savannah

The Cyber Security Leadership Crisis

CYBER SECURITY LEADERS ARE FACING A PERFECT STORM

Global challenges, including the cost-of-living crisis, are driving more susceptibility to bribery, increased threats from organised gangs or government-backed bad actors, deep fakes, and ChatGPT for targeted phishing. These are, on the one hand, creating intense demand for Security leaders' skills and, on the other, creating a fiercely difficult environment in which to operate.

The shortage of cyber security professionals is an enormous threat to organisations, their business continuity, supply chains and existence. Organisations with unfilled roles are more likely to face higher costs after a breach. IBM have estimated that the United Kingdom is now the fourth costliest country for data breaches at an average of $5.05 million, up from $ 4.67 million. Germany follows closely behind, with average costs of $4.85m, France $4.34m and Italy $3.74m. Scandinavia is the lowest at $2.08m.

Savannah's analysis[1] of cyber security professionals, specifically CISOs, (Chief Information Security Officers), identified that CISOs are starting in positions younger and staying for less time. The current median tenure for CISOs is under three years. The confluence of greater pressure from senior business leaders, a more complex digital landscape, and the hydra of external threats is leading to burnout and a significant impact on mental health. All of which is exacerbated by the difficulties in hiring and retaining talent, which is further compounded by more

IN **2022** THERE WERE AN ESTIMATED **3.5 MILLION** VACANT SECURITY ROLES.

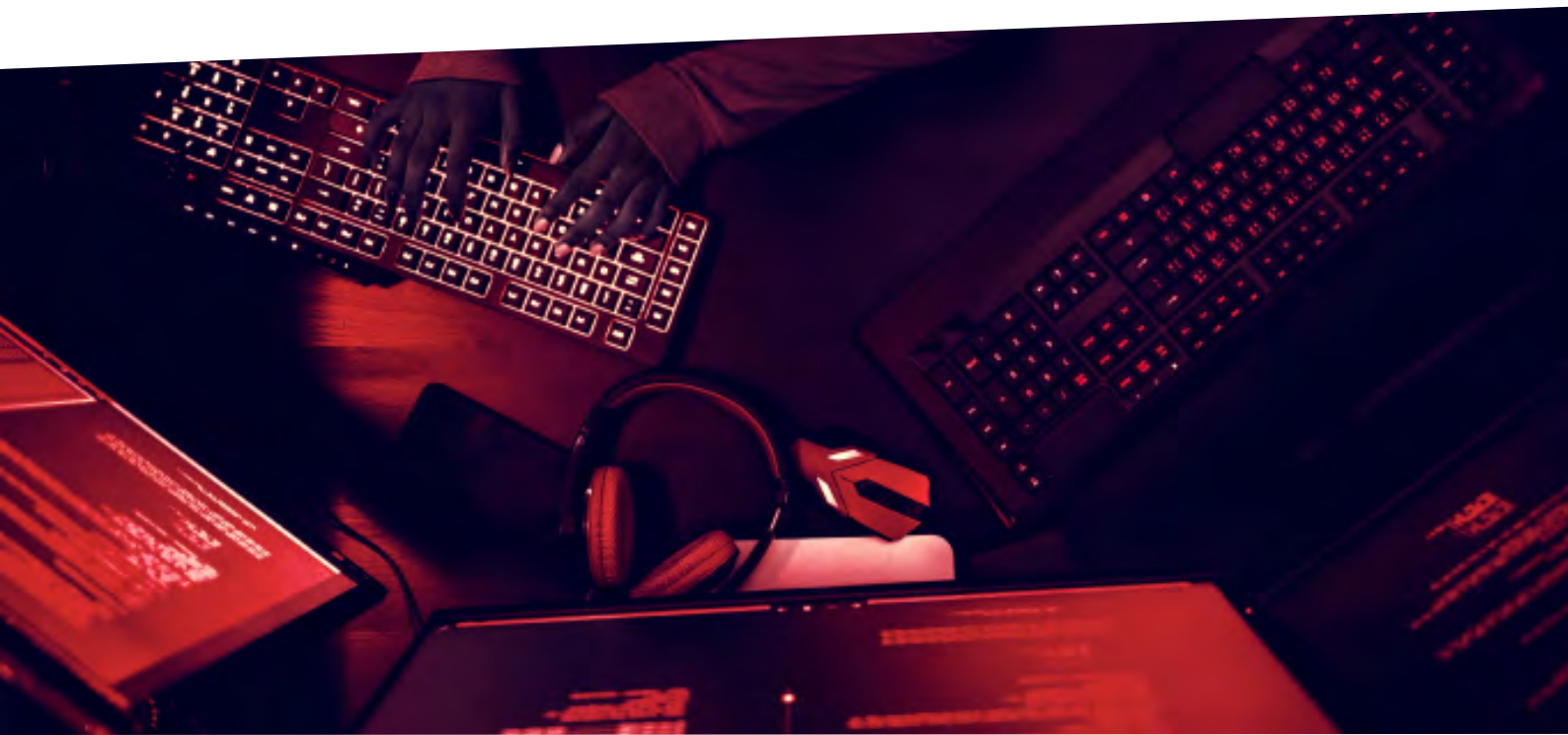
[1]Savannah Group, using its proprietary AI technology MapX, analysed a global sample of 200 CISOs

CISOs resigning with no intention of returning.

An additional challenge for CISOs is their increasingly client-facing role and responsibilities, particularly in organisations that hold a significant place within broader ecosystems. Indirect cyber-attacks have increased from 44% to 61% (IBM Security), and with companies regarded only as strong as their most vulnerable link, CISOs offering assurance to external parties is a necessity. Leaders are justifiably becoming more concerned about the weaknesses in their own supply chains, and those of third-party partnerships. The nature of these challenges means that CISOs must progressively become more externally focused and adept at selling how resilient their business is to CEOs, the board and other stakeholders.

WE ARE AT A **CROSSROADS**, A POINT AT WHICH CYBER RESILIENCE HAS BECOME THE DEFINING MANDATE OF OUR TIME – **BEYOND FOUNDATIONAL SECURITY CONTROLS** – TO ANTICIPATE FUTURE THREATS, WITHSTAND, RECOVER FROM CYBERATTACKS, AND ADAPT TO LIKELY FUTURE DIGITAL SHOCK

(World Economic Forum,



THE CHANGING SECURITY LANDSCAPE

With the increasing prevalence of more sophisticated cyber breaches and organisations becoming more dependent on digital technologies, cyber-criminals are utilising every avenue available to exploit vulnerabilities. They are more agile than ever, quickly adapting to new technologies and tailoring them to their needs, whilst cooperating with each other to create sustained attacks. More traditional criminal gangs are now going 'digital', procuring the services of 'Cyber Criminals as a Service'.

There have been instances of malicious hacks used to change share prices and Deep Fake audio and video being manipulated to make false business announcements to control financial markets.

Ransomware attacks are more frequent, causing an estimated €18 billion worth of damage in 2021 – a 57-fold increase since 2021 (EU Agency for Cybersecurity, 2021). In 2022, there was an average of 270 attacks per organisation, an increase of 31% over 2021.

Phishing attacks jumped by 61% in 2022, with an estimated 255 million attacks detected (Slash-Next). Almost 60% of the breaches across EMEA included the exploitation of human error and social engineering.

Insider threats are growing in prevalence, partly driven by the cost-of-living crisis. At the analogue end of the cyber threat spectrum, the use of stolen or compromised credentials remains the most common cause of a data breach and the longest to identify and contain, with an average of 243 days and 84 days respectively (IBM Security).

During 2020/21, with large swathes of the population shifting to remote work, there was a marked decrease in instances of malware. This trend reversed rapidly by the end of 2021, as people started returning to their offices (European Parliament).

According to Accenture's 2021 State of Cybersecurity Resilience report, there are currently 1,900 distinct active hacking groups that employed 514 new malware strains and an estimated 100 different strains of ransomware currently active.

According to Enisa (European Union Agency for Cybersecurity), there were more **Internet-of-Things (IoT) attacks in the first six months of 2022** than in the previous four years.

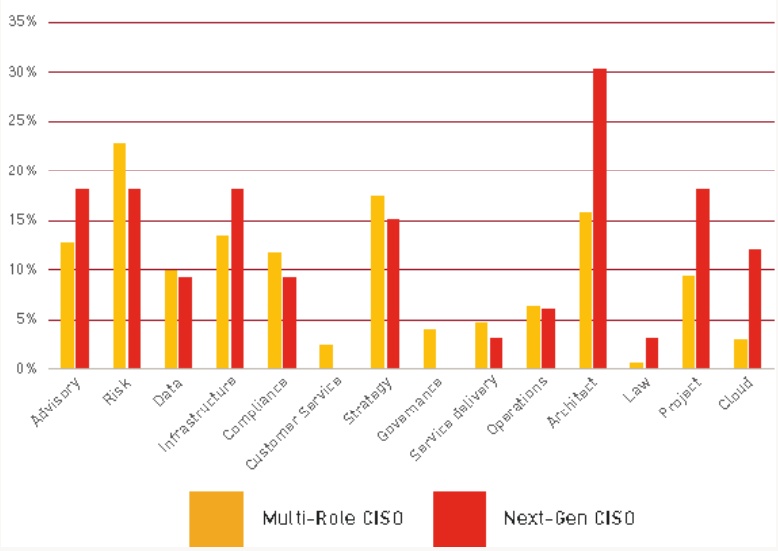
QUANTUM COMPUTING - THE STANDARD 40BIT PASSWORD WILL BE CRACKED IN **MILLISECONDS**. SECURITY IN A QUANTUM PROCESSING WORLD WILL FURTHER SHIFT THE PARADIGM FROM BUILDING **CYBER SECURITY** TO BUILDING **CYBER RESILIENCE**

THE EVOLVING SECURITY TALENT LANDSCAPE

We used Savannah Group's proprietary AI technology, **MapX**, to analyse the backgrounds and pathways of over 200 CISOs. We compared established, multi-role individuals with the next generation of CISOs who had just taken their first role. Our research covered privately owned and listed large businesses across UK, US, Europe and Asia.

Unsurprisingly, noticeable differences between the two populations surfaced, no doubt because of the significant evolution of the CISO role over the last few years:

- **First time CISOs have a higher rate of emerging from a technical pathway,** with Architecture, Cloud and Infrastructure being the more common gateways. Conversely, established CISOs, who have had multiple roles, have a greater representation from Governance, Risk and Compliance (GRC).



Multi-role vs Next-gen CISOs

We discovered that more established multi-role CISOs typically had experience in **Risk, Strategy**, and **Compliance**, which are historically common specialisations in financial firms, whereas the new generation of CISOs who have landed their first roles in the last three years have more technical experience in areas such as **IT architecture**, **Cloud**, and **IT infrastructure**.

Our Interpretation: This was particularly interesting, as we felt it indicates where Security is deemed to sit within the organisation. Sitting within Technology tends to result in a reporting line into the CIO, further up into the COO or CFO and then into the board. It is a widely held belief within the CISO community that the CISO should sit outside of Technology and report directly to the ExCo (Executive Committee). This maintains impartiality and mitigates undue pressure on the CISO to align with the CIO.

Sitting apart from Technology will also ensure that the role is somewhat protected from cost-cutting measures focused on the broader Technology teams.

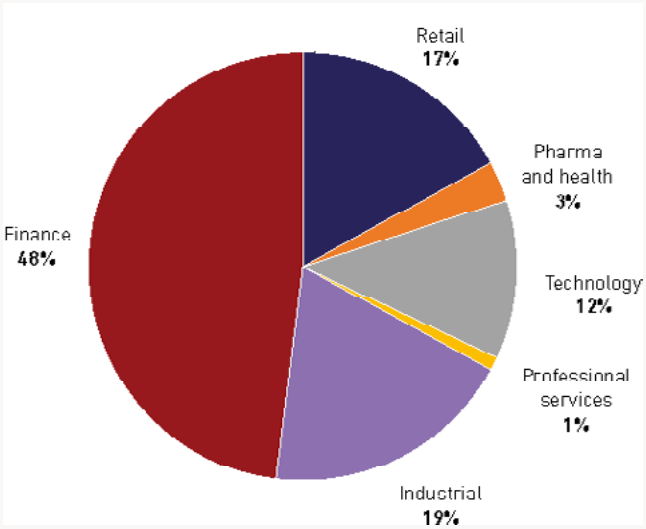
- **Next generation CISOs are also getting younger.** Today it takes just 19 years of experience on average before an individual steps into their first CISO role, whereas historically, this figure has been closer to 23 years.

Our Interpretation: We believe this shows that Security is now a viable career path which is allowing candidates to achieve their first role of CISO four years sooner. It can also mean there are more CISO opportunities for people, whereas before there were fewer roles and more candidates.

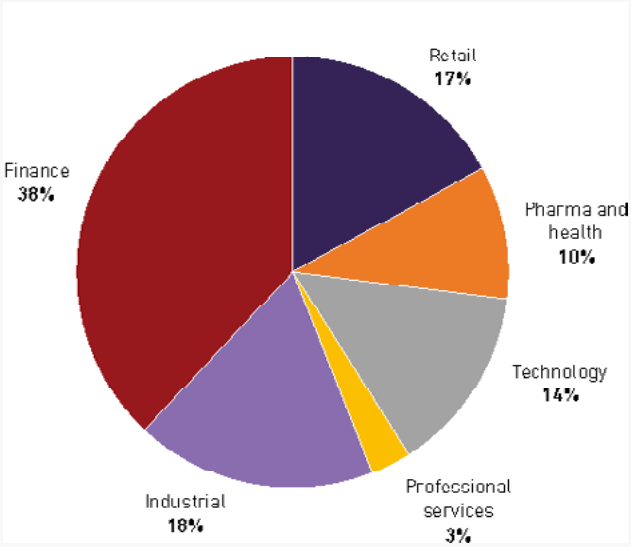
Since Steve Katz became the first CISO in 1995 at CITI Group, the Financial Services sector has historically dominated the demand for security talent. Our research shows that of those CISOs who have had multiple roles, **48% started their careers within Finance and Banking.** This drops to 38% for those who are in their first CISO role now.

With a broader range of sectors and organisations holding more critical data and being susceptible to debilitating attacks, such as the 2017 NotPetya ransomware attack, the role of the CISO has proliferated. The largest increase in demand and growth is within Pharma and Health, where we have seen a 7% increase in CISOs beginning their careers in this area.

CISOs' previous industry



CISOs' current industries



Many CISOs historically started their careers in Finance and Banking (**48%**), however have moved into other sectors, such as Professional Services or Pharma and Health.

ALL ORGANISATIONS IN THE **FORTUNE 500** AND THE **FTSE 100** NOW HAVE CISOs

BUILDING SECURITY LEADERSHIP RESILIENCE

While the candidate market is more competitive, we found that most organisations still hire CISOs from outside, rather than promote them internally. Of the 431 CISO hires that were analysed in this study, an **internal successor was selected in only 35% of cases.** This brings into question how organisations can build resilience and succession planning into their security teams.

With 3.5 million vacancies, burnout and stress impacting those already in these critical leadership roles, how do business leaders protect the people who are protecting them?

We offer 10 considerations for ensuring your business is protected from the security leadership crisis:

1. **Diagnose your organisation's unique talent requirements.** Do you have a CISO on your board? Do you know the right organisational structure of cyber skills to protect the specific requirements of your business?
2. **Focus on retention, development, and succession planning.** Be aware of rising salaries and ensure adequate compensation and incentives.
3. **Proactively develop an active cyber talent pipeline.**This will help mitigate the risks posed by losses that might occur.
4. **Think about gender diversity.** Currently 25% of all security leaders are women, with this expected to go up to 30% in the next few years.
5. **Drive initiatives for organic growth and inclusive hiring.** How are you attracting talent? Qualities attributed to certain neurodiverse groups are well suited to careers in Security, so it pays to ensure that your wording and approach are inclusive.
6. **Align your HR processes.** This will enable rapid hiring and onboarding of talent.
7. **Define urgency and timeline.** What cyber skills do you need to access quickly to guard against reputational or other risks? Build relationships with external partners who can deliver quality leaders at pace.
8. **Benchmark your internal succession candidates** against the external market, based on the previously defined set of expertise and experience.
9. **Build reporting lines for transparency and trust.** Who does your CISO report to? Is this the best set up? The CISO should have direct lines of communication to the board and have built up relationships and trust.
10. **Think outside the box.** Consider looking at different pathways and adjacent sectors, roles and profiles for future talent. Look beyond Technology.

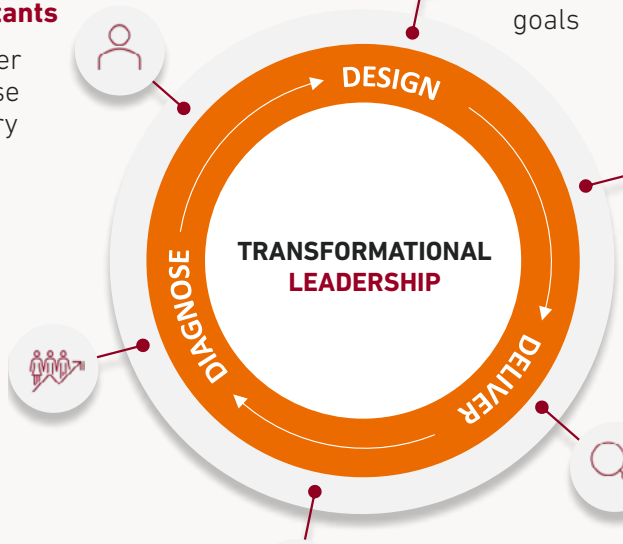
ABOUT SAVANNAH GROUP

Talent Mapping

Know the pool of talent that exists necessary to achieving your company's goals

Transformation Consultants

Matching you with Top tier consultants who diagnose how to tackle a necessary transformation



Succession Planning

Benchmarking successors against potential external candidates

Talent Strategy

Answering the talent implications of your business strategy

Executive Search

Delivering transformational leaders

Interim Management

Deploying proven executives, at pace

A unique combination of data analytics and knowledge insight

An innovative team of trusted leadership advisors

Enhanced by revolutionary **AI technology**

Reducing the limitations imposed by geography, sector, tradition or bias

PRIMARY CONTACT

kbletso@savannah-group.com

Kersty Bletso
Partner

Kersty works closely as a trusted advisor to organisations globally, delivering technology leaders who enable organisational transformation through digital, technology and data. She works across all sectors across the UK, Europe and Canada in listed, privately owned, and Private Equity backed businesses.

She has an extensive track record of senior interim Digital & Technology and CIO Advisory appointments.

Kersty graduated with an MBA from the University of Leeds, a Post Graduate Diploma from UWE and a BSc from the University of Southampton, before starting her career in executive search.

An advocate for greater diversity and inclusion, Kersty is passionate about her relationship with Tech She Can and actively supports women looking to move into an executive interim, fractional or NED career.

TECH & DIGITAL LEADERSHIP PRACTICE

Alex Langridge
Partner
alangridge@savannah-group.com

Sam Sullivan
Principal
SSullivan@savannah-group.com

George Balfour
Principal
gbalfour@savannah-group.com

Daniel Yeates
Associate Partner
dyeates@savannah-group.com

Nick Davies
Partner
ndavies@savannah-group.com

CONTRIBUTORS

Alex Martin
Managing Partner
amartin@savannah-group.com

James Davies-Love
Principal
jdavies@savannah-group.com

Rebecca Walker
Senior Research Associate
rwalker@savannah-group.com

Cara Hirst
Research Analyst
chirst@savannah-group.com

Heather Walpole
Research Analyst
hwalpole@savannah-group.com

Kersty Bletso
Partner
kbletso@savannah-group.com

Savannah is a **next generation** executive search and leadership consulting firm.

Our solutions are **diagnosed**, **designed** and **delivered** by a team of experts in executive search, interim management, talent intelligence and transformation consulting.

Our team, enhanced by Savannah's revolutionary **AI-powered** technologies, collaborate to bring competitive advantage through transformational leadership.

www.savannah-group.com

savannah