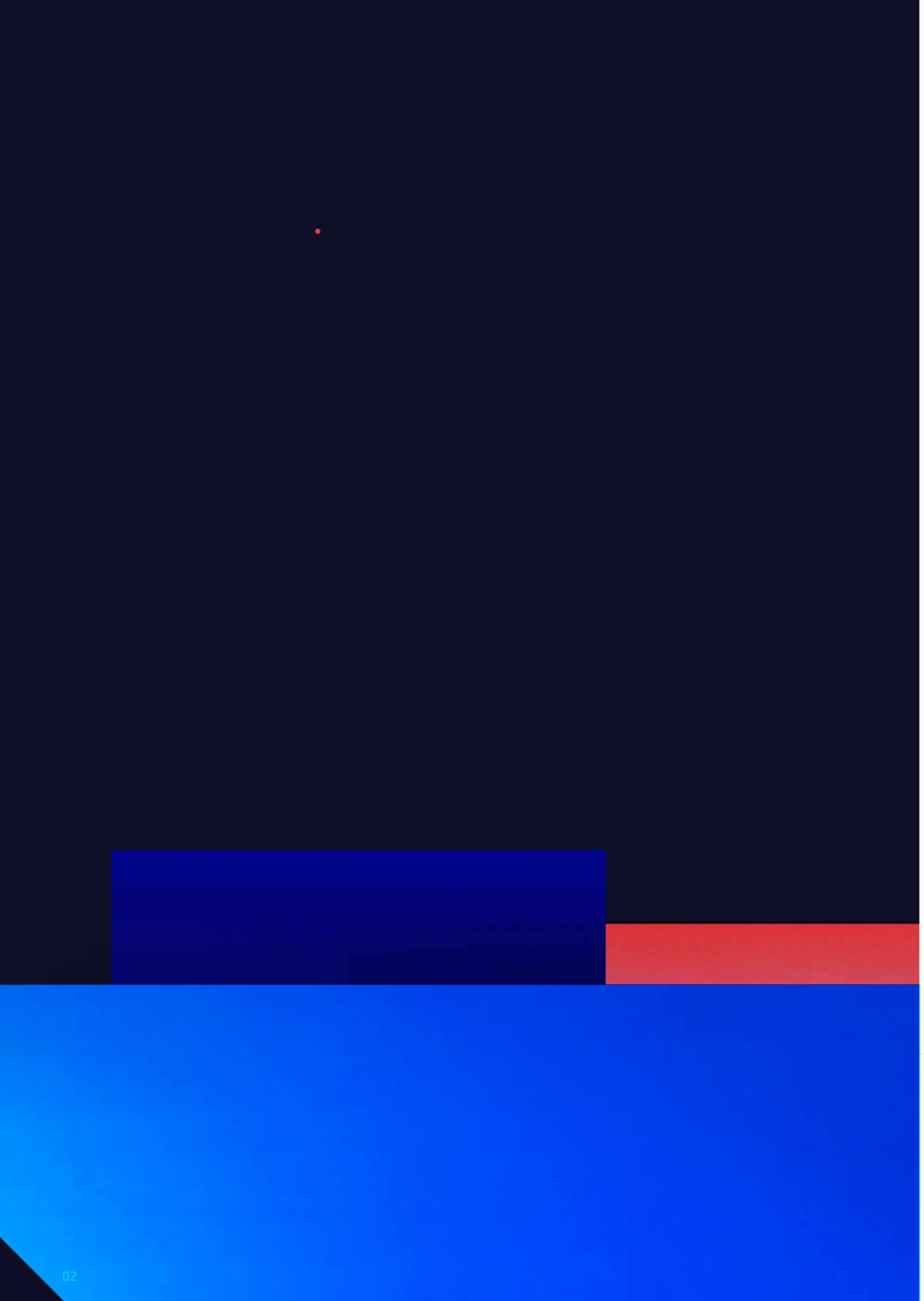
Cyber Workforce Benchmark

A data-led understanding of global cyber knowledge, skills and judgment

2022



Index

Foreword

Phil Venables

VP - Google / Chief Information Security Officer - Google Cloud
Member of President's Council of Advisors on Science and
Technology, The White House

Achieving cyber resilience requires a shift in thinking for many organizations.

Traditionally, the ability to address adverse events is a by-product of a well-worn planning process. Potential risks are identified, proposed responses outlined and then filed away for use when the situation arises, along with all the other plans.

Against a dynamic risk, this approach falls short. Plans enshrined on Tuesday fall short when Wednesday's threat arises out of left field with a whole new set of variables. The further you try to flex existing approaches, the more irrelevant they become. Previously innocuous or unpredictable minutiae set off a chain reaction. Your plan is static. The risk isn't.

The answer lies not in plans, but capabilities. Developing an organization which has the ability to be open minded, agile and adaptable in the face of change – one which has cognitive agility – is critical.

Against modern all-encompassing threats, this means bringing the abilities of the entire workforce to bear. With risk spreading across the organization, so should mitigation. In this way, cybersecurity teams play a more strategic role – as well as being applied technically – but responsibility is also distributed across everything from the SDLC to executive teams. This brings ownership, encourages a foundational approach to resilience and minimizes resource burn.

By taking into account how all the elements of adverse events interact, organizations can move towards operational resilience. Not only does this enable a more holistic approach to both downstream and upstream risk – everything from supply chains to customers and regulators – but it also allows for impact tolerances to be set and assessed.

This is all said with an understanding that it is not an easy task. For most organizations, having a consolidated picture of something as seemingly intangible as capabilities seems a mammoth task. However, as current events compel organizations to step back and consider a bigger picture of risk and resilience, I believe it is a necessary path to be on. The first step is a better understanding of our capabilities as an industry.

Methodology

Our platform tests, measures and improves human cyber capabilities inside large organizations, giving us a unique global view. This report shares some of this insight for the first time.

We continually run cybersecurity, application security and executive teams at large global organizations, as well as the talent of tomorrow, through cyber exercises and simulations, collecting data on their ability to mitigate the latest threats. This involves everything from wide-scale crisis exercises to specific threat simulations.

Every section is written by the relevant lead in the capability being analyzed. Additional analysis is then applied by Chartered Psychologists Rebecca McKeown and Dr. John Blythe – specialists in applying behavioral science to cybersecurity and high-intensity situations.

Over the last 18 months we have visibility of the workforce cyber capabilities from:

2,100
organizations

> 500,000
exercises and simulations

> 1,500
separate threats and incidents

We analyze these and cross reference them with metadata such as engagement rates, decision-making effectiveness, speed of learning, sector and more. Each section adds more detail on specific datasets.

01

Understanding organization-wide crisis resilience

Ben Hockman_Cyber Crisis Management and Response Lead

Introduction

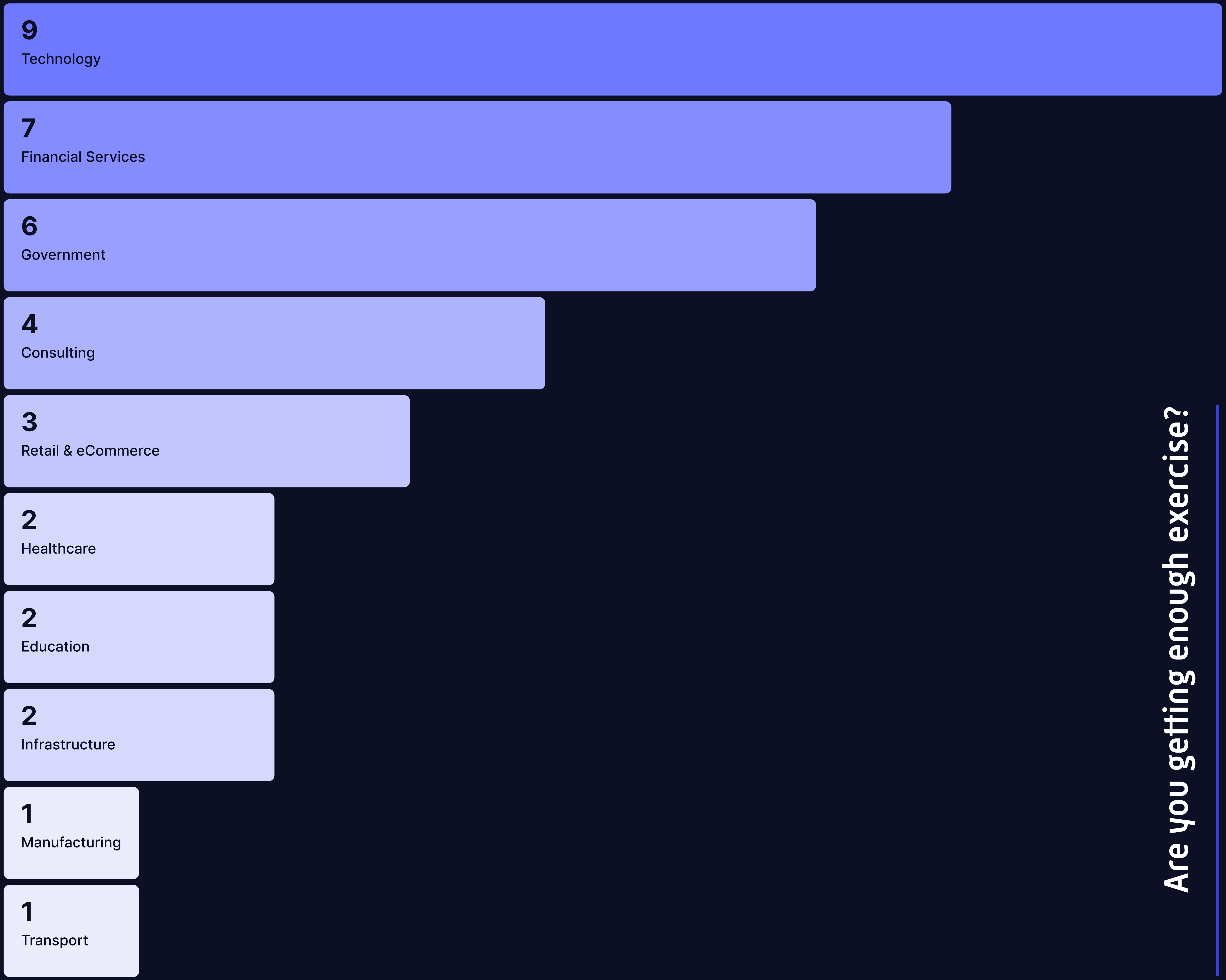
The modern cyber crisis is an all-encompassing organizational trauma. Stopping incidents bringing operations to a halt and destroying reputation, corporate value and stakeholder relationships requires a holistic response from the entire workforce. Achieving this kind of resilience requires a continually maturing responsive capability for technical and non-technical teams, developed by exercising with a cadence that traditional tabletop exercises struggle to achieve.

Baseline

This section analyzes the data produced by 500 crisis scenarios run by participants on the Immersive Labs platform in 2021 – everyone from board members to cybersecurity teams. These exercises tested some of the world's largest commercial brands and government organizations with nearly 6,400 'wicked problems' using simulated online cyber crises.

Industry

Average number of exercises per year



Are you getting enough exercise?

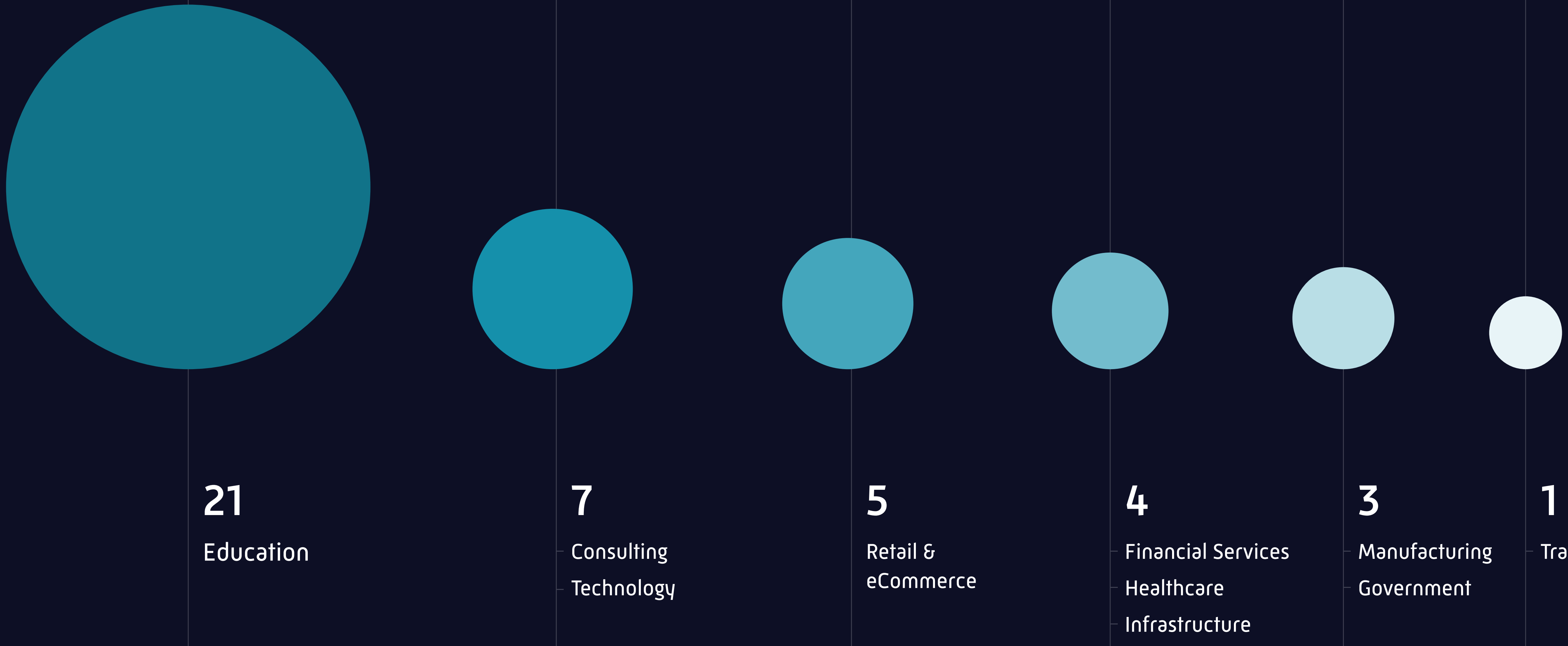
The number of crisis exercises carried out by Immersive Labs' customers varies widely by sector from one to nine a year.

It's no surprise that prized, high-profile targets run the most crisis exercises. Technology and financial services companies prepare the most for cyber-attacks, running an average of nine and seven exercises per year respectively. Banks, as critical national infrastructure and being highly regulated, have extra impetus for preparation.

Interestingly, other critical national infrastructure organizations are at the opposite end of the table for exercising cadence. Manufacturing, infrastructure and transport lag behind on cyber crisis preparedness, running an average of just one exercise per year. This slow cadence is despite the proven vulnerability of the underlying industrial control systems they run.

Better together

Average number of participants



The average crisis exercise has six participants. When analyzed by sector, it appears educational organizations value collaborative crisis preparation far higher than any other, exercising three times as many team members together than the next highest – technology.

In terms of how the breadth of team members affects performance, only 3% of the 500 crisis scenarios run scored below 50% in terms of performance. Each of these, bar one, was when people were tackling a crisis scenario alone. By contrast, every exercise scoring over 90% effectiveness had an average of 11 people participating.

Questionable healthcare

The average performance score[1] across all exercises analyzed was 68%. This score is an amalgamation of the quality of all decisions made throughout the entire simulation and suggests cybersecurity response, in general, has some way to go.

The worst performing industry in terms of cyber crisis response, by some margin, was healthcare with a score of just 18% – markedly worse than the leading sector, manufacturing. Finance and government, two heavily targeted sectors with complex stakeholder sets and a heavy regulatory burden, performed third and second worst respectively.

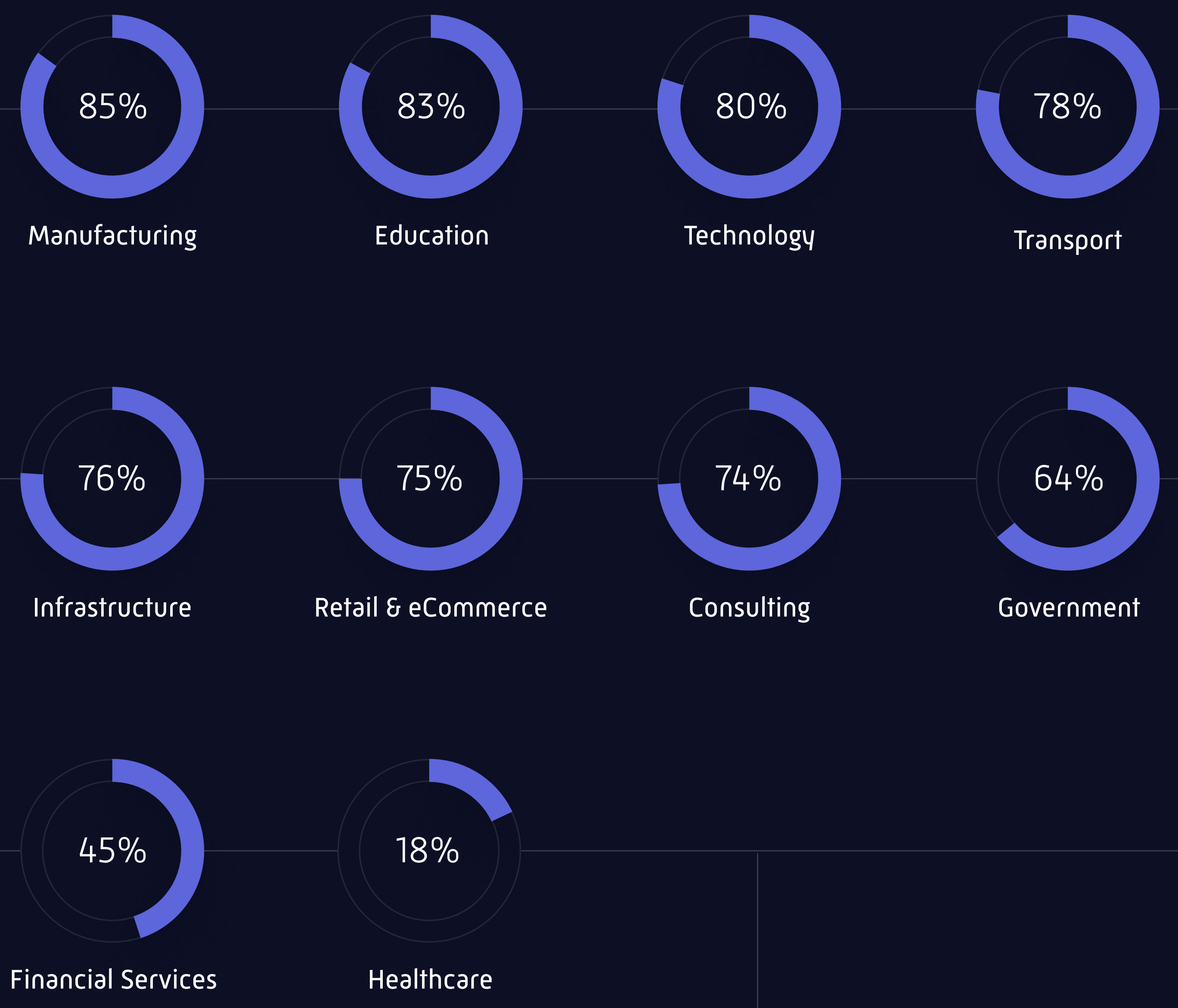
Out of the top ten worst scoring decisions, five came from the financial services industry. The lowest performing of these was how to respond after being double extorted following payment to a ransomware actor.

While you might assume that the innovative technology sector would lead in terms of performance, manufacturing and education did better in terms of crisis response.

Out of the **top ten worst scoring decisions**, five came from the financial services industry.

Industry

Average performance score



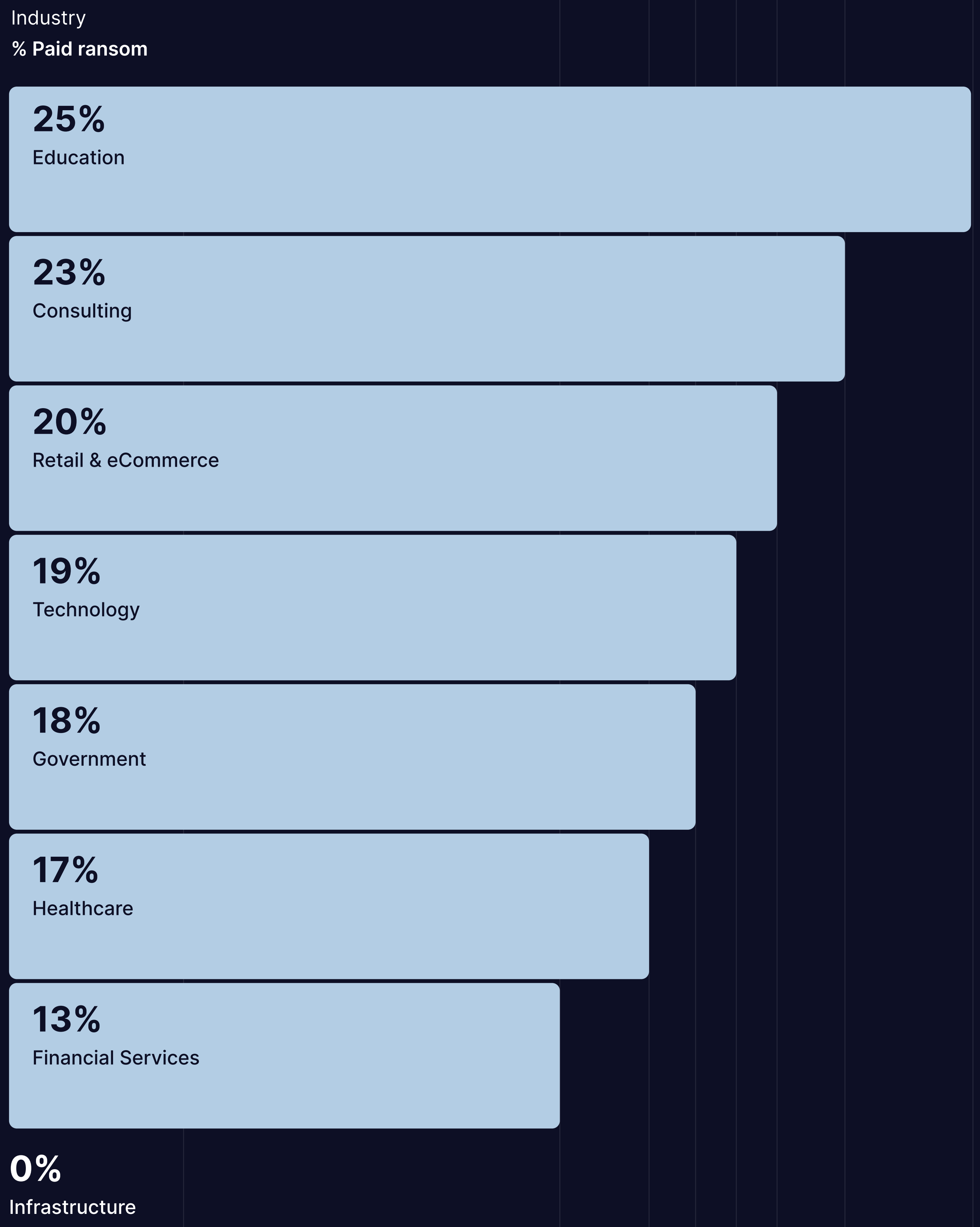
[1] Each separate decision throughout a crisis simulation is given a score depending on how well it addresses the overall crisis. The performance score amalgamates these.

Ransomware – difficult decisions to make

Crisis response teams trying to defend their organization against ransomware were plagued by uncertainty. Seven out of the top 10 crisis scenarios with the lowest overall confidence in respondents' answers were ransomware simulations.

Teams did not want to pay the ransom but were uncertain about the outcome of not doing so. The predominant desire was to not pay the ransom, with 83% choosing not to do so. There are some interesting sectoral trends to note here: not a single crisis response team in the infrastructure sector paid the ransom, with only 13% of those in financial services capitulating to ransom demands.

The keenest sector to pay the ransom was education, with a quarter paying up. Interestingly, 18% of government crisis response teams paid the ransom in an exercise, despite official guidance in most countries stating not to.



The Psychologist's View

Rebecca McKeown /
Dr. John Blythe

Cyber crisis response presents an interesting new area for the psychology of incident planning because the hybrid digital/real world environment imposes a very high cognitive workload. Optimizing human capabilities by developing cognitive agility can have a powerful cumulative effect on crisis resilience. The data raises some interesting questions on how this is being achieved:

Cadence
The more an organization exercises their abilities, the better they become. Skills acquisition is iterative for three reasons:

- Individuals first develop surface-level knowledge of a capability – an understanding of the fundamentals – before graduating to more advanced thinking. People start with the 'what' but over time graduate to understanding the 'how' and 'why', which are all vital when making decisions in intense situations.
- If these capabilities aren't reinforced, they fade. Your crisis response quickly goes back to square one if not exercised.
- Only with regular exercising will crisis response teams be able to consciously develop the ability to make connections between previous decisions and how to apply them – or not – during an incident. A real crisis is not the time for learning. This is a core tenet of cognitive agility.

Suggestions for senior leaders: A regular cadence of exercising is central to building cognitive agility. Once per month should be a minimum. Crisis resilience is all about continual maturity. A mindset shift is needed for this to occur: exercising must become a 'business as usual' function, not an occasional luxury.

Breadth
In a crisis, diversity of thought is important. This is more than spreading workload: the research shows that a wider pool of knowledge, skills and judgment provides a more rounded solution to the problem. With a cyber crisis requiring an understanding of everything from technical to reputational issues, a depth of understanding of each is important. It also encourages more creative solutions to emerge.

Suggestions for senior leaders: Consider each business risk point from a cyber crisis – everything from technical to customer teams – and ensure representatives from each area exercise together. Avoid groupthink by encouraging independent decision-making in a judgment-free environment and apply external and data-based analysis of team decisions.

Ransomware
It's impossible to talk about cyber crisis psychology without mentioning the data on ransomware. The analysis on confidence points towards a classic 'wicked problem' for crisis response teams – where, when considering options, there isn't a clear-cut resolution. These types of decisions are characterized by data overload and decision-fatigue. The brain is overwhelmed with the sheer volume of information, choice and decisions, so we settle on a compromise. This is why we see low confidence scores.

Suggestions for senior leaders: Again, developing cognitive agility with decision-makers across the organization will help. Rushed decisions based on fear, uncertainty and gut-feeling or founded in ethical and moral biases lead to poor outcomes. Instead, crisis response teams need to develop the ability to make self-aware decisions at a distance which take into account a broad spectrum of opinions.

02

Building more resilient cybersecurity teams

Kev Breen_ Director of Cyber Threat Research, Immersive Labs

Introduction

The workforce cyber challenge facing large organizations is complex and demanding. A continual barrage of fast-moving threats – each executing in a multitude of phases and targeting different parts of the organization – stretch capabilities to the limit. A gap quickly emerges between the cybersecurity knowledge, skills and judgment an organization has and what it needs. Understanding the data is the first step.

Baseline

We analyzed data from over 300,000 simulations completed by cybersecurity teams in 12 sectors. These helped cybersecurity teams understand how to do everything from dissect the latest malware to packet analysis in the Security Operations Center (SOC). The aggregate data was then mapped to MITRE ATT&CK™ to provide structure.

MITRE ATT&CK™

For those unfamiliar with MITRE ATT&CK™, it is an information security framework which consolidates the various techniques used by adversaries. The framework breaks cyber risk down into 12 separate tactics, denoting different phases of an attack. This provides organizations with a unified view of attacker tactics, techniques and procedures.

A focus on initial point of attack

The data shows us which capabilities cybersecurity teams within large organizations are choosing to develop, with 1 being the most popular and 12 the least.

01 Execution	02 Defense evasion	03 Discovery	04 Privilege escalation
05 Persistence	06 Initial access	07 C&C	08 Credential access
09 Lateral movement	10 Impact	11 Exfiltration	12 Collection

Broadly, cybersecurity teams are more focused on workforce capabilities on the left of MITRE ATT&CK – the techniques used by an attacker to establish a presence and maintain a foothold – than those that relate to the fallout from an attack. It seems cybersecurity teams prefer to understand the process of being pwned than the resultant impact of malicious actions.

The fact that labs on execution – understanding how malicious code is run – are five times more popular than data collection or infiltration (some way down the attack chain) bears this out. A deeper dive shows that understanding the basic tenets of code execution, such as scripting and understanding the Command Line Interface (CLI), are the most desirable of these specific skills. This trend plays out across all sectors.

It seems cybersecurity teams prefer to understand the process of being pwned than the actual problems it causes.

The data opposite underlines the relative lack of desire to understand techniques that allow attackers to collect, manipulate and exfiltrate data, making up just 9% of all labs completed in total. By contrast, the categories in the earliest portion of the attack chain – initial access, execution and persistence – made up 34% of all workforce capabilities developed.

Sector	Most popular	Least popular
Leisure	Initial access	Exfiltration
Government	Execution	Impact
Transport	Defensive evasion	Impact
Tech	Execution	Exfiltration
Consulting	Execution	Collection
Media / advertising	Initial access	Exfiltration
Healthcare	Defense evasion	Exfiltration
Financial Services	Execution	Exfiltration
Educating	Execution	Collection
Retail	Execution	Collection
Manufacturing	Execution	Collection
Infrastructure	Discovery	Collection

Interesting, but difficult?

To understand how effective cybersecurity teams at large organizations are at developing human capabilities, we also analyzed data on completion times. **The ranking opposite** provides an analysis of how much longer over the expected time it took cybersecurity teams to complete these MITRE capabilities: **1** is closest to the expected complete time, **12** the furthest away.

This shows another interesting trend. Whereas the high-profile compromise-focused skills might be more popular, they seemingly take longer to master. With the average MITRE lab taking 12 minutes longer than expected, those on the left-hand portion of ATT&CK took nearly twice as long, at 23 minutes over expected complete time. By contrast, collection, command and control, exfiltration and impact were under the average, at just over 10 minutes.

As well as being slow to develop, many of the capabilities on the left-hand side of ATT&CK also saw high abandonment rates from cybersecurity teams. Just over half (56%) of all users completed hands-on simulations on initial access once started. Exploiting public-facing applications was particularly hard, with the most difficult aimed at getting users to complete a blind SQL injection.

By sector, the transport and financial services space took the longest to complete MITRE labs, at 23 and 21 minutes over the expected time respectively. The industries quickest to develop workforce capabilities were the leisure and media and advertising sectors at 8.3 and 10 minutes longer than expected.

Time to complete MITRE capabilities

Fastest

01_IMPACT

02_COLLECTION

03_EXFILTRATION

04_C&C

05_LATERAL MOVEMENT

06_CREDENTIAL ACCESS

07_EXECUTION

08_DEFENSE EVASION

09_DISCOVERY

10_PERSISTENCE

11_PRIVILEGE ESCALATION

12_INITIAL ACCESS

Slowest

Poor time to human capability leads to exposure

Baseline

For this section, we analyzed the speed at which over 35,000 members of cybersecurity teams inside 400 large organizations globally developed the knowledge, skills and judgment to address 185 breaking threats. The times quoted are numbers of days taken for users to complete threat intelligence labs once they were available. Typically, we provide these hands-on exercises with hours of a threat being identified in the wild.

Months not days

Cybersecurity teams inside large organizations take, on average, over three months (96 days) to develop the skills necessary to defend against breaking cyber threats. One particular breaking threat – a critical, actively exploited vulnerability in popular mail transfer agent Exim that left 4.1m systems potentially vulnerable – took over six months (204 days) for security teams at large organizations to master on average.

By comparison, national cybersecurity bodies recommend that technical infrastructure is patched in days, or some cases, hours. The US federal cybersecurity agency, CISA, says vulnerabilities should be patched within 15 calendar days of initial detection, while the Australian Cybersecurity Centre recommends as short as 48 hours if an exploit exists.

Critical sectors left exposed

Critical national infrastructure providers show the slowest time to complete when it comes to developing the human capabilities necessary to defeat attackers. Infrastructure and transport took an average of over four months (137 days) after a threat broke to equip their cybersecurity teams with the necessary skills. This is twice as long as the fastest sector, leisure.

It is perhaps no surprise that sectors with digital at their heart, such as ecommerce, entertainment and media, outperformed other sectors by building human capabilities against breaking threats faster. Government organizations also performed well, arming their cybersecurity teams with the necessary skills to defeat breaking threats faster than even the technology and financial sectors, which are traditionally considered to be two of the more security-mature spaces. Interestingly, consulting, a business model based on imparting knowledge, was the third slowest in terms of learning new human cyber capabilities against breaking threats.

Sector_Average days to complete

● Leisure / Entertainment	65
● Retail & eCommerce	68
● Media & Advertising	69
● Government	88
● Technology	92
● Financial Services	97
● Education	100
● Manufacturing	108
● Healthcare	116
● Consulting	118
● Infrastructure	128
● Transport	145

Motivated by profile

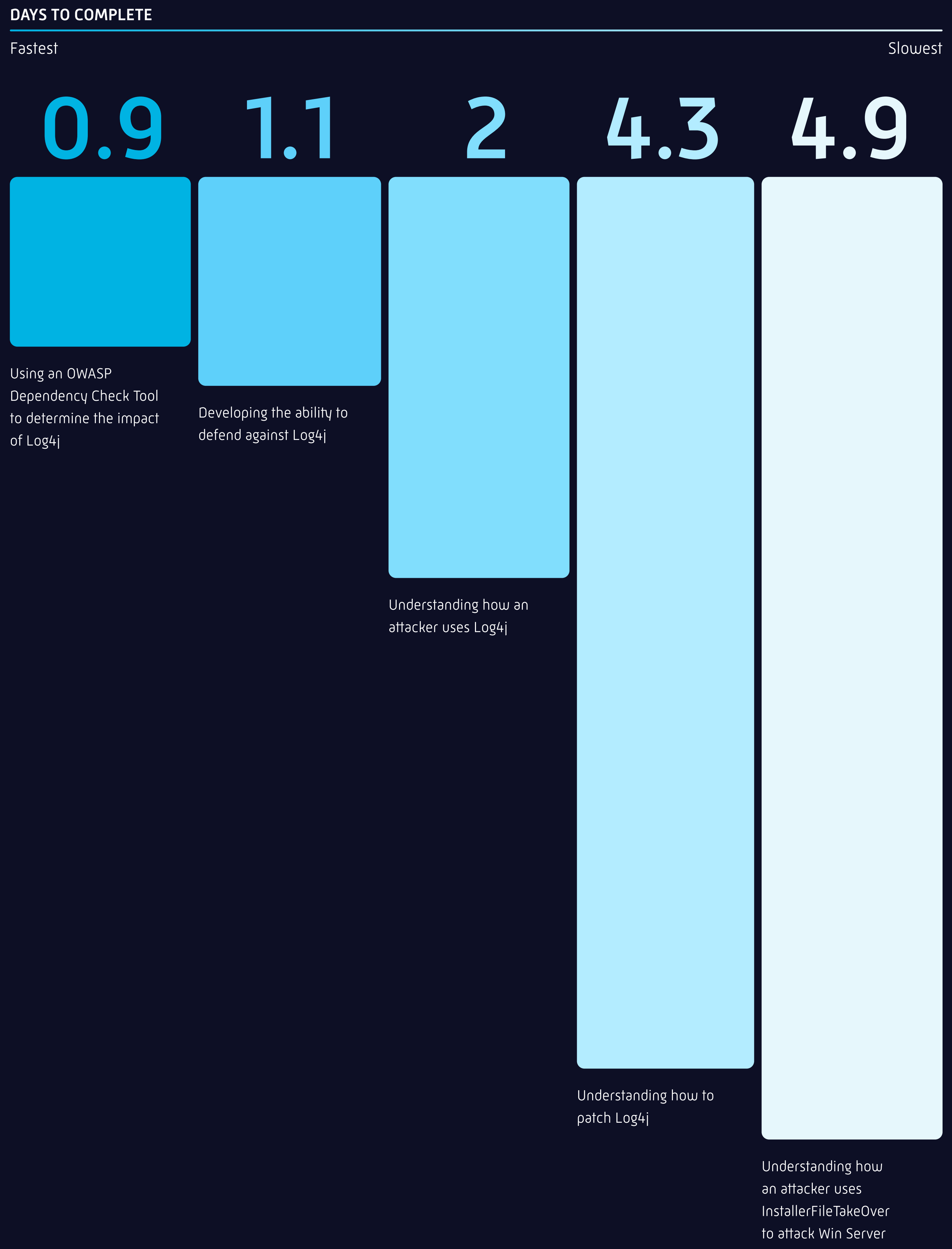
Four of the top five fastest developed skills in 2021 came around Log4j, the high-profile software flaw in a widely used software library that saw millions of global exploit attempts. This reflects not only the vulnerability's profile, but also perhaps the scramble to understand and rapidly defend against the threat. The average number of days for cybersecurity teams to develop knowledge, skills and judgment around Log4j was two – 48 times faster than the average threat intelligence lab.

An analysis against specific threats shows high-profile vulnerabilities see a significantly decreased time to capability.

Tellingly, it was one of the few threat intel labs where defensive, not offensive, skills were a priority for cybersecurity teams. Perhaps just as illuminating is the fact that the fastest human capability ever developed was the ability to use one of OWASP's free tools for determining the impact of Log4j across an enterprise. This was completed nearly 100 times faster than other threat intelligence labs.

The only non-Log4j related capability developed at speed in the top five was from cybersecurity teams looking to quickly understand how attackers used a zero day in Windows Server, for which a proof of concept exploit was publicly available.

Fastest developed human capabilities_2021



Threat groups

Supporting the theory that cybersecurity teams are keen to understand high-profile attacks, the data shows capability development around well-known threat groups is also prioritized. Receiving significant interest from media, research teams, intel feeds and other trusted sources, the development of knowledge, skills and judgment against known nation-state and criminal groups is more rapid.

Capability development for the group behind SolarWinds, for example, was nearly eight times quicker than the average, with most teams having an understanding of the issue within 12 days. The interest in big-name threat actor groups runs throughout all threat intel labs, with the top five in the period analyzed being:

Top five labs
by threat actor groups

1 **UNC2452 (Solarwinds)**
The infamous nation-state group responsible for the SolarWinds compromise

2 **Iranian Threat Groups**
Iranian nation-state attacks have driven recent government warnings to enterprises

3 **FIN 7**
Notorious Russian hacking group charged by the US for crimes against hundreds of companies

4 **Hafnium**
Nation-state group responsible for the 2021 Exchange Server breach

5 **Darkside**
Cyber extortion group tied to the Colonial pipeline attack

Known malware

Considering specific pieces of malware are required for today's advanced attacks, human capability development around these also sees significant usage. Teams have an inherent interest in executing and analyzing emerging malicious software in a safe environment.

In terms of the top five specific pieces of malware focused on by cybersecurity teams, an all-too-familiar story emerges, with the onus being placed firmly on developing the technical knowledge, skills and judgment to defend against ransomware:

Top five specific threats
focused on by cybersecurity teams

1 **Maze**
Sophisticated ransomware actively targeting Windows machines across many industries

2 **Annabelle**
Characterized by ghoulish artwork and an all-encompassing list of targeted processes

3 **WastedLocker**
Evil Corp's customizable ransomware payload targeting organizations globally

4 **Ryuk**
Thought to be run by Eastern-European cartels, victims are targeted in a business-like manner

5 **Sodinokibi**
Ransomware used by the enigmatic REvil ransomware group

The Psychologist's View

Rebecca McKeown /
Dr. John Blythe

There are a number of interesting findings here for those looking to understand how to build human capabilities better:

The tendency for cybersecurity to focus on execution: There are potentially two psychological effects at play here. First, like anyone in a large organization, individuals in cybersecurity teams will be hungry for the praise of their superiors. It may be that they see stopping threats from 'executing' as something directly aligned to this – if they stop the risk, they'll save the day.
Given the choice, they will choose capabilities which achieve this. Second, a cybersecurity space that has made hacking and subverting technology 'cool', execution is the ultimate prize. The so-called 'bandwagon effect' means people become overly focused on such topics, reducing independent thought and negatively impacting decision-making quality.

Suggestions for senior leaders: Ensure a solid balance of capability development by reinforcing the business impact of every part of the attack chain. Teams need to understand the value of every aspect of mitigation, not just 'stopping attacks.' Measure capabilities to ensure an even spread.

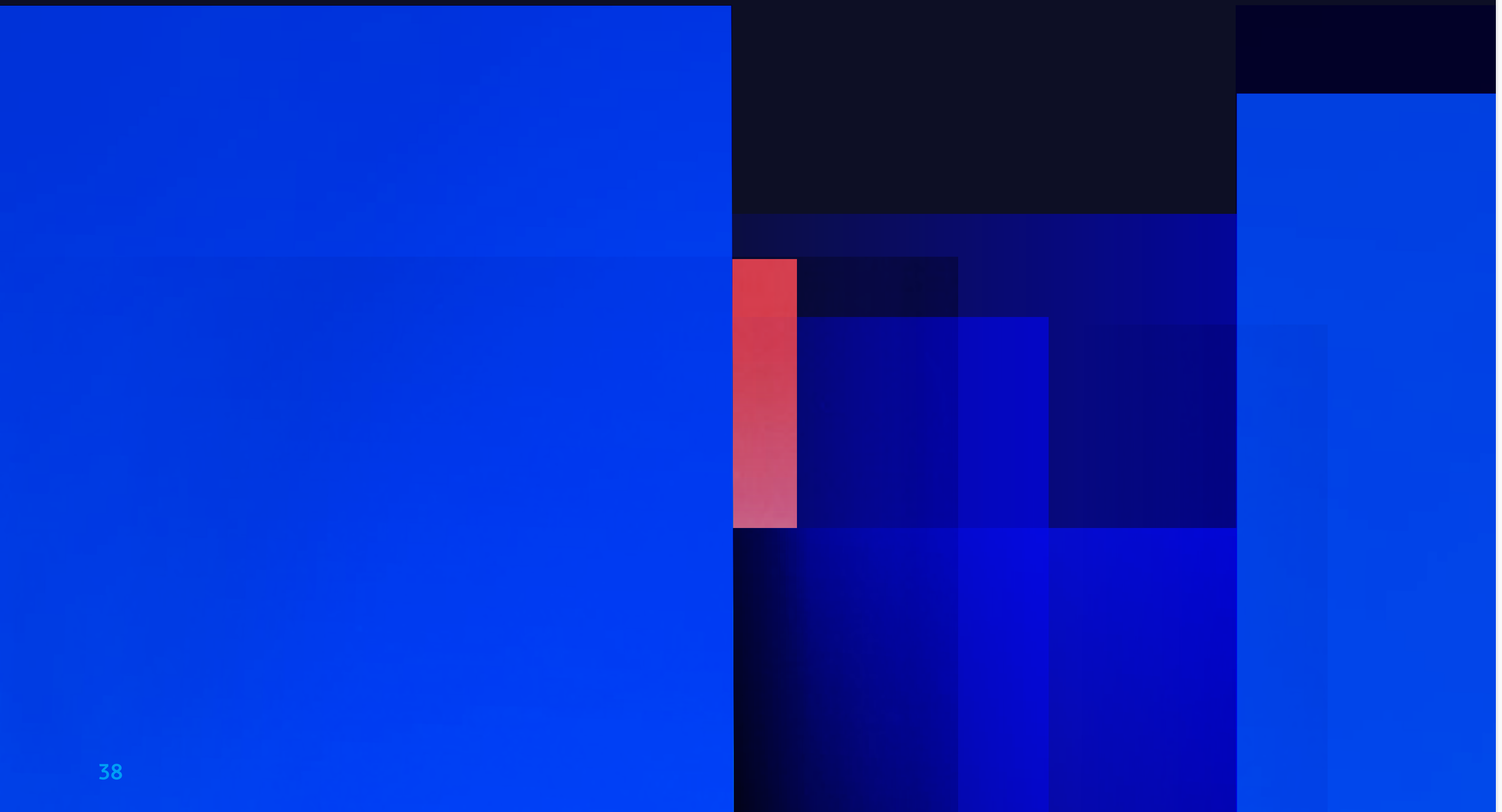
High profile threats: Outside of a need to ensure systems are protected against emerging threats, there may also be a deeper psychological reasoning for the interest in high-profile attacks. The human need to take action is an automatic response hardwired into the way the brain functions. News headlines and full threat intel feeds trigger this impulse. This could cause people to rush in and decision-making quality to deteriorate at speed as the brain makes assumptions and takes shortcuts based on previous experiences. For a cybersecurity team, this could be fatal. As each threat is unique, assumptions could lead to irrelevant decisions that could set mitigation efforts back – or even make them worse.

Suggestions for senior leaders: Those responding to threats need to develop advanced thinking skills called cognitive agility. This is the ability to 'think about thinking', creating distance from the impulse to act and consciously controlling decision-making to challenge automatic responses. Practically, this is a skill built over time by being continually exposed to new but relevant scenarios. Cognitive agility leads to people being open to new perspectives and discarding embedded biases. It also helps develop focus – the ability to discard irrelevant information.

03

Secure applications using human capabilities

Sean Wright_Principal Application Security SME



Introduction

Application security faces challenges from a human capability standpoint. Vulnerabilities in software have directly contributed to the most high-profile security issues of recent times – Log4j and SolarWinds to name but two. Despite this, application security faces cultural headwinds and knowledge gaps in many organizations which strangle human capabilities, ultimately increasing risk.

Baseline

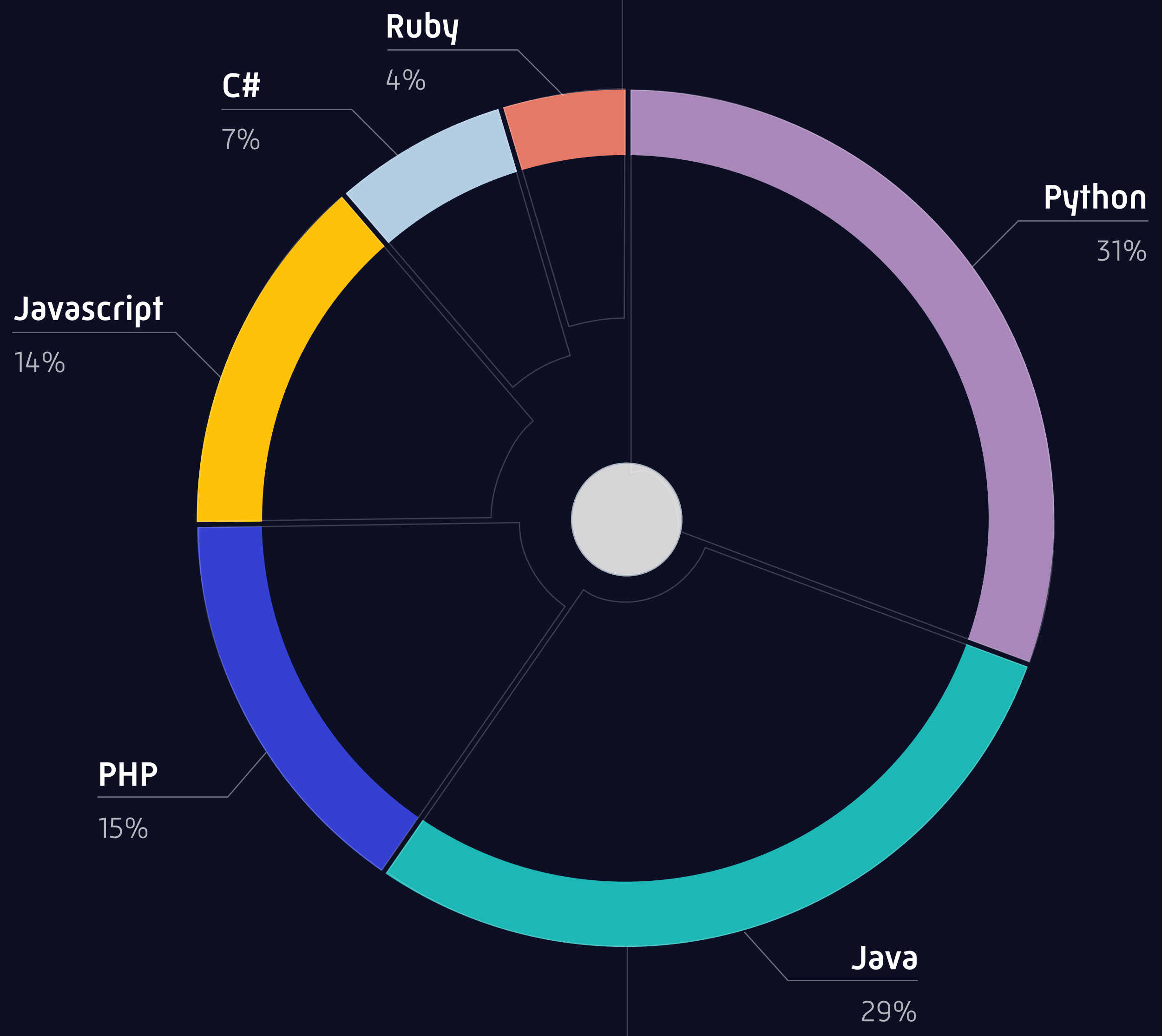
The analysis that follows is based on insights from 43,000 hands-on application security exercises. These simulations were used by 40 enterprise organizations to develop cybersecurity knowledge, skills and judgment amongst development teams in 12 sectors.

Which language do you secure?

As a start point, it is interesting to understand what languages development teams are looking to secure. While this is inherently influenced by the predominant language being used inside each organization, it provides some guidance on where appsec knowledge, skills and judgment lies.

Across the board, organizations are most concerned about securing Python and Java, with around twice the number of appsec skills development labs being undertaken in these languages than the next nearest (PHP). By contrast, Ruby and C# are less popular, with just 4% and 7% of all labs run respectively.

% of total completions

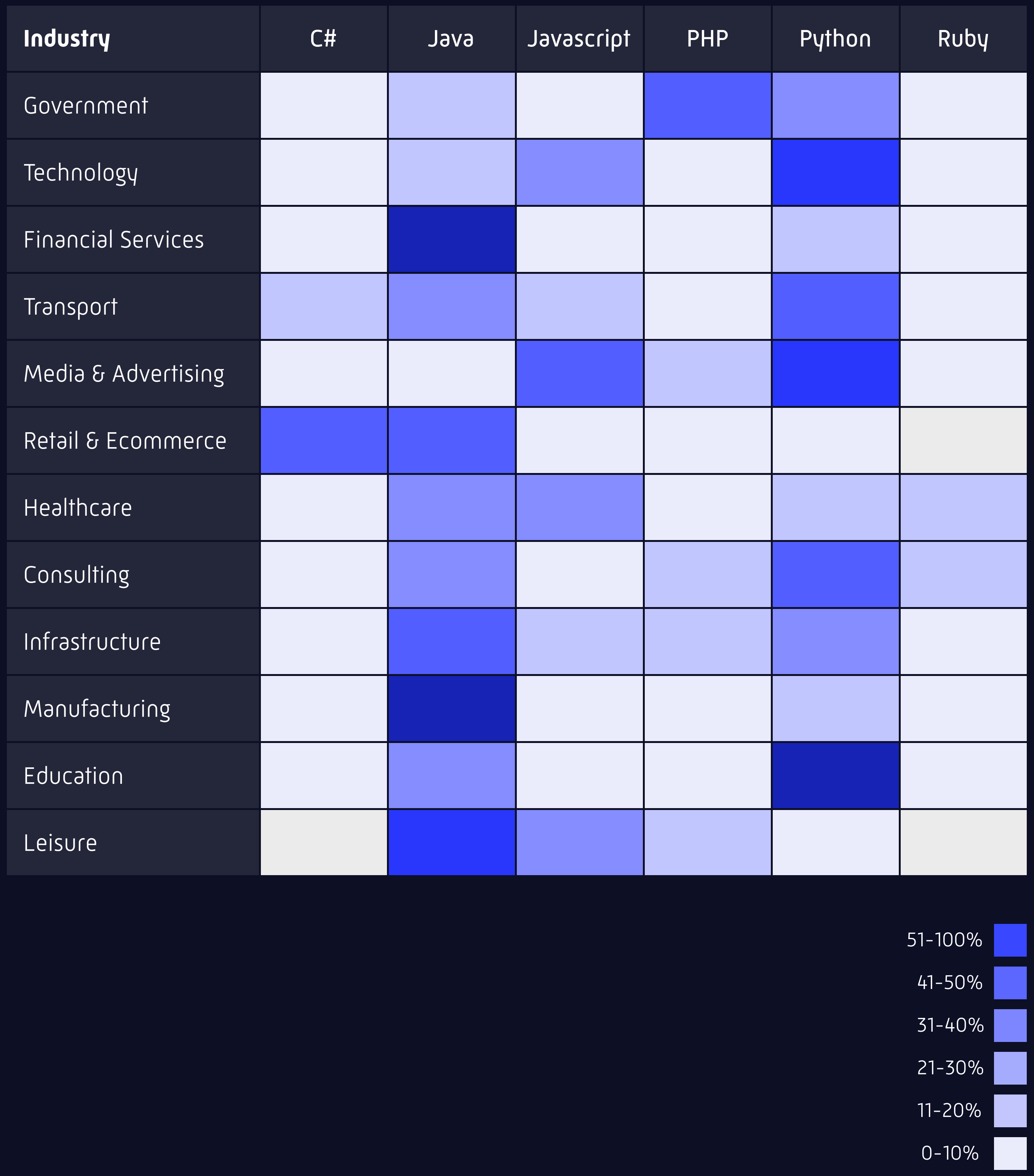


Which language do you secure?

Analyzing by sector

Analyzing by sector goes a bit further towards understanding whether appsec is language focused or dependent on commercial application. Financial services and manufacturing, for example, lean heavily towards Java, with 58% and 62% of all application security skills in this language – over three times the next nearest language (Python). A similar leaning towards PHP in government is also noticeable.

% of total industry



Faster time to capability than cybersecurity

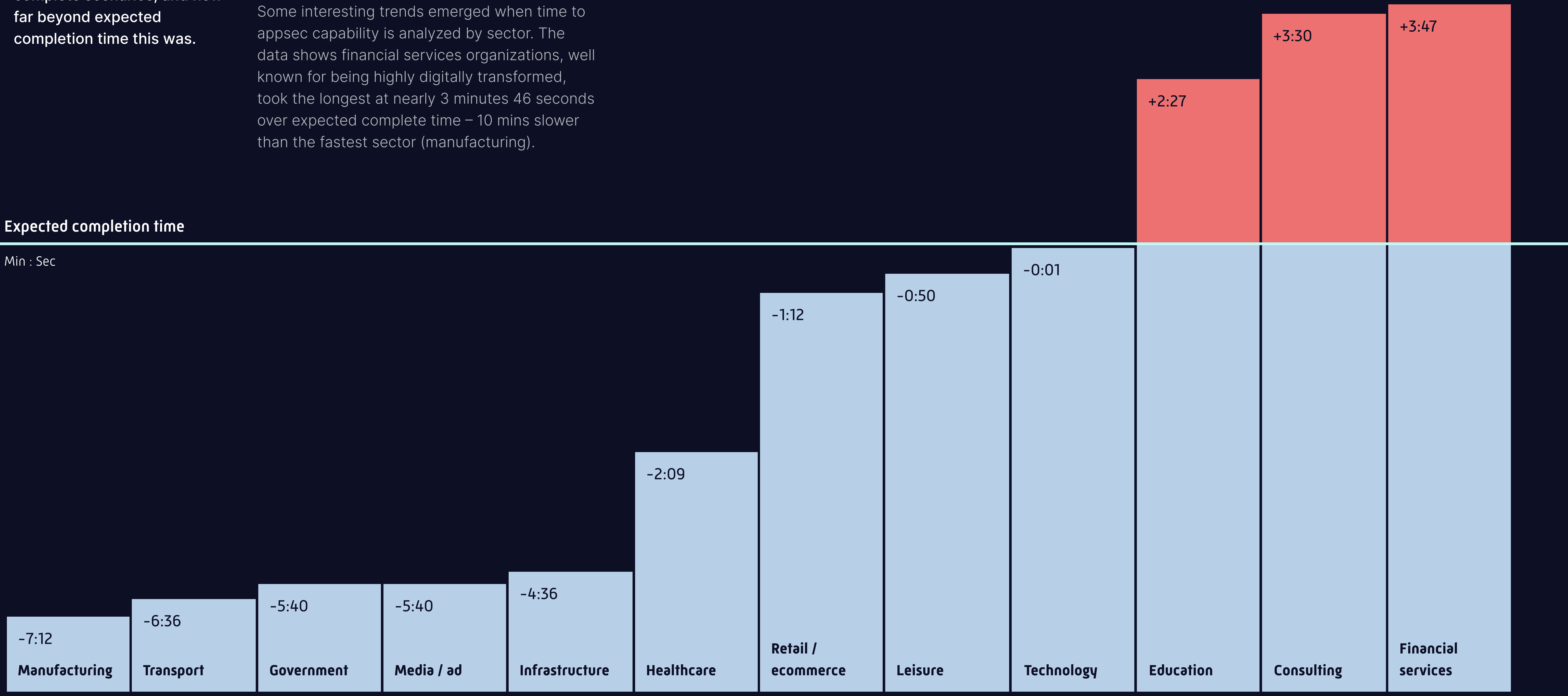
An interesting marker of how efficiently application security knowledge, skills and judgment can be a part of wider resilience strategies is how long it takes to build them. To achieve this, we looked at the time outlay for individual members of the development team to complete scenarios, and how far beyond expected completion time this was.

The data shows that, on average, application security teams develop human cyber capabilities faster than cybersecurity teams. In fact, 78% of all application security skills are developed faster than the expected completion time, in stark contrast to just 11% of cybersecurity labs. The average application security lab is completed 2.5 minutes under the expected complete time, whereas the average time to finish cybersecurity labs is 17 minutes over.

Some interesting trends emerged when time to appsec capability is analyzed by sector. The data shows financial services organizations, well known for being highly digitally transformed, took the longest at nearly 3 minutes 46 seconds over expected complete time – 10 mins slower than the fastest sector (manufacturing).

Counter to Ruby's reputation as a programming language for fast-moving startups, government coders were actually far more efficient at writing secure code than the technology industry in this language. Employees at government organizations developed secure coding skills for Ruby 8 minutes and 10 seconds under time compared to technology companies, which were typically 13 minutes over.

On average, application security teams develop human cyber capabilities faster than cybersecurity teams.



Appsec teams also have an eye on the news

Interrogating the data on the most commonly developed human appsec capabilities by specific attacks shows the same desire as cybersecurity teams to develop skills that are seen as offering protection from an imminent threat.

The top ten application security skills developed are largely either those which are perpetually front of mind for development teams (four out of 10 are XSS and SQL Injections, for example) or those linked to colorful and high-profile attacks. Considering the second most commonly developed human appsec capability is learning about vulnerable libraries – the cause of Log4j – it is fair to say the news agenda also influences appsec skills development.

Top ten human application security capabilities developed

	Language	Capability	OWASP category
1	**Java**	Blind SQL injection	Injection
2	**Java**	Vulnerable library	Vulnerable and outdated components
3	**Java**	Command injection	Injection
4	**Python**	Stored XSS	Injection
5	**Python**	Forced browsing	N/A
6	**Java**	Reflected XSS	Injection
7	**PHP**	Introduction to secure coding	N/A
8	**Python**	Default error pages	Security misconfiguration
9	**Python**	SQL injection	Injection
10	**Python**	Code comments	N/A

Fundamental understanding

As organizations rely on development teams to design security into the heart of connected infrastructure, the fundamentals of application security are critical. With simulations on essential topics such as OWASP's Top Ten vulnerabilities, encryption and secure testing, we thought comparing some data insights would be interesting.

Generally, OWASP labs see a high amount of usage and completion rates and are among the best on the platform, with 95% of all participants going from start to finish. Secure coders building capabilities in North America are particularly keen on OWASP, followed by EMEA and then APAC.

Labs that help users understand how to build encryption into software, by comparison, see a higher bounce rate, suggesting the topic is harder to complete. We could find a clue for why this is in the average completion times of encryption labs. Only two of the 12 sectors analyzed completed skills development labs on encryption under the expected variance time. All the rest were over, some significantly, including education (16 mins 30 seconds) and financial services (10 mins). This could speak to a more complex subject that needs to be given time to mature within development teams.

Despite being a critical part of the software delivery lifecycle, just over 8% of all labs completed were focused on secure testing – the process whereby developers check their code is secure before committing. With these exercises being targeted at testers and QA teams, this is an interesting finding potentially pointing towards either a lack of upskilling amongst these individuals, or a lack of engagement. On average, those exercising secure testing capabilities completed the labs nearly six minutes quicker than expected. Infrastructure companies took longer than most, completing labs on secure testing mostly at the expected time.

OWASP

Completion rate	Variance from expected time
95%	-1.5 mins

Insights

Interestingly, the OWASP category which shot up from fifth to first in the 2021 OWASP Top Ten – Broken Access Control – is one of only two appsec labs which took participants longer than the expected time to complete.

Encryption

Completion rate	Variance from expected time
79%	+5.4 mins

Insights

Devops teams are hungry to understand the basics of encryption. 18 out of the top 20 labs used by devops teams teach fundamental concepts such as Block Ciphers, One-Time Pad and even the Vigenère Cipher used by the Confederate Army.

Testing

Completion rate	Variance from expected time
87%	-5.5 mins

Insights

Of all the application security labs run in the period focused on by this analysis, just over 8% developed secure testing capabilities.

The Psychologist's View

Rebecca McKeown /
Dr. John Blythe

Comparing skills development in appsec teams and cybersecurity teams opens an interesting view for analysis.

Cultural differences with cybersecurity teams bleed into capability development: The data showing that development teams complete labs so much faster than cybersecurity teams is interesting. While speed on its own isn't a marker of effective cyber skills development, it is an interesting insight into the cultural differences between roles and how these affect upskilling. This is backed up with research[2] into application security culture which shows the perceived 'drag' cybersecurity has for developers on an otherwise fast-paced process.

Suggestions for senior leaders: Embrace the desire for developers to upskill at pace by providing them with quick and engaging capability development tasks. Ensure these are ring-fenced from time in the SDLC to bring focus and discourage the idea that they impact application development cycles. In this way, application security becomes a more organic process embedded in the team, as opposed to being perceived as a drag on innovation.

Bias towards high-profile threats: Appsec teams skew capability development towards well known threats in the same way, and for the same reason, cybersecurity teams do. The fact that vulnerable libraries, the cause of Log4j, was so popular, for example, clearly showcases the human need to take action when under threat. It could also be said this points towards the 'bandwagon effect' occurring again.

Suggestions for senior leaders: Remove this bias by encouraging capability development which balances fundamental application security skills such as encryption and testing with higher profile threats. Help teams become aware that while breaking threats are important, they also act as a honeypot for upskilling efforts – basic skills are just as essential.

04

Understanding the cyber knowledge, skills and judgment of tomorrow

Noopur Davis_ Executive Vice President, Chief Information Security and Product Privacy Officer, Comcast Corporation and Comcast Cable

Introduction

The shortage of human cyber capabilities in the global economy is well documented. Regardless of location or industry, there is a dearth of relevant knowledge, skills and judgment in everything from specialist to broader roles.

Baseline

This section seeks to understand the human cyber capabilities of the future by analyzing data from over 22,000 university students, military veterans and members of under-represented groups who use Immersive Labs' free Digital Cyber Academies (DCA) to prepare for a role in cybersecurity. Delivered to over 1,200 academic organizations and charities around the world, the analysis takes into account the abilities developed by users who have completed more than 176,000 labs in total.

Noopur Davis

Executive Vice President, Chief Information Securityand Product Privacy Officer, Comcast Corporation and Comcast Cable

Ensuring a flow of future talent has become bigger than just the cybersecurity sector. Everyone from policy-makers to academic institutions are tackling the task to ensure that, as the institutions which make up modern life become irrevocably entwined with connected infrastructure, they cannot be abused by those with malicious intent. As with any emerging problem, the best approach is hotly debated, with the underlying issue being how to create and prove human capabilities at scale.

As part of this, it's critical to have a diverse set of role models to help inspire the next generation into choosing cybersecurity as their next job move. Not only does this provide career pathways to those who might not have had the opportunity previously, it also injects diversity of thought into defensive teams – something critical to beating attackers.

The grassroots work being done by Immersive Labs is important and valuable. Providing access to free foundational cybersecurity skills development and then matching this directly to organizational need, is a promising mix of idealism and pragmatism. Part of being resilient means matching candidate capabilities to direct need, whatever the pace, rather than focusing only on certificates and job tenure. Being able to measure candidates' abilities to do the task at hand is an important part of this work.

Ensuring a flow of future talent has become bigger than just the cybersecurity sector.

A lack of application

First, it is important to understand what topics the cyber talent of tomorrow is engaging with. While 'numbers of labs done' might be a rudimentary way of doing this, we felt that understanding engagement is more important. Therefore, we calculated an engagement score by analyzing how many users completed labs in a range of cybersecurity skills categories once started. These categories ranged from understanding the fundamentals to more specific cybersecurity skills brackets such as offensive skills, malware and reverse engineering.

This analysis shows the importance of basic skills as a gateway into the industry. Engagement rates for content covering the fundamentals (core concepts such as awareness and management, risk and compliance) are more than double that of those wanting to focus on specific skills.

Engagement score *by category*

	Avg number of labs completed
Fundamentals	15.9
Offensive	6.9
Defensive	5.7
Tools	4
Cloud Security	3.8
Malware & Reverse Engineering	2.3
Challenges & Scenarios	2.1
Cyber Threat Intelligence	1.9
Application Security	1.8

Mirroring the trend with professional cybersecurity users

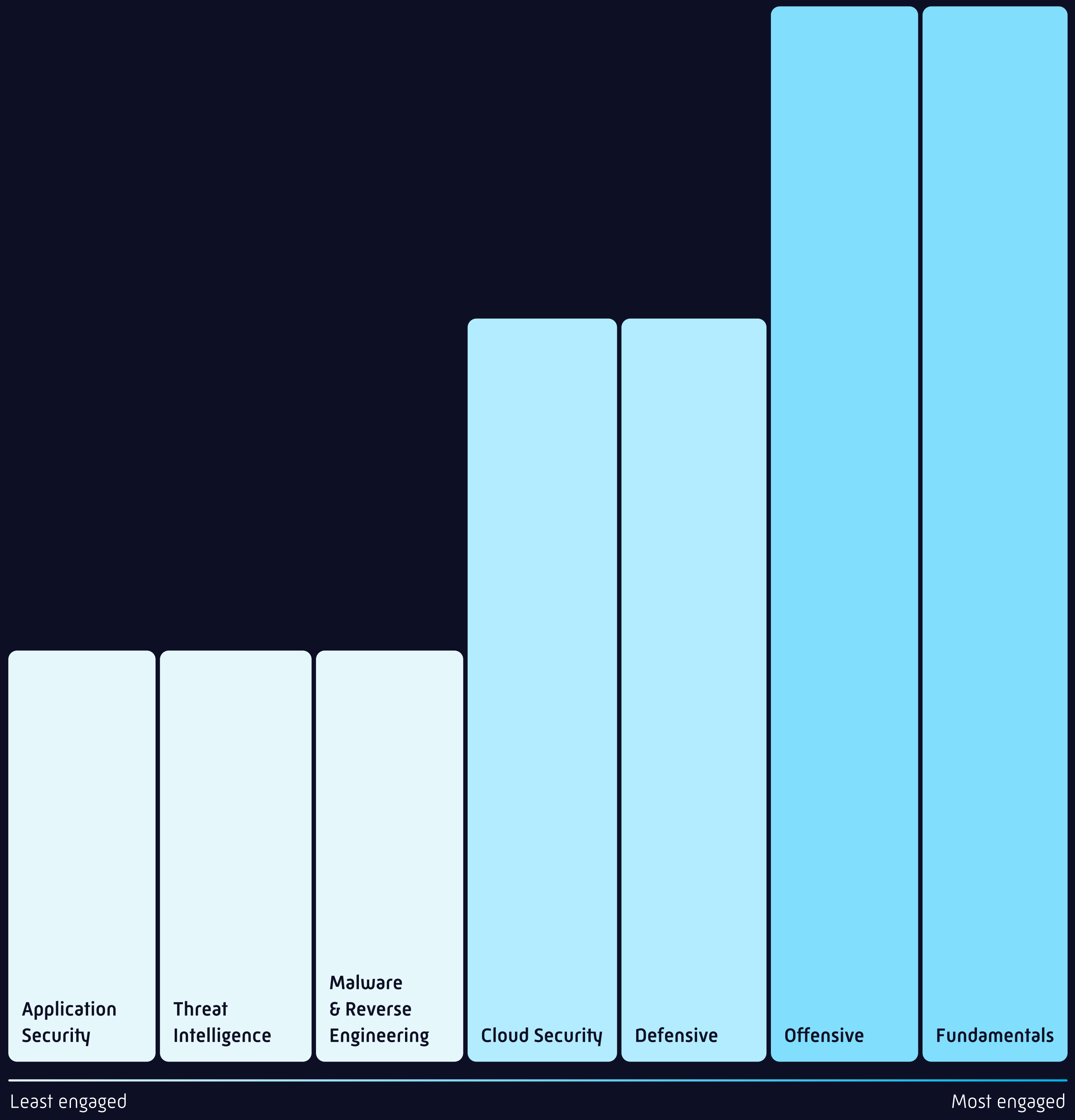
The highest engagement rates for up-and-coming cyber talent outside of the basics is Red Team skills, with an average engagement rate of 6.9. In fact, offensive skills make up around 15% of all labs completed. Infrastructure hacking and reconnaissance saw the highest engagement rates of all the capabilities developed by tomorrow's infosec teams, again mirroring the trend seen earlier for cybersecurity professionals to be focused on the initial point of incursion. These two capabilities made up 73% of all offensive skills developed in total.

Pointing towards a potential future problem for the industry, application security skills have, by far, the lowest engagement, with only a quarter of the rate of offensive cybersecurity skills. In fact, only 0.5% of all of the labs completed were application security specific. With insecure software being the cause of some of the largest breaches of 2021, this highlights a burgeoning future problem for the industry.

Talent of tomorrow and enterprises engage with the same capabilities

A sign the cybersecurity teams of tomorrow are engaging with market need, or perhaps a sign of an innate bias in cybersecurity talent in general, is the uncanny similarities in the graphic below. It shows that those set to enter the industry are engaging with exactly the same topics used by enterprise cybersecurity teams in the Immersive Labs platform.

Talent of tomorrow and enterprises shared results



Clouds on the horizon

Finally, we thought it might be interesting to pit the up-and-comers against our enterprise users, who are professionals in cybersecurity. We did this by directly comparing time and accuracy on a number of identical labs used by both groups.

As expected, the professionals completed exercises with greater accuracy and pace in almost all areas. However, perhaps as a sign of an emerging human cyber capability, the talent of tomorrow edges cybersecurity professionals slightly on one of the most important newer skills: securing cloud environments. Students completed cloud security tasks 34 seconds quicker on average.

Once again, the data pointed towards a potential lack of understanding of application security for the people who are set to feed the cyber workforce of the future. Building secure code was where there was the greatest difference in accuracy between users of the free Digital Cyber Academies and enterprise users. The talent of tomorrow also took 24 mins and 30 seconds to complete these labs on average, around 1 minute and 30 seconds slower than enterprise users.

Interestingly, the performance of both groups is closely matched when it comes to fundamental cybersecurity concepts, even though professional users have obviously been in the space for a sustained period of time. This suggests that the core concepts of cybersecurity are universal.

> While the accuracy of completion of these labs is even, students completed cloud security tasks 34 seconds quicker on average.

Accuracy

Shown as %

Category	Talent of tomorrow	Enterprise cybersecurity	Difference from professionals
Application Security	78.0	82.0	4.0
Cloud Security	85.3	89.0	3.7
Tools	77.6	81.2	3.6
Cyber Threat Intelligence	79.7	83.3	3.6
Defensive	80.4	83.6	3.2
Fundamentals	89.4	92.0	2.6
Offensive	82	84.3	2.3
Challenges & Scenarios	80.7	82.2	1.6
Malware & Reverse Engineering	75.4	76.1	0.7

Time

Min:Sec

Category	Talent of tomorrow	Enterprise cybersecurity	Difference (mins)
Application Security	24:30	22:59	01:31
Cloud Security	11:27	12.01	-00:34
Tools	25:14	25:10	00:08
Cyber Threat Intelligence	20:56	18:12	02:44
Defensive	22:00	21:30	00:30
Fundamentals	11:52	11:56	-00:04
Offensive	19:29	17:55	01:34
Challenges & Scenarios	20:20	22:28	-02:08
Malware & Reverse Engineering	18:27	19:22	-00:55

The Psychologist's View

Rebecca McKeown /
Dr. John Blythe

Trying to understand the way up-and-coming cybersecurity talent develops human capabilities could be crucial for government organizations and others seeking to increase the flow of capabilities into the industry. Understanding the trends in the above data could be important in optimizing skills development to ensure initial participation – and continued engagement – in two key ways:

1 **The appeal of the fundamentals:** While the keenness shown towards learning the fundamentals is, on the face of it, unsurprising, it could be a powerful attractor mechanism for organizations seeking to build talent at scale.

With data showing a marked enthusiasm for basic skills acquisition, there is an opportunity here to create a clear pathway into the industry for potential talent. Such capabilities can be framed as the building blocks for a future career and, with direction, more specialist expertise built over time.

2 **Maintaining involvement:** Engagement is obviously important for early-stage capability development. In short, it stops potentially skilled workforce members dropping out early. The data tallies with what is seen in professional teams: offensive topics grasp the imagination and see a high level of engagement.

This should be seized as an opportunity. Meaningful and relevant skills development interactions which 'actively stimulate the learner's mind to do those things that improve ability and readiness to perform effectively'[3] are critical. Outside of this showing a need to use offensive skills acquisition as a recruitment and retention tool, it also speaks to the value of gamification, puzzles and other hands-on challenges.

[3] Allen, M. W. (2003). I Had No Idea: How to Build Creative e-Learning Experiences. Educational Technology, 43(6), 15–20

05

Conclusions

James Hadley

CEO of Immersive Labs

True cyber resilience is difficult. A continual slew of compromised networks, organizations being held to ransom and supply chain attacks is testament to this.

However, resilience now has greater significance than ever before in the cybersecurity lexicon. While the ability to protect and defend is still important, it is not enough. Addressing today's all-encompassing, continually evolving threat requires cyber risk strategies that are deeply embedded across the entire organization, while also agile. Cyber resilience is no longer just about cybersecurity teams being kept relevant and ready to address risk – it's about the entire workforce.

Achieving this requires a continual cycle of cyber knowledge, skills and judgment development across the entire organization. Technological countermeasures may be good at identifying and collecting data on cyber threats, but human capabilities take the actions that reduce risk. For this reason, exercising to gather evidence, and then using these insights to equip teams with relevant skills, is critical to ongoing resilience.

It is my hope the insights included in this report will open up a wider discussion around the value of workforce capabilities in cybersecurity and the possibility for applying them more strategically. Traditionally, their seemingly intangible nature has seen them playing distant second cousin to technology. We believe it is time to change this. By acting as measurable, accountable assets we believe the potential for optimized cyber workforces has only just begun. Only together can we become more resilient.

All Together. More Resilient.

immersivelabs.com / @immersivelabs