE

The investments which have the largest impact on prevention of security breaches are those which implement or improve processes and procedures. For example, over 50% of organisations do not have a mature patch management system in place.

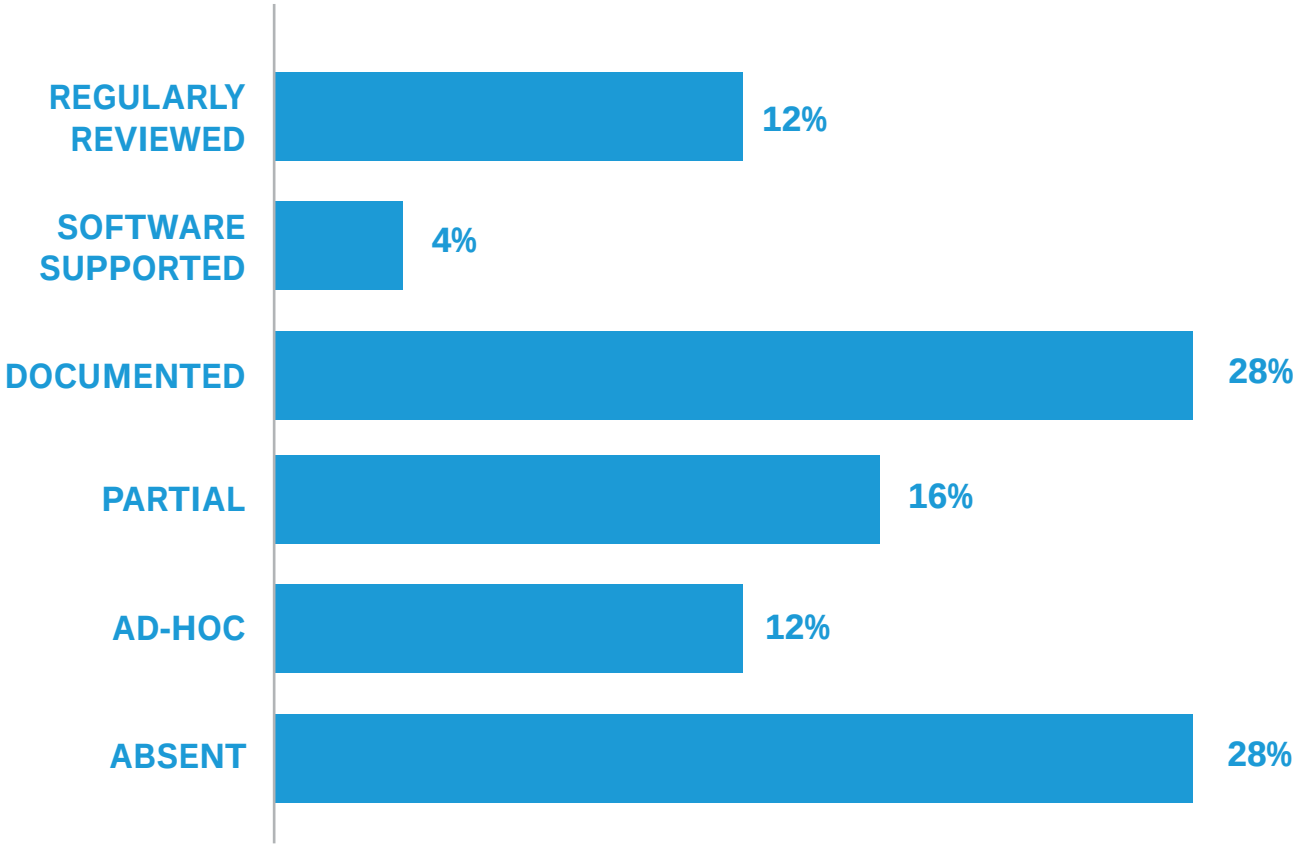
Is There A Patch Management Process In Place?



Patch management is not simple – there are production outages to negotiate, and regression tests to carry out, on dozens, or even hundreds, of systems. But this observation must be balanced against the fact that many successful data thefts are prevented by patches which are over a year old. Patch management is an ideal subject for a risk-based conversation with senior management – security teams need to ensure that business decision makers are aware in commercial terms just how important it is to be current, even if that means some production down-time.

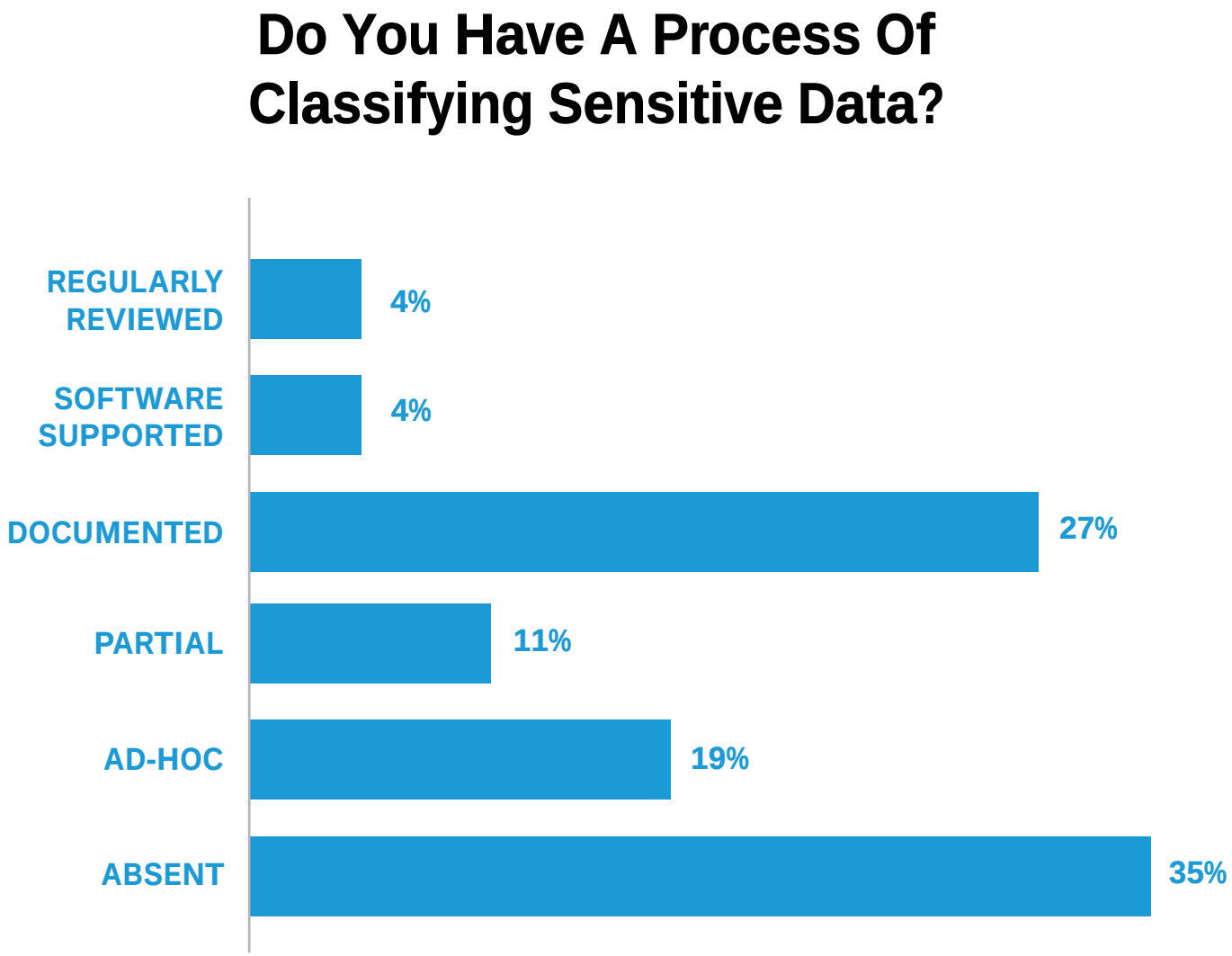
Remarkably, nearly 15% of respondents did not have a change management process of any kind in place, and 40% have either little or no involvement with IT projects from a security perspective.

Is Security Considered Before Commencing IT Projects?



Many breaches could be prevented by treating security as inherent to all IT projects. Attempting to retrofit security once a product or solution has gone live is next to impossible to do well. Project sponsors must realise that security is not something which is done to the project, or applied retrospectively. Instead, it is something that needs to be treated as an integral part of the project from the outset.

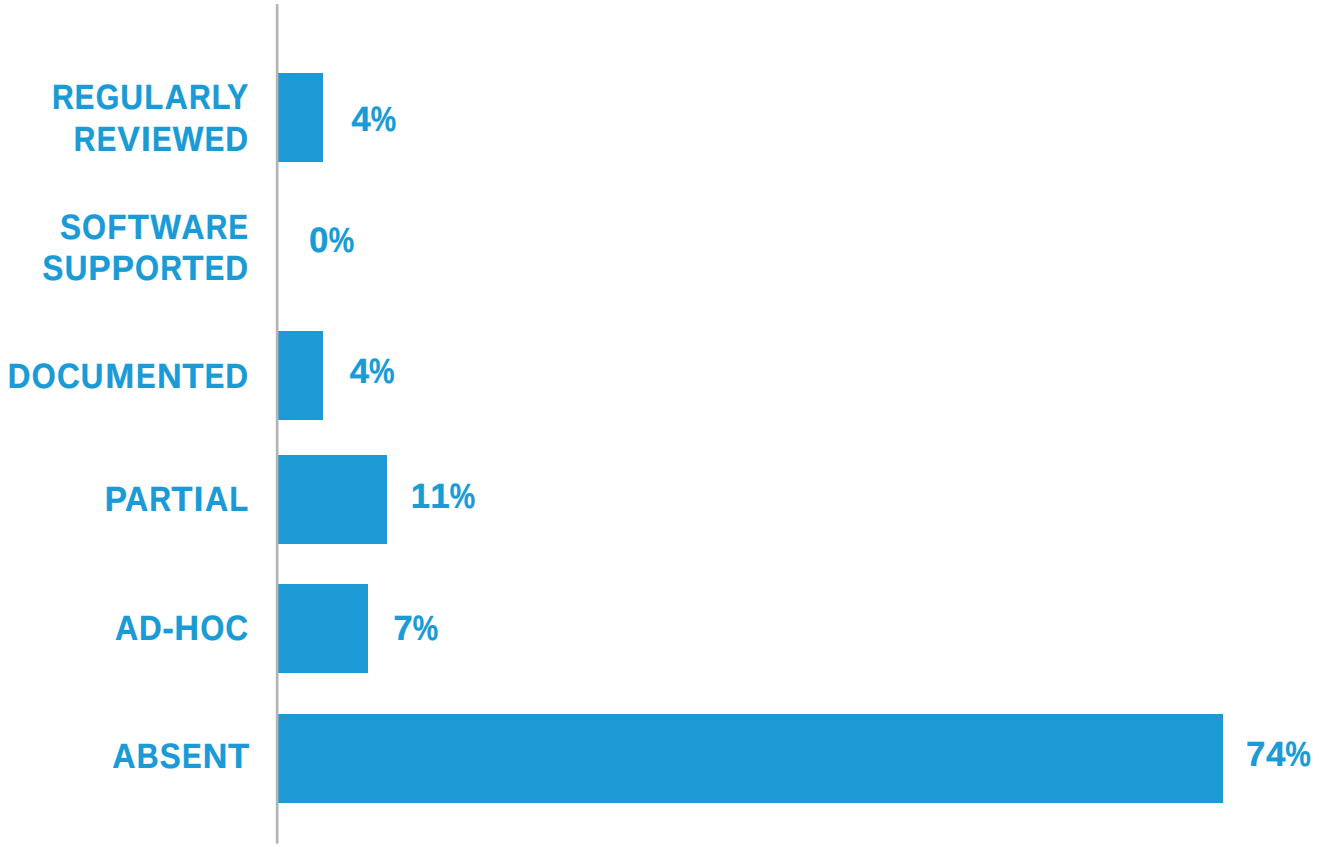
Finally, the data shows that over 34% of organisations have no data classification in place. This is crucial when trying to understand where the “crown jewels” are, and therefore where to focus budget and resources when implementing security. It is also impossible to quantify, post-breach, what has been lost and how important this loss is, if there is no idea of the classification of the lost data. There is a myth that classification is very difficult to implement – and it can be – but it doesn’t have to be. By starting with a definition of which classes apply to your business (and this could be as simple as “confidential” and “other”), and mandating that staff write it on the cover page of their documents, you will yield good results for little investment.



PROCESS & PROCEDURE

Many businesses have been on the internet for a very long time. As a result, there are often production webservers, remote access systems, email and DNS services, developer test machines and dynamic marketing micro-sites, which may or may not be monitored or maintained. In many cases these systems have been forgotten about as new systems are implemented and people move on to other jobs. And this is before we take into account any unauthorised use of the brand or content on third party apps, websites or link referrers – all of which can have a significant reputational impact. There have been many high-profile cases of data theft, where the attacker discovered and used a forgotten, unpatched and unmonitored server to gain a foothold on the network and establish trust with other production devices. The data shows that some 74% of organisations have no visibility of their digital footprint – which is all the more worrying, given the fact that 80% of organisations have assets (unknown to their security teams) reachable from the internet.

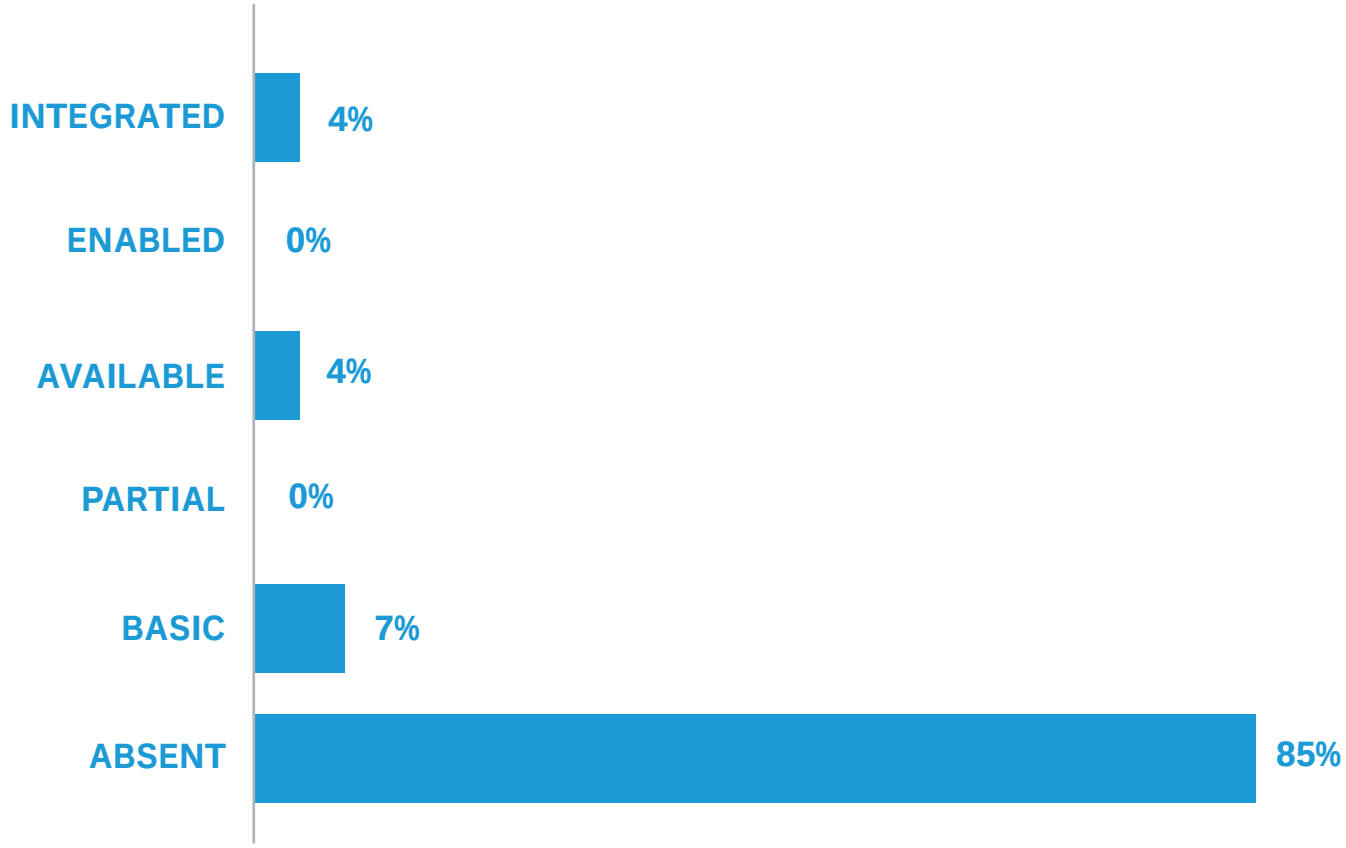
Do You Have Visibility Of Your Digital Footprint?



DATA ACCESS VISIBILITY

Data shows that nearly 50% of organisations do not monitor activity on standard user accounts, either via an automated tool or by routine alerts from operating system audit logs. Additionally, nearly 90% of organisations do not have any form of file integrity monitoring in place. Of course, these processes and systems are normally implemented separately, but taken together this reveals that many cybersecurity teams are not aware of what user accounts are doing, or whether data is moving around the internal network in an unusual way.

Is There A File Integrity Monotoring Tool Deployed For Critical Files?



This is important because, without proactive monitoring of user accounts and privileges, it is often the case that the first a security team will hear about a compromised account or internal data leak is when sensitive data appears on the internet - or, worse, in the press. Traditionally many users only come into contact with IT teams when something isn't working, and often the resolution is by necessity and design, as quick and simple as possible. The result is often that user accounts are created or re-created from templates (for example, a new user in the finance department will be modelled on someone else in the same department), and unusual file activity is treated as "odd", logged, remediated and forgotten about. Security teams tend not to look at day-to-day activity through a security lens, and this means they miss a significant opportunity to identify compromised accounts or other activities that constitute a risk.

One example often used is that of a disgruntled sales employee getting ready to hand in their notice and copying a customer database to an external drive before leaving. Security is all about detecting the abnormal, and processes and tools which recognise normal status make it a lot easier to notice when something unusual is happening.

PREVENTION STRENGTHS

When using the assessment data to analyse what cybersecurity teams are good at, a familiar pattern emerges. Many organisations have a mature process for maintaining secure firewall and router configurations, and they are good at choosing the right technology for perimeter networks and know how to assess them for effectiveness. Many organisations are also very good at vulnerability scanning and packet analysis.

These are all crucial elements of effective security and are not to be underestimated – their absence would be catastrophic – though the more data-centric activities are not done so well, if at all. Traditional technologies are well understood and well managed, but as the threat has moved on from malicious actors trying to gain shell access to our firewalls, to attacks based on malware or social engineering (which simply ignore all the traditional equipment), organisations have begun to lag behind.

PREVENTION INSIGHT

Security strategy must evolve with the threats. Organisations can never be one step ahead of the malicious actors, and even staying current is a challenge. But the aim of being just one half-step behind, and at least *aware* of developing trends and motivations, would put them among the most secure environments in the world. Getting there is a lot of work, but it can be done a little at a time. By starting with identification and classification of the most important data, for example, one could quickly move on to working out how to monitor its journey throughout the infrastructure, without having to attempt the impossible by applying dynamic classification to all data all of the time. Cybersecurity teams should prioritise by getting better at identifying and explaining risks to business stakeholders. Risks are no longer purely technical and so they shouldn't be quantified in that way. To some organisations the biggest risk will always be financial, while others value reputation or intellectual property more highly. Security teams should lead these conversations with the business in order to work out what to protect first.

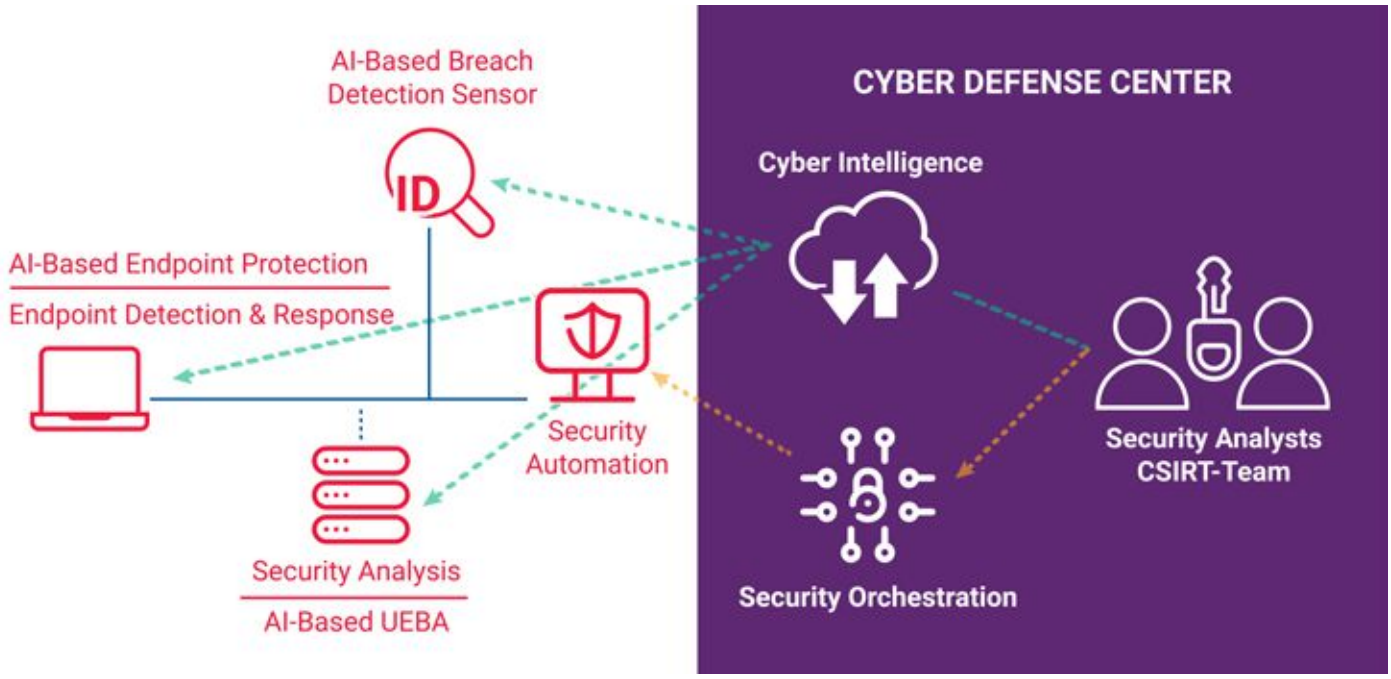
While technology is still a key part of prevention, the data shows that technology is becoming less and less important, especially at the perimeter. Hackers have learned that firewalls and IPS systems can be bypassed, which perhaps means that time and money should be reallocated towards better preventative measures, such as preventing malware spreading or a ransomware infection. These are just examples, of course, but the overall picture presents a need to be more dynamic. Security teams have the basics covered and do a good job with managing them. But, while the hackers have been largely beaten at the perimeter, they have moved on and security teams must move with them to the next battleground – the data.


MSA
MSA
MSA
MSA

DETECTION

DETECTION OVERVIEW

Detection is hard. If it wasn't, cybercriminals would not be as prolific and prominent as they are today. And prevention is even harder of course. But if an attack can't be prevented, it can probably still be detected and stopped. However just as organisations have given up and started to look at detection and response, a technology silver bullet is on the horizon.



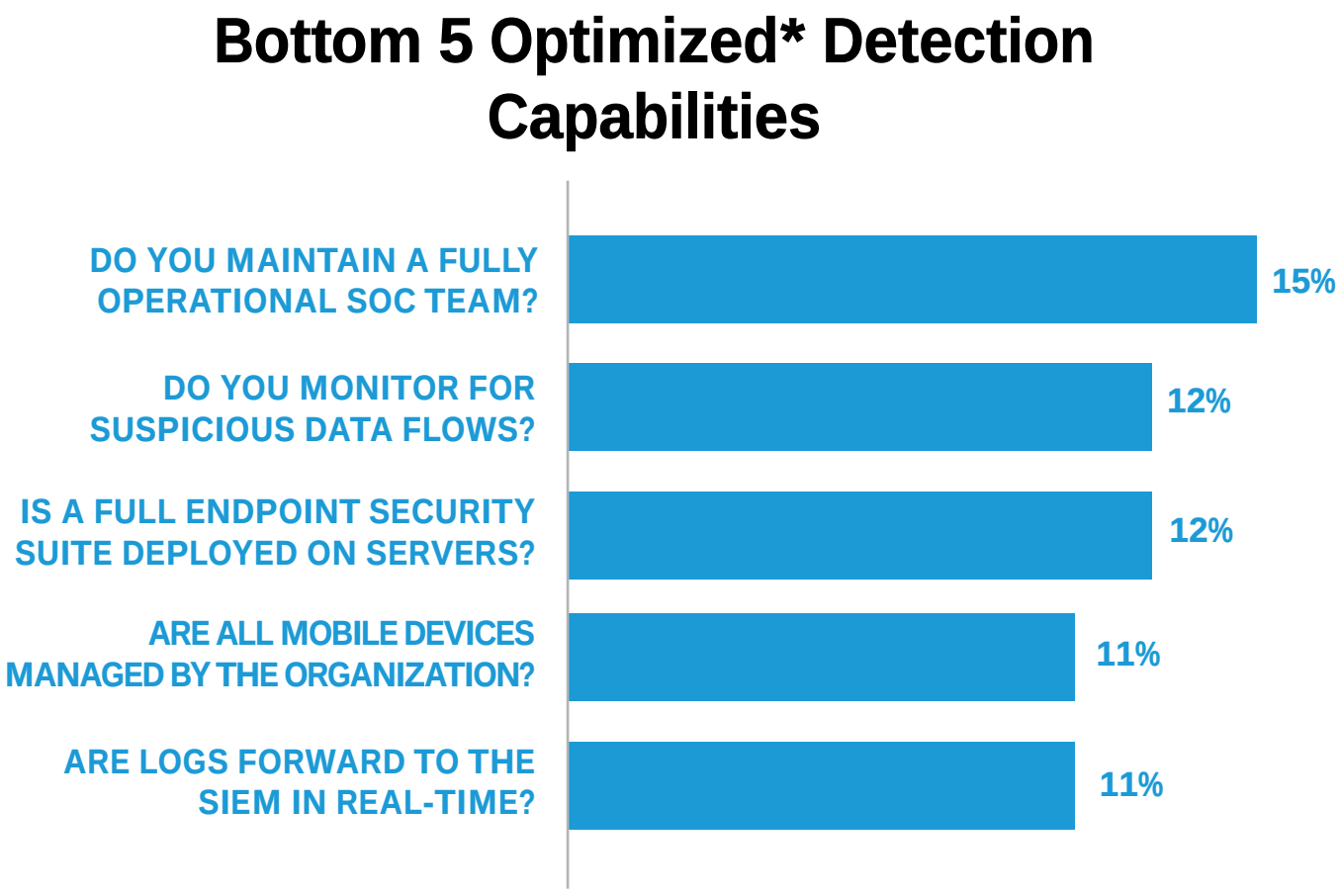
Artificial Intelligence and Machine Learning is dramatically changing prevention technology. Yet, more than ever, these technologies are driving the need for a better *Detection* capability. They find more threats, pose more questions and – therefore - require more analysis - as can be seen in the graphic above. While there is still very much a need for people and processes, technology is the catalyst for these functions, by increasing people and process efficiency. However, it cannot replace them just yet.

DETECTION CHALLENGES

From the data, the top 5 “capabilities completely absent” includes more advanced functions of security operations such as “absence of file integrity monitoring”, “absence of visibility of digital footprint” and “absence of deep packet analysis tool to conduct investigations”. If these elements are indeed absent, then maybe the organisations are just not there yet. Cybersecurity maturity is a journey after all. But – startlingly - some of the basics also show up in the top 5 challenges:

63% of organisations have zero capability for Operational Security when it comes to people. That’s nearly two-thirds, a truly worrying statistic.

55.5% of organisations are not collecting log data in real-time.



The highest state of maturity

What these things show is that organisations cannot look at individual elements of detection in isolation. This is where top level cybersecurity capabilities are focused. The Operational Security Management capability: *Establishing and maintaining activities and technologies to collect, analyse, alarm, present, and use operational and cybersecurity information, including status and summary information from the other capabilities, to form an operational security picture* - is the capability organisations find most challenging.

DETECTION STRENGTHS

Although Operational Security features in the top 5 of absent capabilities within an organisation, it is also the most 'optimised' of capabilities for detection. This is interesting, because it points to a significant gap between organisations doing it very well (optimised and those which are not doing it at all (absent).

When looking for Threat Hunters and Security Analysts, organisations should be aware that the best professionals are highly likely to be attracted by employers that can offer them more, such as a superior team of peers to work with and the prestige of working with a prestigious brand. A lucrative salary is, of course, also a powerful lure.

An analysis of the data for the top 5 mature detection capabilities for organisations with a minimum ("defined") level of maturity for that capability shows that *Securing and monitoring the wireless estate* comes in at number 1. This is a reassuring finding, as it implies that most companies recognise the inherent risk in wireless networks, and take appropriate steps to protect this historically vulnerable threat vector.

Top 5 Most Mature Detection Capabilities

Establishing a security policy comes in at number 2. This is a fundamental of cybersecurity, as without policy it is impossible to establish what is bad.

As far as the positions of third, fourth and fifth are concerned in this 'league of strengths', the data shows that only two-thirds of organisations are doing the relevant element well. This, of course, means that one third of organisations find these critical elements challenging.

DETECTION INSIGHT

Most cybersecurity Leaders recognise that finding, hiring, training and retaining good people are the principle challenges in delivering detection capabilities. This, coupled with the selection of state-of-the-art technology, and building robust processes, means that establishing in-house detection capabilities can take over two years. A managed service however, could deliver step maturity in 3-4 months.

We should note that changing to a service architecture still demands that organisations retain experienced cybersecurity people. All the same, such a change will free up much needed resource to allow a focus on other aspects of the cybersecurity programme.

RESPONSE

RESPONSE OVERVIEW

The Response function is very closely linked to Detection, so findings will inevitably be related to those above. In fact, Response demands capabilities that are also part of the Detection function (e.g. maintaining a fully operational SOC team). After all, when developing detection capabilities, teams have to consider how to respond. Conversely, without detection, there is nothing really to respond to.

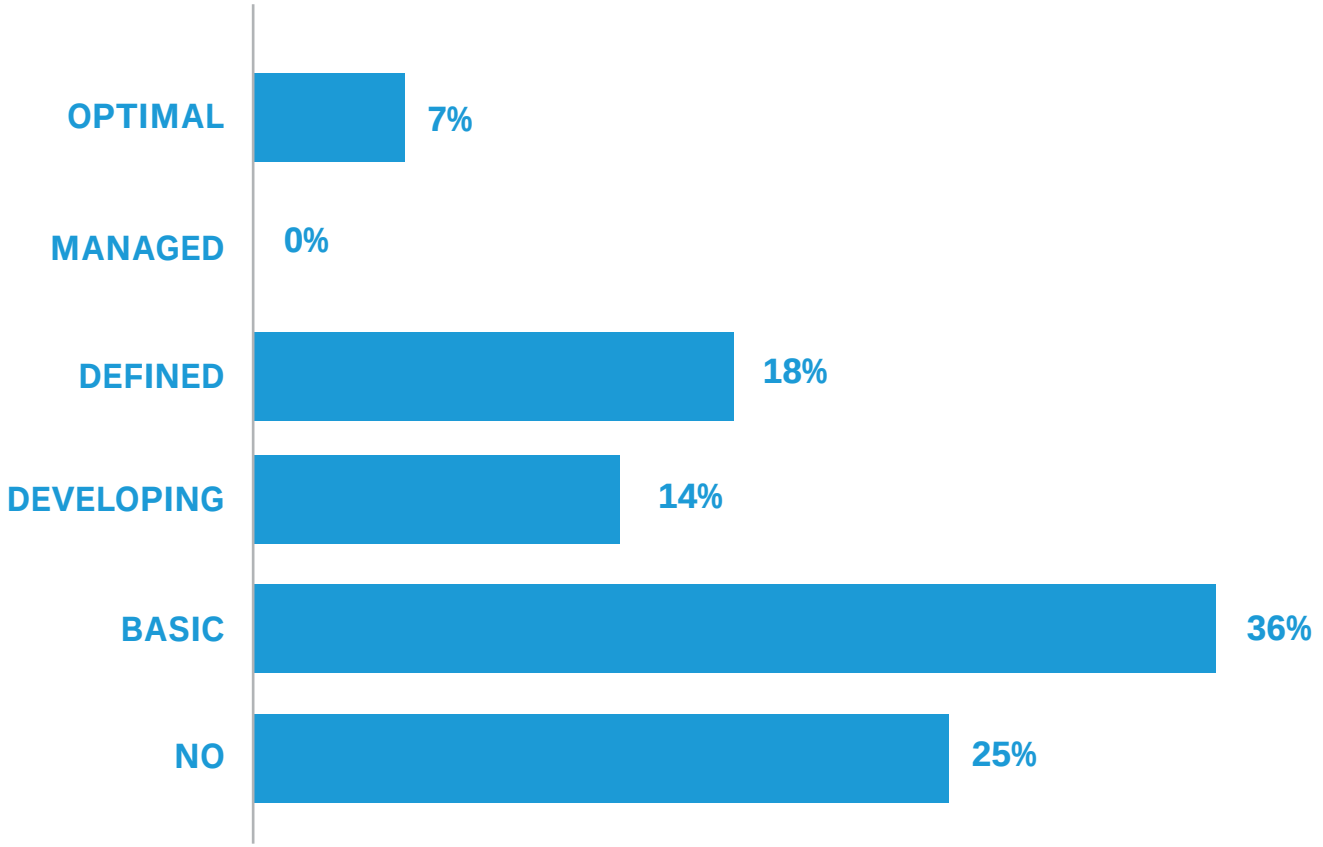
A fully-enabled Response function must be carefully planned, documented, executed and tested – indeed, Response testing is just as critical as business and service continuity tests. With ever-growing and variable methods of attacks on organisations, both large and small, there are many variables that drive response actions. Therefore, a dedicated Response capability is critical, and should be ready to manage the various methods of attack while remaining cognizant of the risks and required roles and responsibilities (for example, a crippling distributed denial of service (DDoS) attack is often used to masquerade data exfiltration). The Response function must then consider business impact, as well as legal and regulatory obligations, further maturing its relationship with risk management. This is often considered to be a more complex process than general incident management – it should really feature within crisis management.

RESPONSE CHALLENGES

Eight out of the top ten absent capabilities are related to Technology. One of these, related to Response only, is having “designated incident response staff”.

The data shows that over 60% of organisations have little or no dedicated incident response staff. But, even if an organisation uses managed services for detection and initial triage, some form of dedicated, or partially dedicated, incident response staff is critical to maintaining a response capability.

Do You Have Designated IT Incident Response Staff?



RESPONSE STRENGTHS

The top 5 optimised capabilities are dominated by *change management*, properly *segmented and managed networks* and a good patch management process. It is also essential that an Operational Security team is present and optimised.

Let us look again (as in detection), at the top 5 capabilities being conducted at a reasonable and defined standard or better.

Top 5 Most Mature Response Capabilities

This data shows us how ingrained incident response is, within these broader supporting capabilities.

However, several questions arise. For example, do those 75% who maintain a *secure wireless estate* have a process for responding to rogue threats detected through that process / technology? Does the overarching *security policy* include incident response? Is *network segmentation* used in the incident response process when conducting active response on identified endpoints or devices that are confirmed as rogue/compromised? And, does the *full endpoint security suite* include Endpoint Detection & Response capabilities? Our data does not answer these questions.

The chances are that, because none of these top 5 are specific to incident response in isolation, and because (as previously shown) over 60% of our dataset have little or no dedicated incident response heads, then the answer to many of those questions could be no. It is only when looking at the core capability of *Event & Incident Response and Continuity of Operations*, and how all the different capabilities and supporting functions play into this, that we can realistically look at making improvements and embedding Response as a function.

RESPONSE INSIGHT

As with Detection, Response is lacking as a mature capability in many organisations, despite many years of trying to *prevent* as much as possible. This wasn't necessarily a wrong strategy – it's just that the whole industry has shifted. Now, though, it's critical that we recognise that shift and incorporate it into a broader strategy.

The recipe for success is similar to *Detection*: the resource, the technology, the processes are more aligned than in any other element. Many organisations offer retainer-based services, allowing them to call upon expert incident response teams when they pull the ripcord. This would imply that the detection capability, and in many respects, early incident response capabilities, are understood, implemented and are essential to leveraging such as service, when called for.

More and more organisations choose managed services for both detection and response.

FINAL THOUGHTS

The journey to maturity is different for every organisation, and the maturity of every organisation is at different stages. However, all organisations share a common fear - a breach in cybersecurity. There are few things more devastating than a data breach.

The reason for this is obvious. The resulting harm for affected individuals, such as those who have had their personal data stolen and used by cybercriminals, is felt for years and amounts to much more than just financial loss. But the practice of considering cyber risk outcomes as more than just financial is still in its infancy. We can quite reasonably ask the question: do organisations even consider harm caused by a data breach, or do they only calculate the resulting losses as financial? Oxford University's Said Business School writes:

Understandably, organisations adopt a threat-based risk model to defend their most critical assets. However, a threat-based cybersecurity approach too often lends itself to a direct, cause-and-effect analysis in which relational and/or second-order harms to individuals, third party organisations - and even society itself - might be overlooked. This often happens when one or other organisational perspective assumes exclusive importance.

Must harm management be considered? The concept of harm and second-order harm is clearly not a priority for most organisations. Is it any surprise, then, then that national governments, and even the European Parliament have prescribed ways for organisations to improve when it comes to cybersecurity and the processing of personal

data. The General Data Protection Regulation (GDPR) is the result of Europe taking action to protect the territory from cyber harm and establish the region as a leader in cybersecurity – and, consequently, as a safe place to do digital business. Protecting the digital economy is a prime objective for European Parliament and western European governments have responded with intent, backing initiatives with significant capital.

Conspiracy theorists may conclude that funding for such initiatives must somehow be recovered and a future revenue stream secured. And what better way to do this than to hit those organisations who fail at cybersecurity with significant penalties!

Thriving in a digital-first economy is hard enough for any organisation. Keeping a competitive edge, maintaining customer loyalty, and growing the top-line challenges even the most influential business leaders. Transitioning into companies that provide products and services in ways aligned to today's digital paradigm requires strong leadership with a healthy dose of cybersecurity.

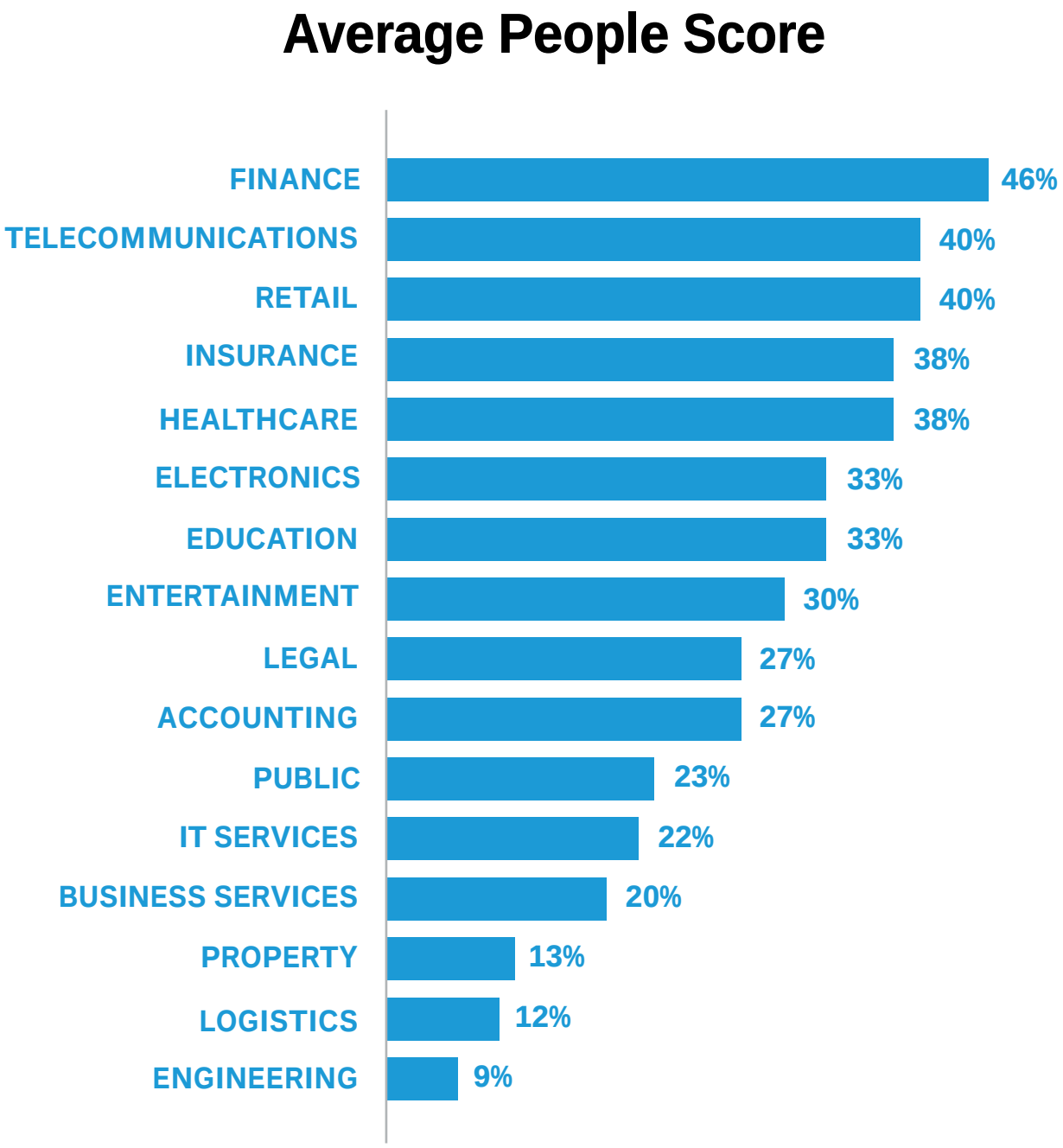
Leadership and governance is the answer we desperately search for, *and need*, to improve cybersecurity maturity.

If the recipe for success is found in cybersecurity management, the best way to mitigate cybersecurity attacks and minimise the resulting impact is to use strong policy and governance, guided by the principles of risk management. Organisations must ensure available defences are active and focused on the assets most at risk. Strong guiding security principles, coupled with strong governance, will ensure organisations safely succeed, where others are likely to fail.

APPENDIX - INDUSTRY INSIGHT DATA

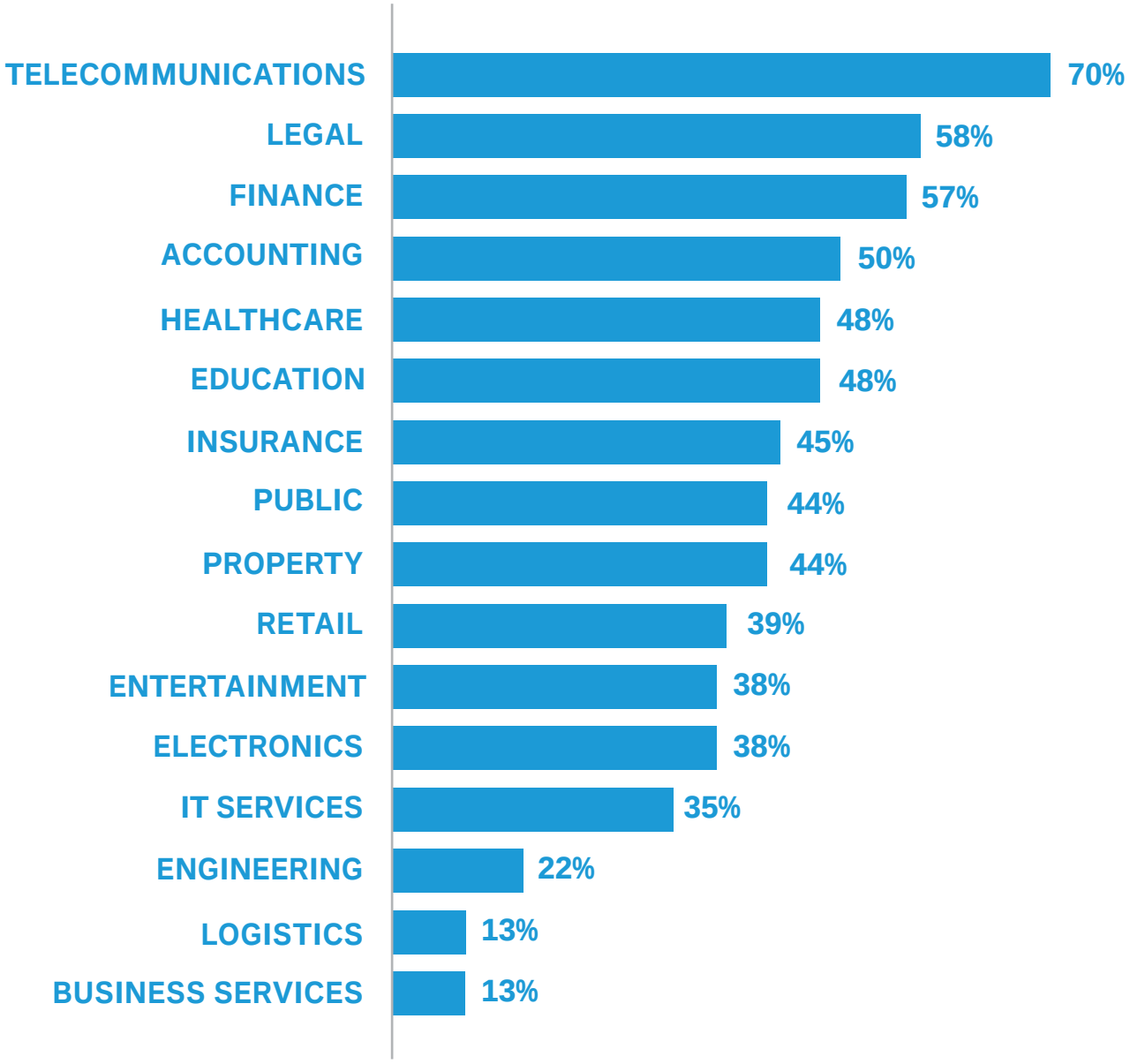
INDUSTRY VERTICAL – ELEMENT AVERAGE

The following charts show the breakdown of the average maturity score across each of the measured industry verticals.

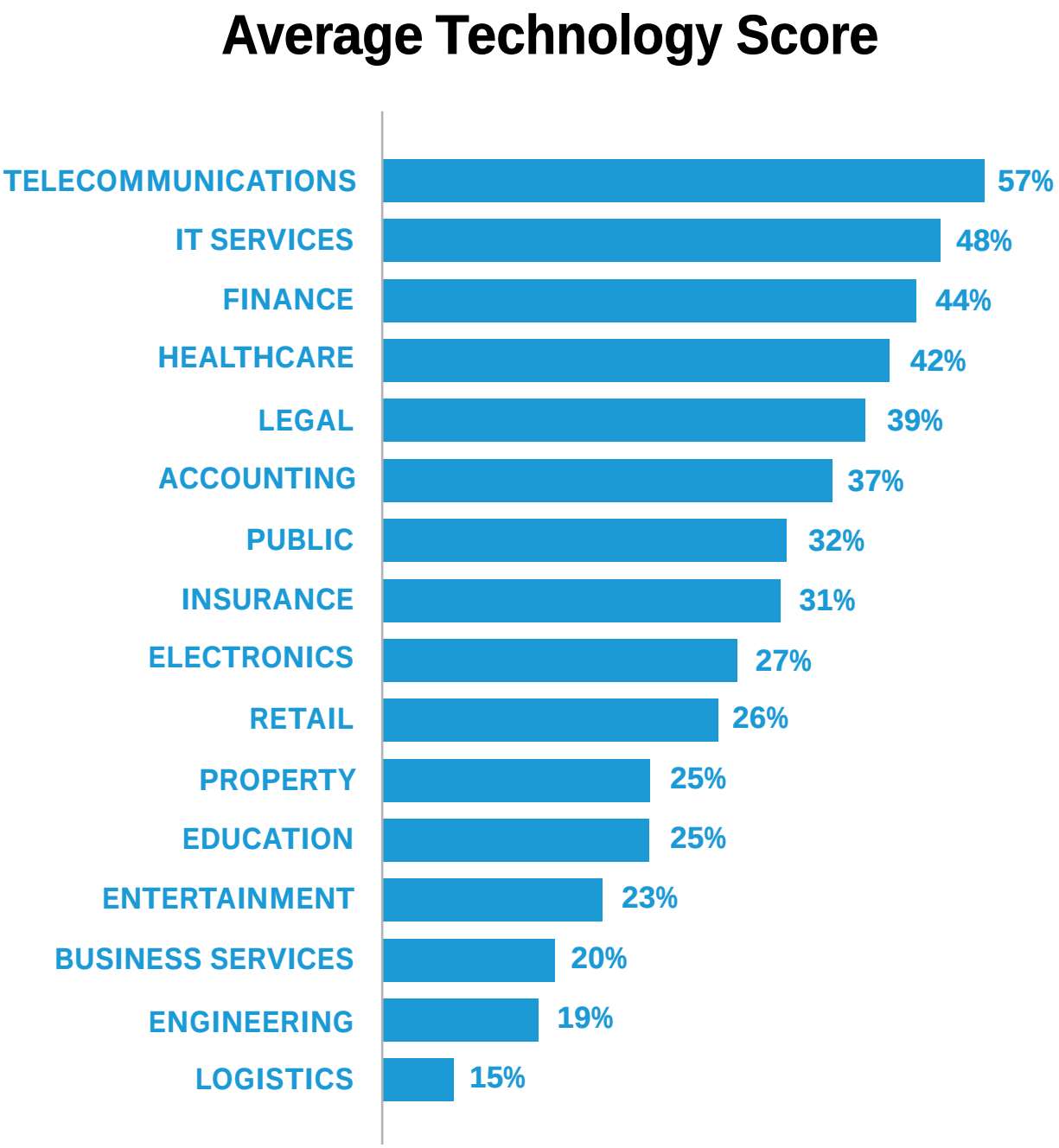


PEOPLE: (Fig 1)

Average Process Score



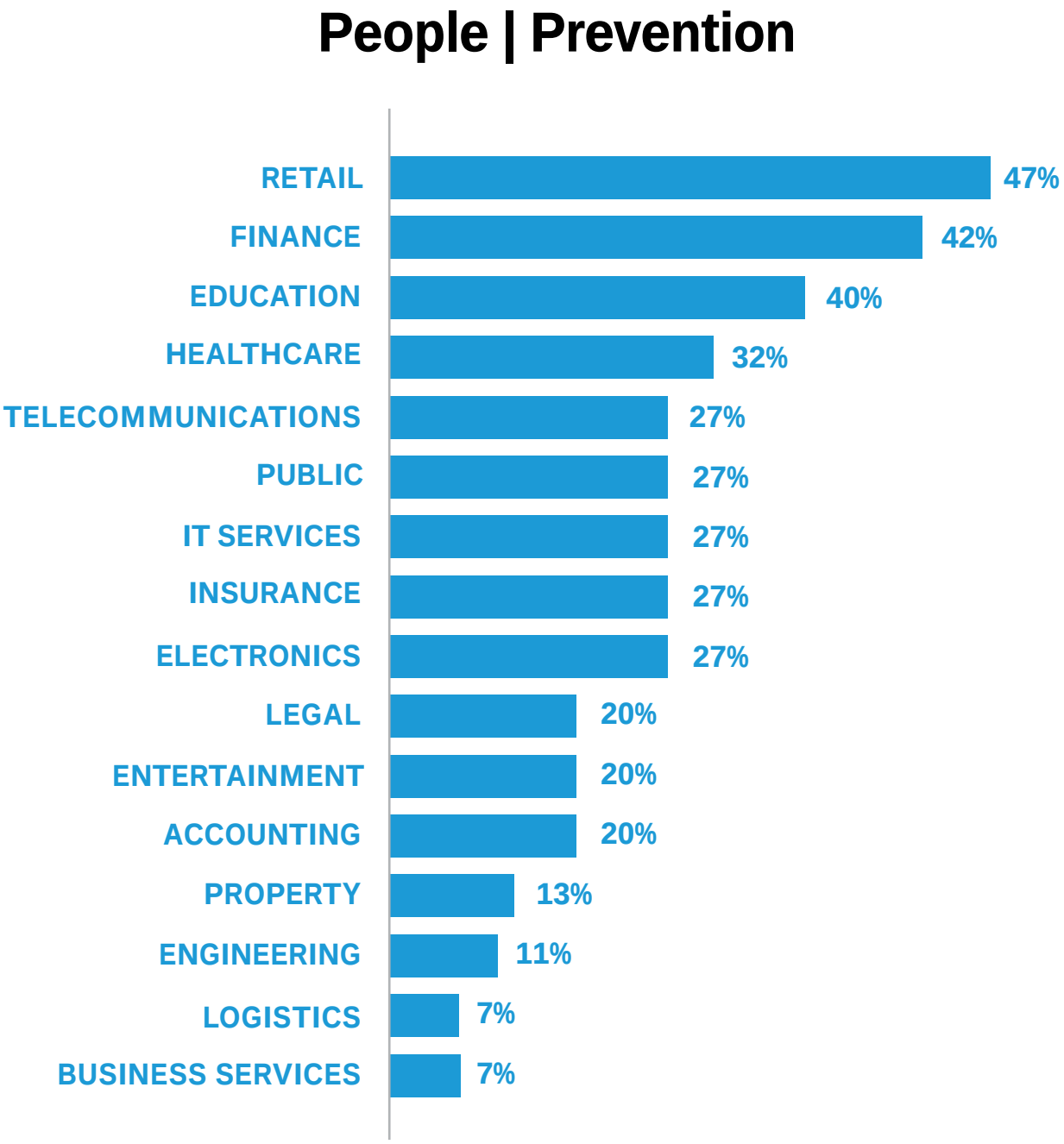
PROCESS: (Fig 2)



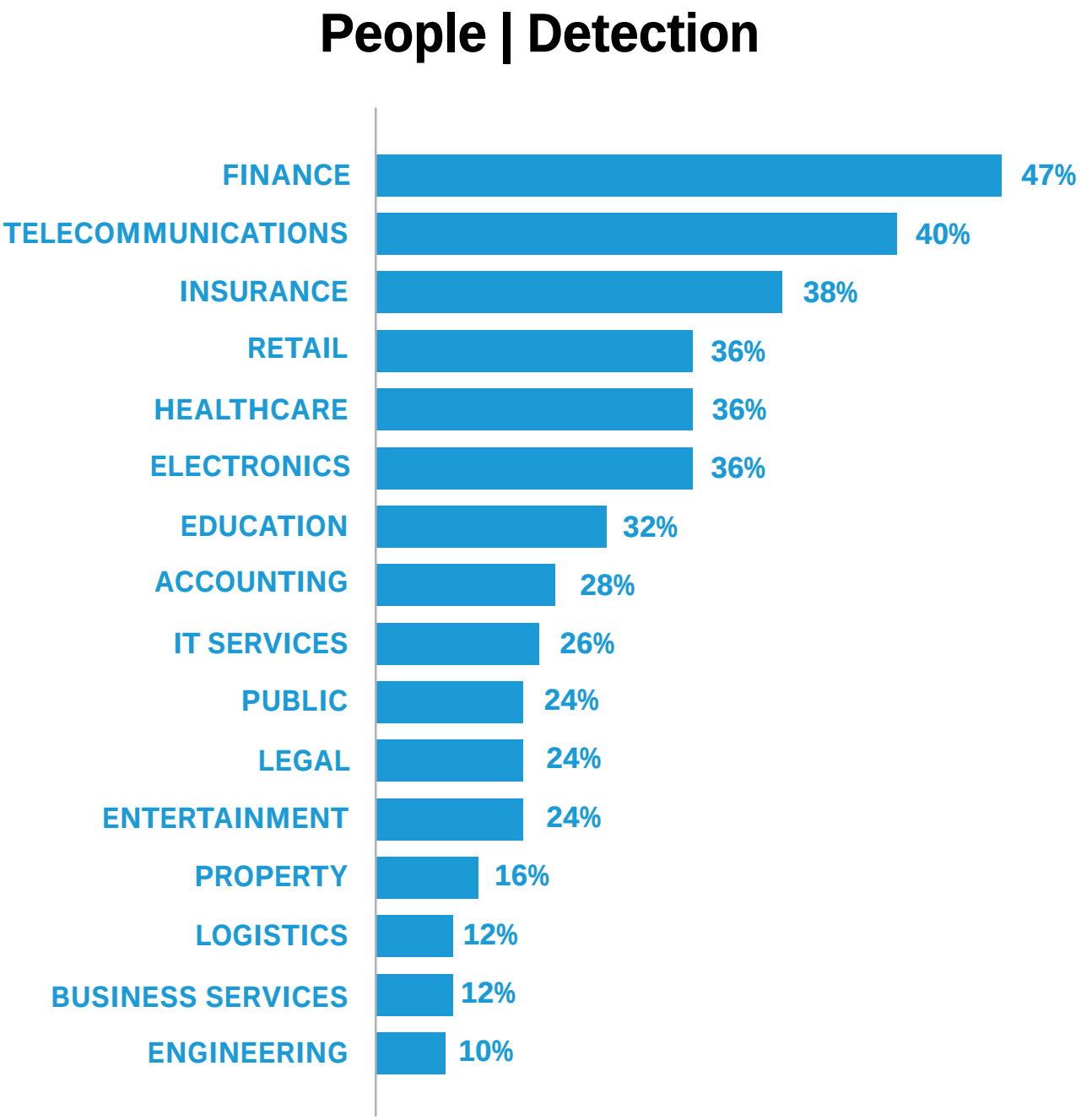
TECHNOLOGY: (Fig 3)

INDUSTRY VERTICAL – ELEMENT AND ACTION AVERAGE

The following charts show the breakdown of the average maturity score across each of the measured industry verticals and across each element and action.

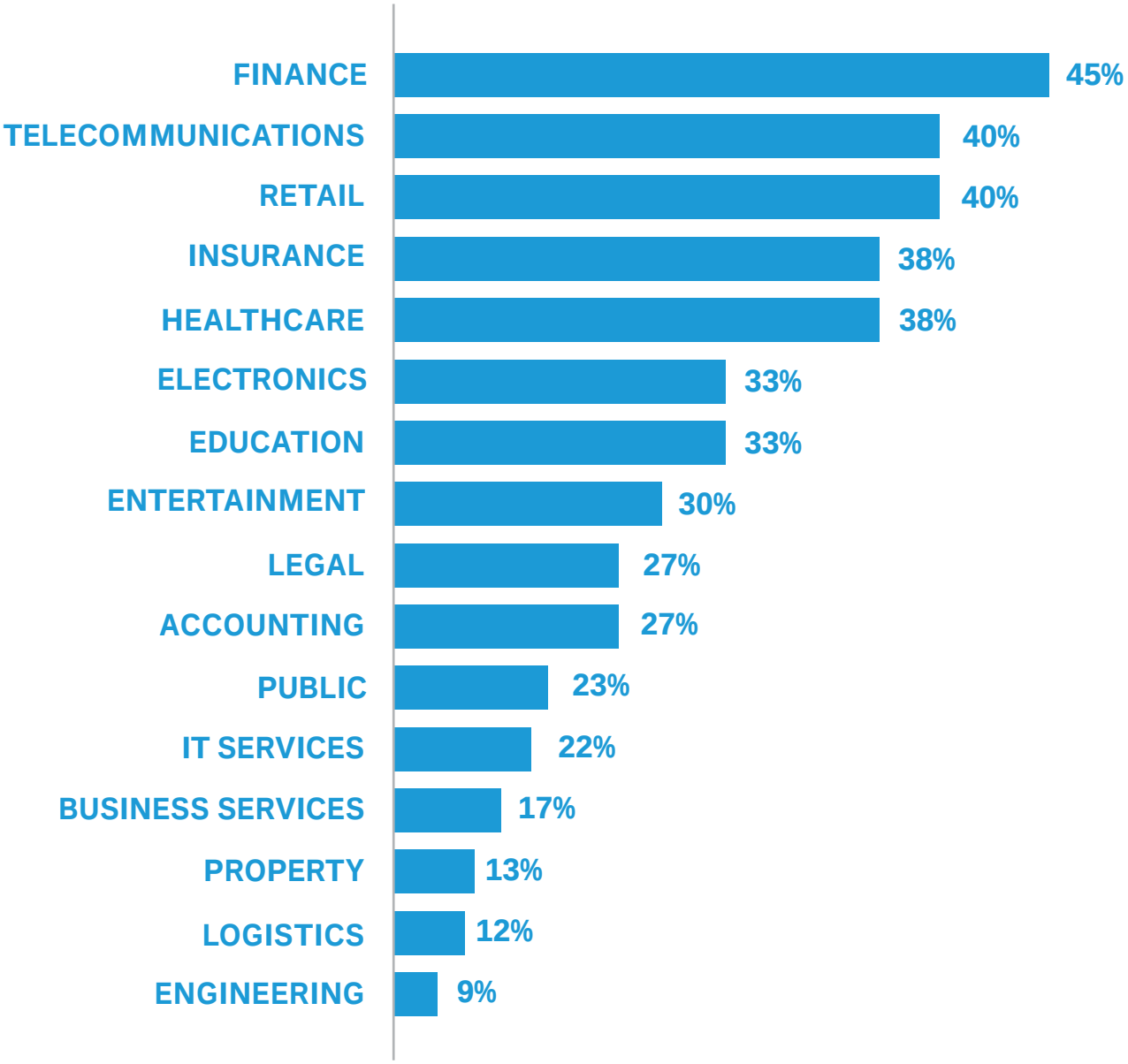


PEOPLE | PREVENTION: (Fig 4)



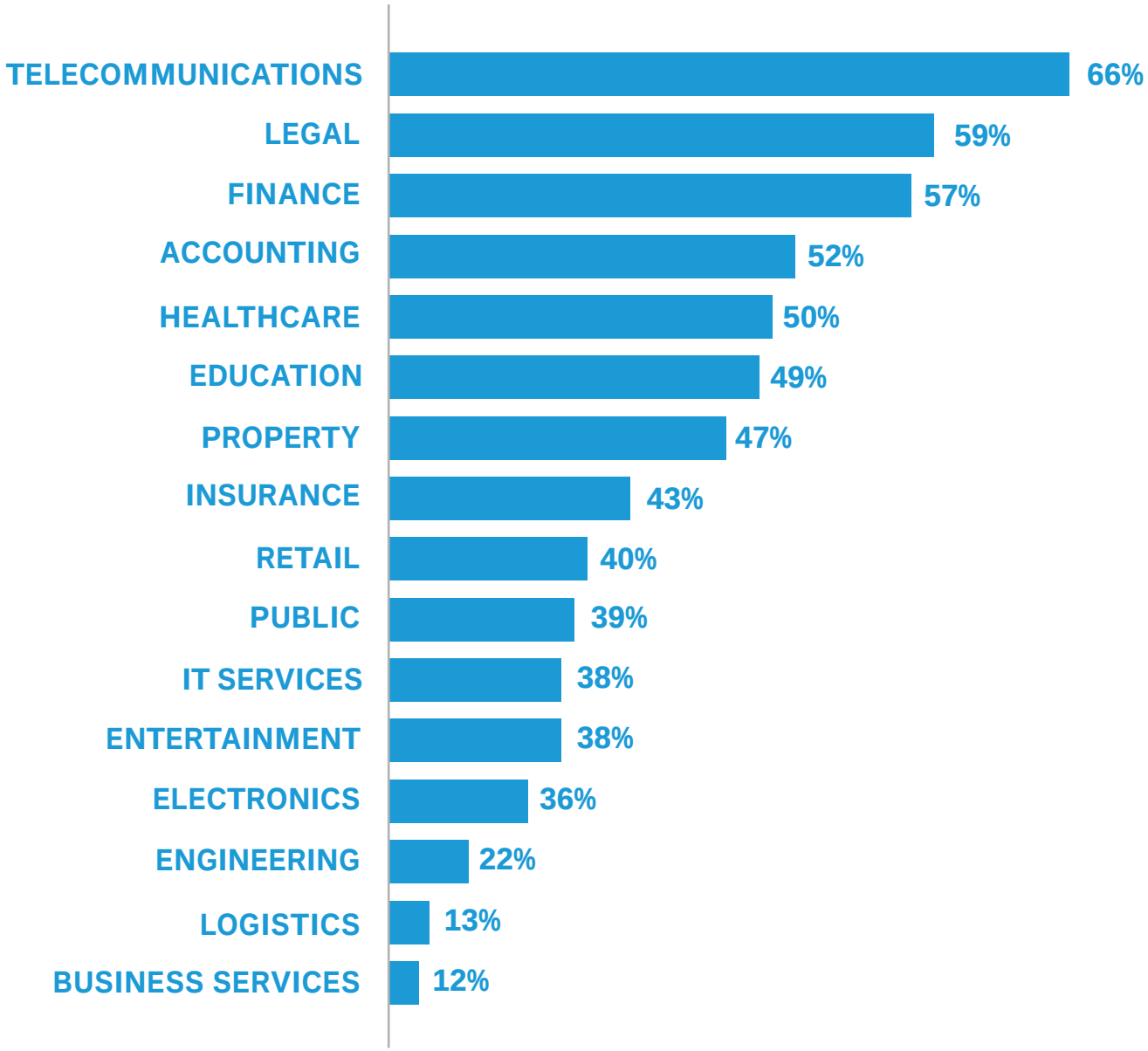
PEOPLE | DETECTION: (Fig 5)

People | Response



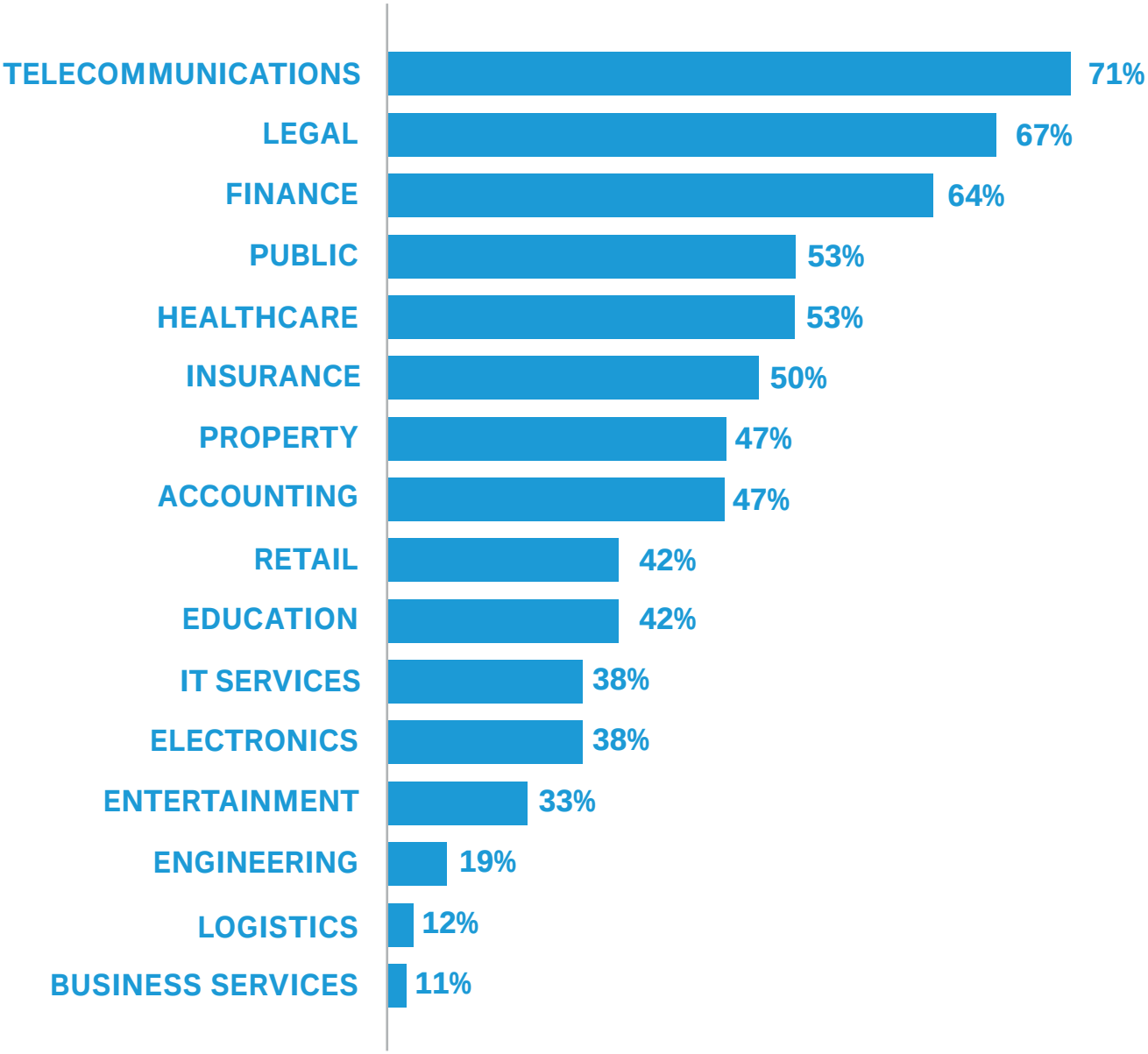
PEOPLE | RESPONSE: (Fig 6)

Process | Prevention

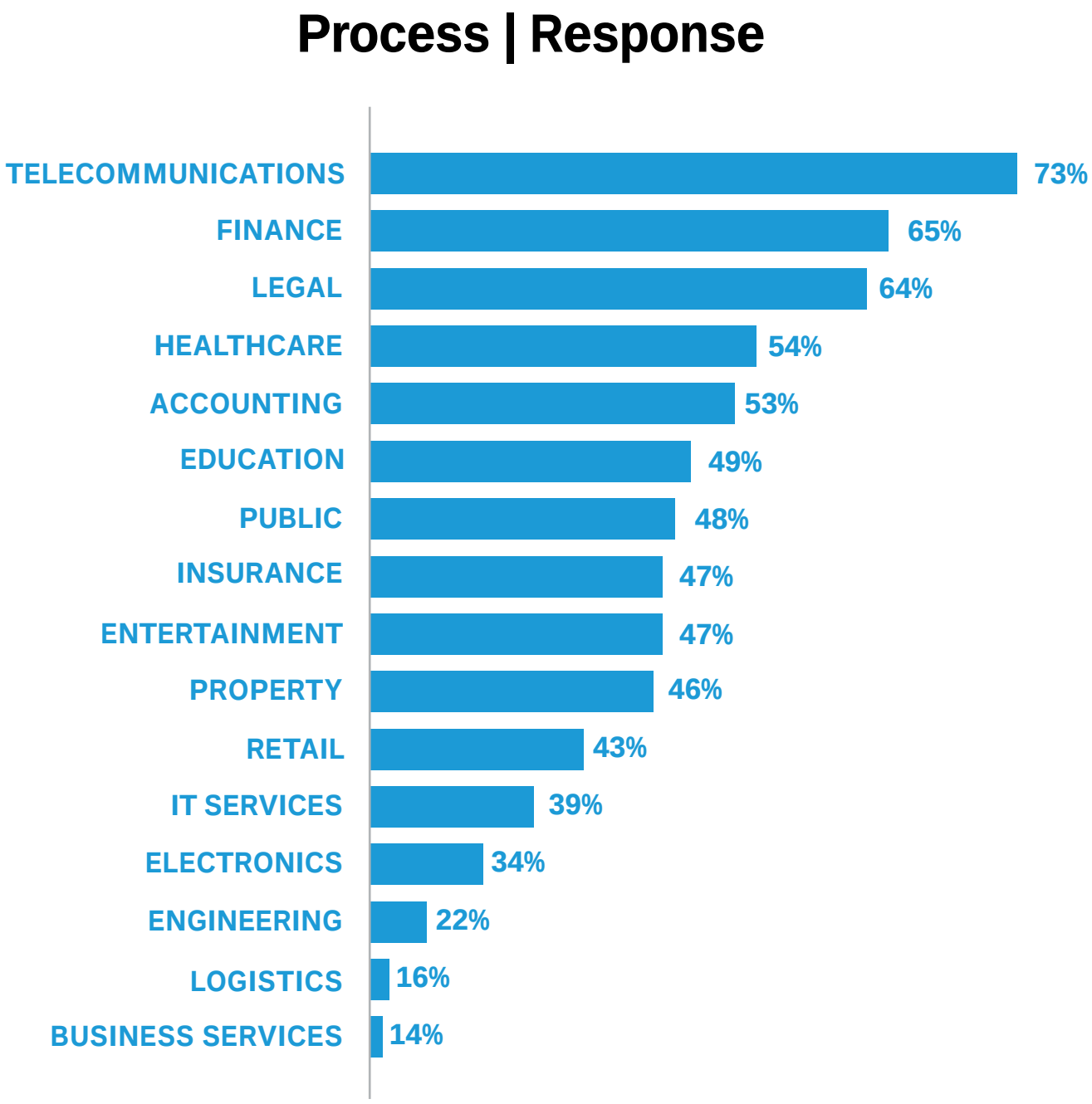


PROCESS | PREVENTION (Fig 7)

Process | Detection

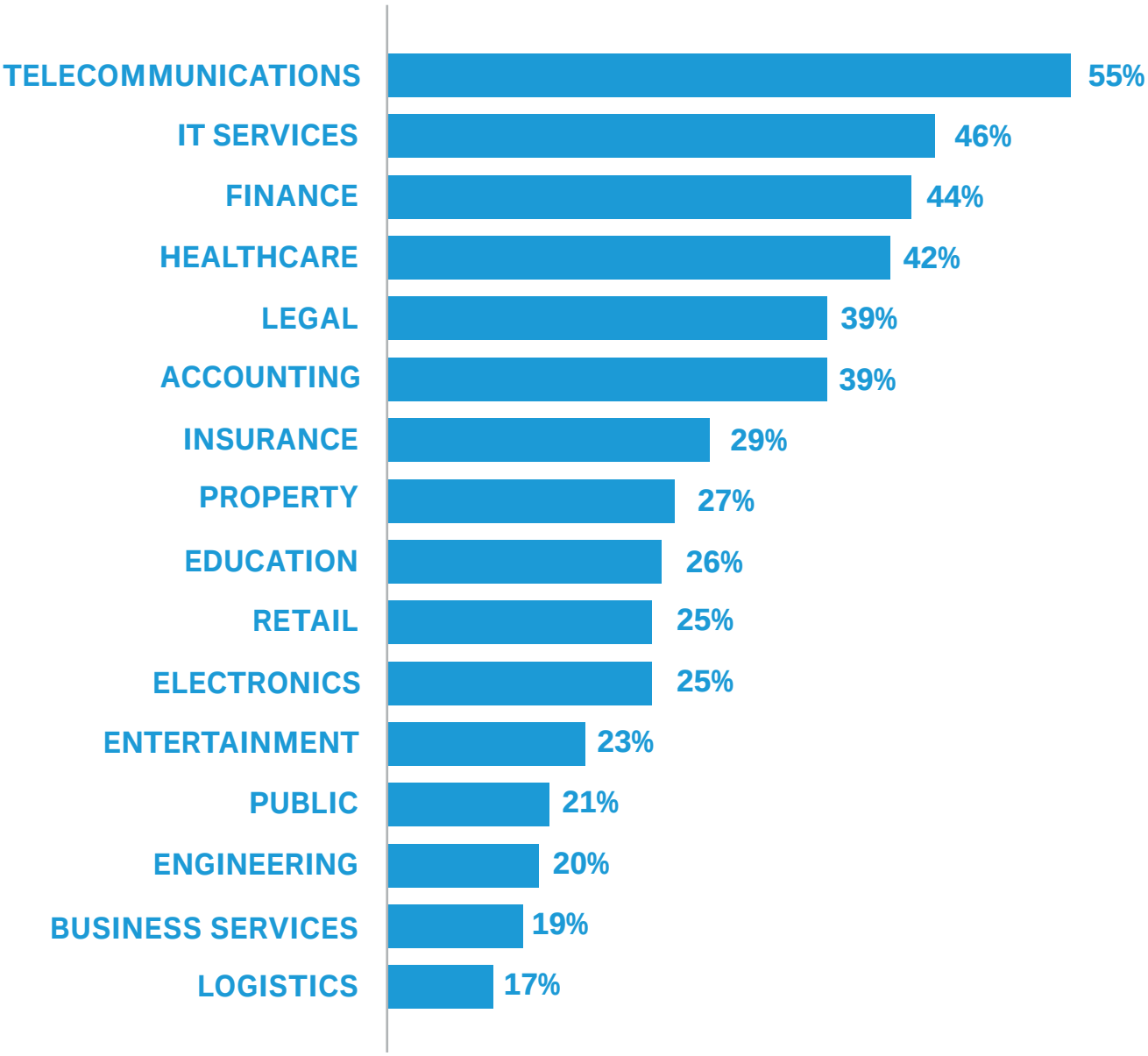


PROCESS | DETECTION (Fig 8)



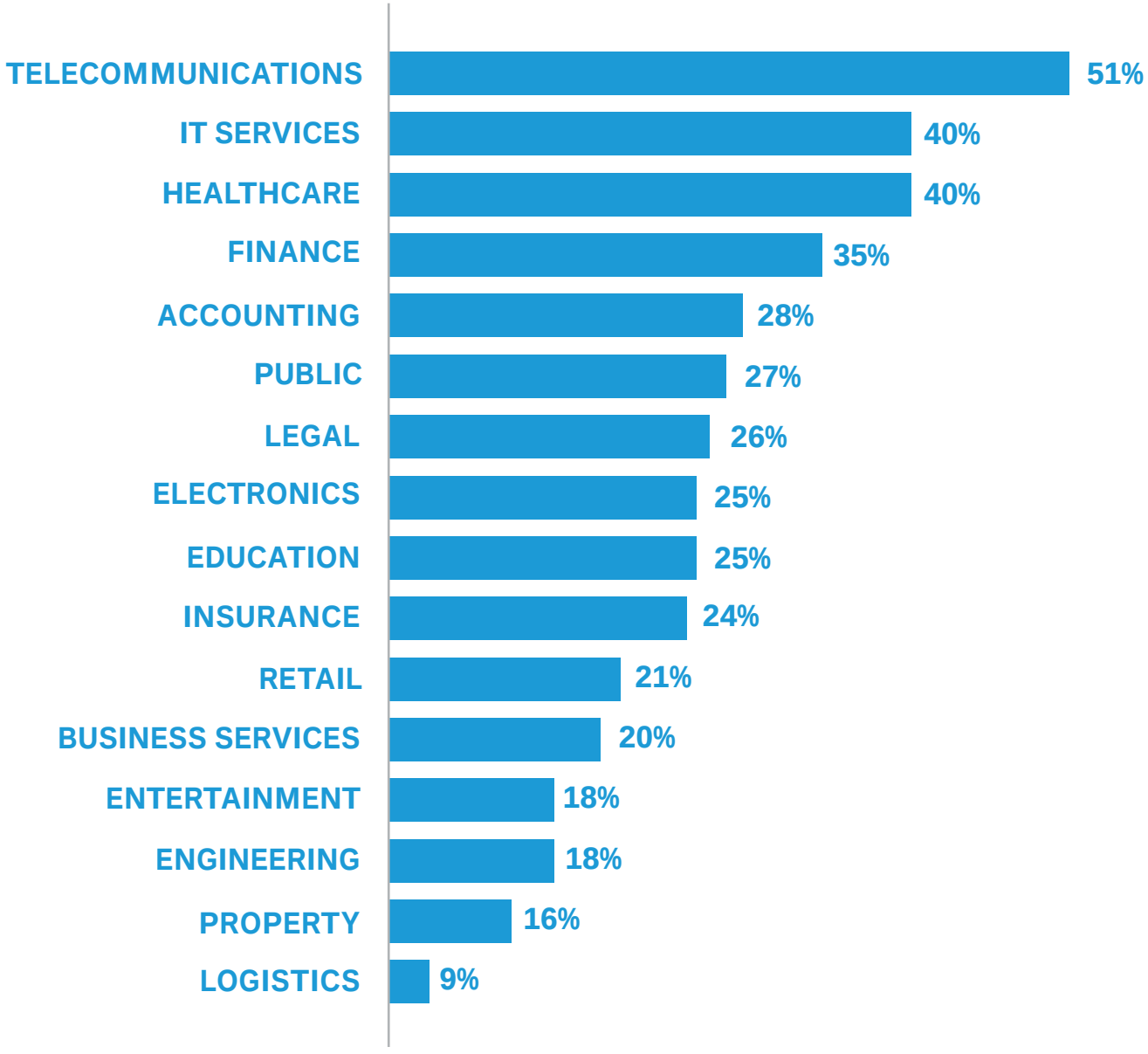
PROCESS | RESPONSE (Fig 9)

Technology | Prevention



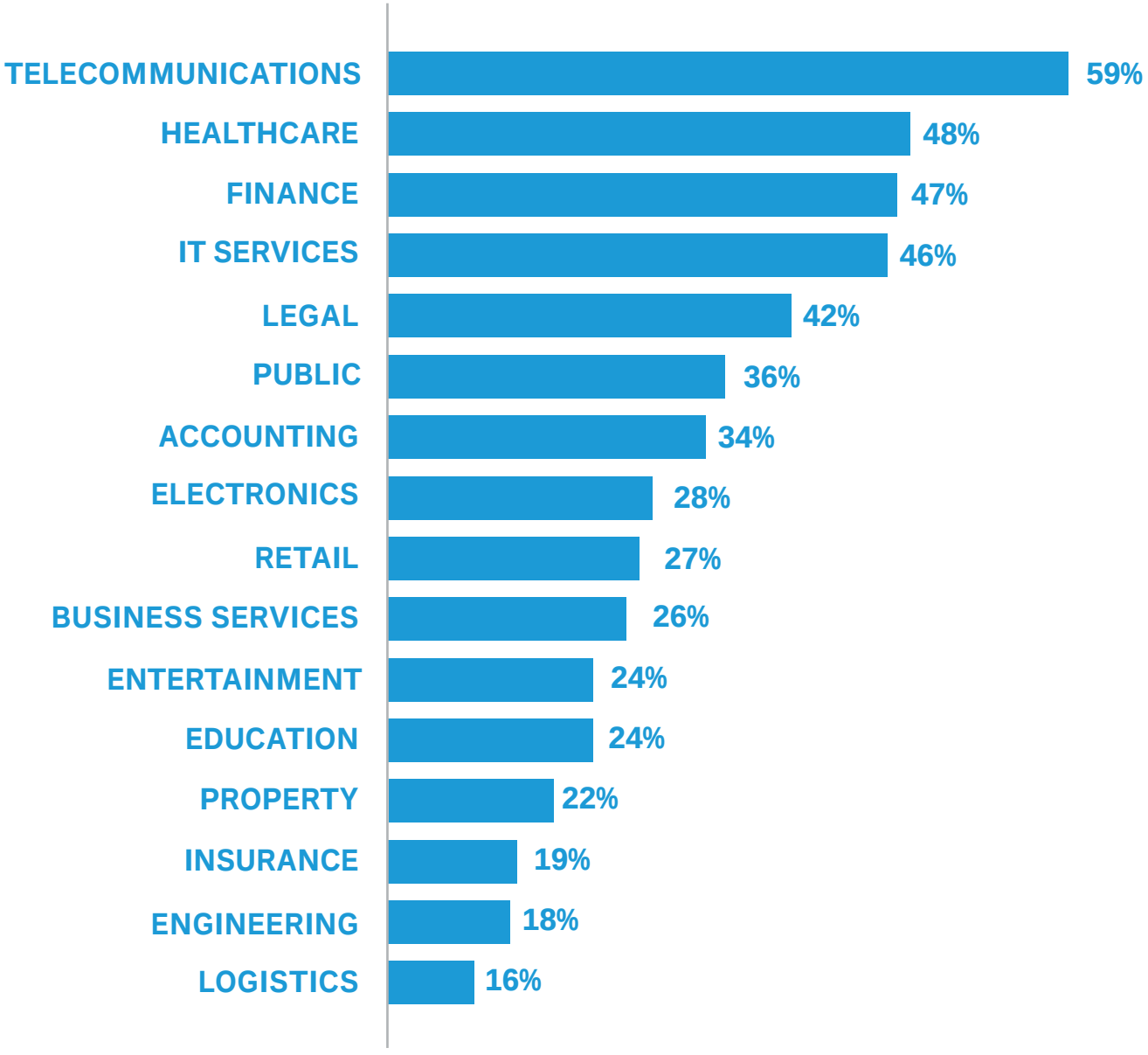
TECHNOLOGY | PREVENTION (Fig 10)

Technology | Detection



TECHNOLOGY| DETECTION (Fig 11)

Technology | Response



TECHNOLOGY | RESPONSE (Fig 12)

APPENDIX - MATURITY LEVEL DEFINITIONS

PEOPLE

MATURITY LEVEL	DEFINITION
0 – ABSENT	Can be described as absent.
1 – BASIC	Can be described as traditional IT or basic responsibilities.
2 – DEVELOPING	Responsibilities have been assigned to a small number of individuals; identified individuals available.
3 – DEFINED	Dedicated teams; management supported.
4 – MANAGED	Resource is appropriate and works in a structured manner.
5 – OPTIMAL	Resource is regularly reviewed to meet the demands of the function. Effective workforce education is in place. Management funding is available.

PROCESS

MATURITY LEVEL	DEFINITION
0 – ABSENT	Process is absent.
1 – AD-HOC	Process is unpredictable, poorly controlled and reactive.
2 – PARTIAL	Process characterised for projects and is often reactive.
3 – DOCUMENTED	Process is characterised for the organisation proactively. Standards defined etc.
4 – SOFTWARE SUPPORTED	Process measured, controlled and supported by software when possible.
5 – REGULARLY REVIEWED	Focus is on improving the process.

TECHNOLOGY

MATURITY LEVEL	DEFINITION
0 – ABSENT	Technology is not in place.
1 – BASIC	Technology can be described as basic or not state of the art.
2 – PARTIAL	Technology is appropriate but partially deployed.
3 – AVAILABLE	Technology has been fully deployed.
4 – ENABLED	Technology has been fully deployed and supported by standards and automation.
5 – INTEGRATED	Technology can be described as fully integrated; events are monitored and support the operational security picture.

www.securelink.net/sma