ESR
Executive Search Review
A HUNT SCANLON MEDIA PUBLICATION No. 1 2023

CYBER TECHNOLOGY RECRUITING SPECIAL ISSUE

Lead Story: Heightened Demand for Cybersecurity Leaders Keeps Executive Recruiters Busy 1
Ranking: Hunt Scanlon Cyber Technology Top 40 6
Spotlight: A Look Inside the Competitive Market For Cyber Experts 7

Heightened Demand for Cybersecurity Leaders Keeps Executive Recruiters Busy

Increasingly, organizations of all sizes are awakening to the perils posed by cyberattacks. For years, many groups tried to ignore the problem, dismissing cybersecurity as a concern only for the biggest, most high-profile entities, be they government or corporate. These days, more groups are coming to understand how ruinous such intrusions could be. And cyberattacks show no signs of abating.

A report last year from **Accenture**, in fact, said the threat is only growing, with an average of 270 attacks per company, up 31 percent from 2020. A report from **McKinsey & Company**, meanwhile, projects that damage from cyberattacks will amount to about $10.5 trillion annually by 2025, a 300 percent increase from 2015 levels. Globally, organizations spent close to $150 billion for cyber protection last year, a number that's growing by 12.4 percent each year. The global cybersecurity total addressable market could eventually grow to as much as $2 trillion, said the management consulting firm.

Attacks from state supported operators, cybercriminals, business competitors, and even lone individuals have the potential to wreak havoc on businesses. Beyond the financial woes, there is the possibility of damage to reputation and trust, shutdowns, harm to the potential sale of a business, lawsuits, even legal penalties that can leave a company reeling. And when the U.S. government is the one under siege the concern only escalates. All of this has led to a dramatic rise in the demand for cybersecurity executives and search firms in this sector continuing to grow.

Globally, there is a severe talent shortage in the cybersecurity job market. The World Economic Forum (WEF) recently reported a shortage of 3 million cybersecurity professionals around the globe. The lack of cybersecurity experts has left many businesses in a tight spot, according to new report from **TriSearch's** Travis Thomas. The National Center for Education Statistics (NCES) says that companies now see cybersecurity as a mission-critical task, so the demand for cybersecurity professionals is growing faster.

"The lack of cybersecurity professionals has led to various issues, such as an increase in malicious breaches and the theft of personal and financial information," said Mr. Thomas. "The nation's digital and cyberinfrastructure, including its economic, utility, and transportation networks, is under threat, and the situation appears to worsen by the day. Cloud security, application security, and security assessment/investigations are the top three technological domains most impacted by a cybersecurity skills shortage. When there aren't enough people with these skills, employers must pay more for them."

BY THE NUMBERS

There will be **3.5 million** open positions...

...in cybersecurity by **2025** due to the global workforce shortage.

Source: Cybersecurity Magazine

As technology becomes more digitally connected, the need for cybersecurity specialists will increase in the coming years, according to Mr. Thomas. "Security threats will grow in parallel with the Internet of Things and cloud computing," he said. "As a result, the demand for expertise to tackle these issues will also surge. Managing cybersecurity is important, and employers need to look for people with experience and a good track record."

Rapidly Growing Market

The need for cybersecurity professionals has been growing rapidly, even faster than companies can hire – and that demand is expected to continue. "With massive industry growth comes the need for more trained cybersecurity professionals," said Jamie Javorsky regional president- technology search and staffing at **StevenDouglas**. "Organizations are challenged in hiring cybersecurity experts who are equipped with the skills to defend the complex attack surface, like the cloud, and can operate the new technologies that are being implemented daily."

"Companies continue to hunt for cyber talent, but many of these jobs require credentials, certifications, or a master's degree in the field," Mr. Javorsky said. "There are simply not enough people in cybersecurity with the skills to handle *(cont'd. to page 2)*

Copyright 2022 Hunt Scanlon Media, LLC All rights reserved.

CYBER RECRUITING SEARCH NEWS

Xxxxxx

Stockholm, Sweden-based executive search firm **Mercuri Urval (MU)** recently added Stephen Spagnuolo to build and lead its cybersecurity Americas practice. "Information and cybersecurity is a priority for CEOs and boards, and it's fair to say will remain so for many years to come. We are delighted to welcome Stephen to further strengthen our advisory expertise in this essential area," said CEO Richard Moore. Mr. Spagnuolo is splitting his time between the firm's newly launched metro New York and heritage Washington, D.C. offices. He will contribute to the firm's science-based solutions – executive search, assessment, and advisory – to corporates, PE/VC backed domain cyber, and fintech companies, as well as professional services firms and consultancies, across the U.S. and Canada and in collaboration with Mercuri Urval partners across Europe and Asia-Pacific regions.

"I first met Stephen over 10 years ago when I initially tried to recruit him," said Darcie Murray, senior vice president and head of the Americas for Mercuri Urval. "The timing wasn't quite right then; but the positive reaction I had toward Stephen's track record, expert knowledge, and values stuck, and I am delighted we will finally have the opportunity to work together to further strengthen our cyber and digital search capability. Sometimes it's not only about being in the right place at the right time, but also the right firm."

the new threat landscape and lack of certified professionals that companies are seeking. Bottom line the demand remains high, and qualified talent pool low. And while cybersecurity professionals can potentially earn high salaries, the pay scale is all over the map and many companies haven't positioned themselves correctly for recruiting and retaining the right talent."

Cybersecurity is a crucial part of all businesses, particularly given the advancements of today's payment platforms and ever-increasing cloud-based data storage, leaving them exposed to threats and cyber-attacks, according to Mr. Javorsky. "Additionally new technology innovation is in rapid deployment including the evolvement of mobile/artificial intelligence/machine learning tools/ Web 3.0/Meta, thus resulting in companies' enablement to keep up in this new era to protect the organizations exposure to data/ financial attacks and breaches," he said.

Mr. Javorsky also notes that as the technology security ecosystem evolves and becomes ever more advanced and intelligent, the demand for these top executives at this strategic level has never been higher. "Companies are unable to ensure that their internal systems will remain protected, meanwhile, turnover for these executives is unusually high due to the level of stress involved resulting in high burnout and short retention," he said. In fact, a recent article in Cybercrime Magazine states that 24 percent of Fortune 500 CISOs are on the job for just one year.

Maturity of the Cybersecurity Market

Mr. Javorsky also says that the ever-increasing maturity of the cybersecurity market has naturally increased demand for people who can combat cybersecurity threats at a strategic and board level. "As this domain continues to grow, more and more organizations are now attracting virtual CISOs to meet the talent shortage and challenges presented," he said. "As cybersecurity becomes more mainstream, I believe we are going to see many people with the right skills being elevated into these positions within most enterprise organizations."

"Twenty years ago, cybersecurity was not in the broader echosystem as we see it today," said Mr. Javorsky. "The advancements started to emerge at the start of the social platforms era and has rapidly scaled in the last decade. This then resulted in more and more data through cross platforms, leading to the rise of ransomware attacks and beginning of multi-factor authentication. Given the current data driven environment we have emerged, and the use of mobile devices allowing access anytime and anywhere, and new generation of users combined with technological advancements within the AI, ML and data domains; this will only intensify as we evolve and enter the next gen of Web 3.0 and metaverse, which will present further unique challenges for organizations within the security landscape."

Cybersecurity remains a domain that is top of mind in the board room, by consumers and business leaders alike, according to Joyce Brocaglia, founder and CEO of **Alta Associates** (recently acquired by **Diversified Search Group**) and founder of the **Executive Women's Forum**, a professional membership organization for women in cybersecurity, risk management, and privacy. "There is a groundswell of demand in the market for qualified and diverse cybersecurity talent, and we don't anticipate that evaporating as the economy softens," she said. "This year Alta Associates | Diversified Search Group has seen an increase in executive and C-suite cybersecurity and IT risk searches with companies seeking unique skill sets that include technical competencies, leadership capabilities and business acumen. Corporate boards are becoming more aware of the importance of their role to ensure the appropriate management of cyber risk. With cyber threats increasing and regulators considering new requirements for disclosure of their cybersecurity governance capabilities, companies will continue to bolster their investment in cybersecurity and those cyber executives who are leading the charge."

Increased Threats

"Cybersecurity is extremely important because it is ubiquitous," said Ms. Brocaglia. "With most companies experiencing digital transformation, remote and hybrid workforces and increased threats, cybersecurity is fundamental to protecting a company's assets, stock price and market reputation. Forward thinking companies are utilizing cybersecurity as a competitive advantage and market differentiator. Having the right cybersecurity and IT risk leaders in place enables businesses to grow faster, partner effectively and innovate and deliver products securely."

Every CISO or cyber leadership role we fill requires a combination of technical skills, business acumen, and leadership capabilities; and each role's exact requirements are unique to that particular organization, according to Ms. Brocaglia. "The CISO role is not a one-size fits all, it varies by reporting structure, staff size, scope, and maturity of the program," she said. "As such, it takes a three-pronged approach to ensure that you are

(cont'd. to page 3)

finding the best possible candidate and not just the best available candidate on the market. That's why Alta Associates | Diversified Search Group does our research and identifies new talent; we utilize our known relationships for outreach to potential candidates and we connect with great leaders for referrals of people they highly recommend."

"Because we understand the different archetypes of CISOs we can identify which background fits best with the requirements of that particular role and then only present candidates that are highly matched to the competencies they are seeking," Ms. Brocaglia said. "The reason why companies have a hard time hiring CISOs by using their internal recruiting departments, is that their recruiters are often not sophisticated enough in their understanding of cybersecurity and lack the relationships and networks to identify, attract, and hire exceptional passive candidates in this highly competitive market."

One of the most recurring challenges companies hiring cyber executives are facing is the increased salary expectations of qualified candidates. Ms. Brocaglia says the quandary is that hiring managers must either recalibrate their compensation ranges or reduce their expectations of what skills are possible to attract. In addition to compensation, candidates are also giving weighty consideration to companies that provide flexible or remote work environments.

The demand for CISOs is extremely high, especially in regulated and high transaction processing companies, according to Ms. Brocaglia. "Many companies are recognizing the need to hire their first ever CISO due to pressure from their board, regulators, or increasing threats," she said. "A great number of Alta Associates | Diversified Search Group's CISO searches in 2022 were for companies that realized the cyber executive that got them here is not the leader they need to take them to the future. They are elevating the role and looking for human-centric leaders who are able to collaborate and drive results. We are placing executives that not only have the technical competencies to understand how best to secure their corporation and its digital transformation efforts, but ones who can also understand the financial/risk exposures and communicate them in a language that business stakeholders can understand."

"Recruiting cybersecurity executives can be extremely challenging," said Frank Scarpelli, managing partner and CEO of technology-focused search firm **HireWerx**. "The top performers are certain to be fully engaged, so posting a job advertisement on LinkedIn unfortunately isn't likely going to yield the best results. That said, there are many factors that can motivate cybersecurity executives to make a move. For example, a lack of buy-in by the board or the C-suite, a toxic company culture, inadequate budget, or insufficient recruiting and training capabilities that hinder building high-performing teams."

Some of the key areas of cybersecurity recruiting include threat intelligence, network and endpoint security, mobile security, cloud security, IoT/IIoT security, behavioral detection, deception security, risk remediation, continuous network visibility, quantum encryption, and website security. "Recruiters look for education, certifications, and other credentials to help validate the skills and capabilities of candidates," said Mr. Scarpelli. "That *(cont'd. to page 4)*

ES EXECUTIVE SEARCH PARTNERS

Executive Search Partners
Specialized in
Senior Level
Information Technology
and
Finance and accounting
Searches

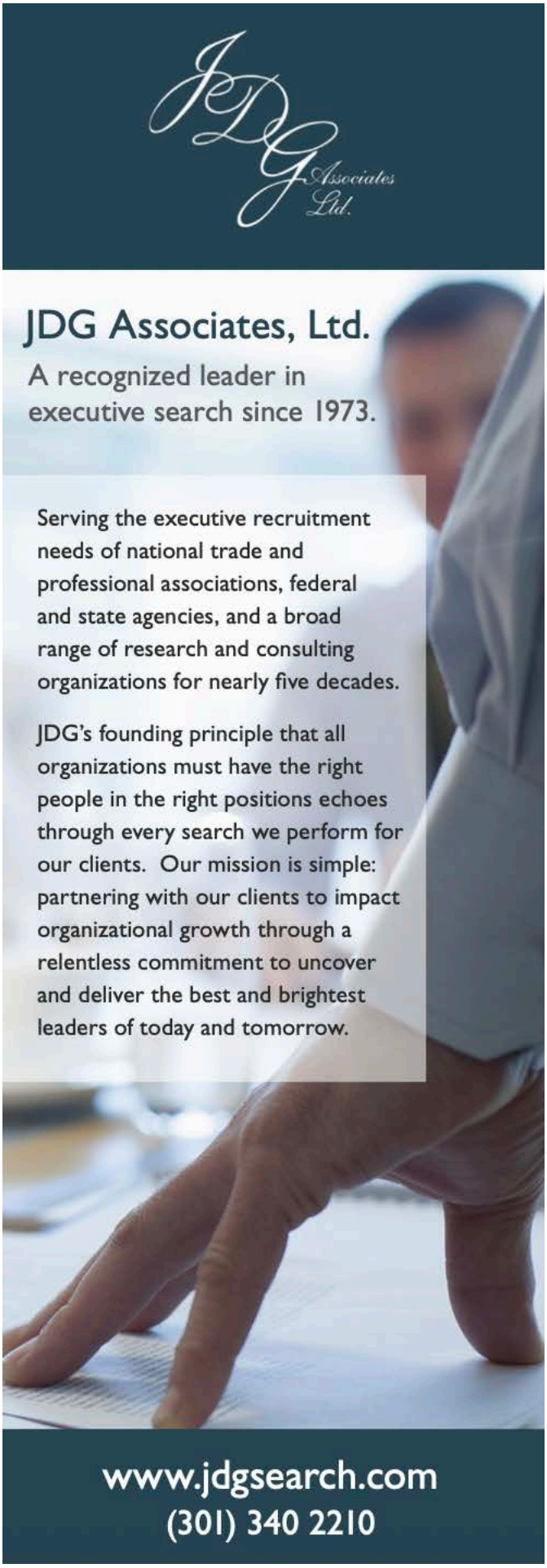
Executive Search Partners
has been in business for 20 years

We interactively work with your
Executives to fully understand
your requirements and then
find candidates that match
or exceed them

"One of the top Search Companies in North America."
-Forbes

Hunt Scanlon CYBER TECHNOLOGY TOP 40

CONTACT US
www.execsearchparters.com
gerickson@execsearchpartners.com
(248) 470-9976



CYBER RECRUITING SEARCH NEWS

ON Partners Recruits Chief Information Security Officer For Trellix

Andy Hickman and Tim Conti of **ON Partners** recently assisted in the recruitment of Harold Rivas as chief information security officer of Trellix, a cybersecurity company based in San Jose, CA. Mr. Rivas' appointment is part of Trellix' ongoing effort to drive the future of extended detection and response, the company said, adding that his leadership will enable Trellix to "best protect against threats, manage compliance needs and third-party risks, and implement industry-wide best practices." Mr. Rivas will lead Trellix's global security and compliance initiatives.

Mr. Rivas joins Trellix from loanDepot, where he served as CISO. In this role, he was responsible for leading information security, privacy, disaster recovery, technology compliance, product security, and other critical functions for loanDepot, its subsidiaries, and its joint ventures. Mr. Rivas previously held additional executive and senior-level information security roles at Santander Consumer, Mr. Cooper, Fujitsu America, and Citi. Trellix is focused on accelerating the use of XDR architecture across enterprises, commercial businesses, and governments to both advance organization security posture and to ease cybersecurity incident response and management.

said, it is more important than ever to be able to assess experience and applied skills, especially those that may be transferable or provide a foundation upon which a company can build upon through training."

High Demand for CISOs

As technology evolves and becomes ever more sophisticated, the demand for experienced chief information security officers has never been higher. "No longer can companies trust that their algorithms, code, or other intellectual property will remain protected," said Mr. Scarpelli. "Turnover for this technology leadership position is unusually high due to the level of stress involved. Let's face it, the consequences of any breach will likely fall directly at the feet of the CISO. The average tenure of a CISO is 18 to 26 months according to multiple sources. *Cybercrime Magazine* states that 24 percent of Fortune 500 CISOs are on the job for just one year."

It is critical that today's CISO bring a combination of technical and business acumen to the table, said Mr. Scarpelli. Equally important, the individual must be able to communicate effectively at the executive and organizational levels. Some of the direct impacts of the role may include risk mitigation, building a strong cybersecurity culture, establishing processes to meet and anticipate current trends of threats, and positively impacting the quality of data across the organization.

"The CISO is in a unique position to view data across the enterprise, which allows the business to identify opportunities for competitive advantage," said Mr. Scarpelli. "Building a strong security process can oftentimes be a unique selling proposition for the company that offers a distinct competitive advantage."

Moving forward as technology continues to evolve, it is imperative for CISOs to operationalize security rather than merely focus on compliance and oversight," *(cont'd. to page 5)*

said Mr. Scarpelli. What's more, depending on your structure, ensuring alignment with the business as well as more traditional IT infrastructure areas is critically important. Mr. Scarpelli said that some key areas to consider as the cyber landscape evolves would be: how enterprise API ecosystems will reveal new vulnerabilities, the increasing sophistication of phishing attacks, new risks that 5G will bring particularly in the area of IoT, and the potential vulnerabilities that can compromise smart devices in order to illustrate network infrastructures.

With a staggering $334 billion global cybersecurity revenue expected by 2026 – vs. $ 220 billion in 2021, the emerging of the cybersecurity topic as top priority on the agenda of the company boards – is not a surprise that the recruiting in cybersecurity is and will continue to boom for the next years, also driven by a significant growth in the consumer market, according to Raffaele Jacovelli, managing director at **Hightech Partners**.

"The rapid emergence of interconnected industrial or consumer devices and associated security risks with scare security upgrades could favor the sector growth as it poses relevant vulnerability risks and issues," said Mr. Jacovelli. "In addition to the rising frequency of attacks, the emergence of zero days, ransomware is also gaining prominence, and has been used in several high-profile attacks. It is the most concerning type of cyberattack for business leaders."

Digital Transformation

As already indicated, the demand for CISOs is very strong – and will remain as such in the near future. Mr. Jacovelli points to two different reasons: "On one side, the increase in digital transformation initiatives, penetration of Internet connectivity, and susceptibility stemming from IoT connectivity is likely to increase the need to adopt of cybersecurity solutions. At the same time, the general structural shortage of skills in the digital domain has increased the gap between demand and offer: The pace at which people are educated is not fast enough in comparison with the acceleration driven by the digital transformation."

"The executive search industry should act certainly on the side of the individuals creating a pool of CISOs to be provided on demand – we are looking at this option currently – or partner with companies that can provide CISO-as-a-service leveraging multiple wide competences," Mr. Jacovelli said. "In this case the role is not covered by a single individual but by several professionals that obviously have operated in an orchestrated but flexible manner. We have already invested in this area acquiring a relevant stake in a company, Ataya & Partner, that is recognized as a leader and a subject matter expert in the domain in continental Europe."

Cybersecurity has become a relevant area of attention since the rise of the internet era, over 25 years ago, says Mr. Jacovelli. At the time the Trojan horses were introduced mainly by email, hence the growth of the 'antivirus' business. With the explosion of broadband, IoT and 4G about 10 years ago the need to create a cybersecurity practice or unit has emerged strongly: we have started running systematically CISOs searches in 2015 and since there has been a constant flow, further accelerated in 2017 by the decision to embrace digital transformation by several leading companies."

Hunt Scanlon Top 40
Cyber Technology Search Firms

3D Executive Search Partners Blake Dunavant, Managing Partner	(972) 402-5767
Acertitude Kevin O'Neill, Managing Partner/Rick DeRose, Managing Partner	(401) 522-5150
Artico Search Matt Comyns, President	(203) 570-7472
Bespoke Partners Eric Walczykowski, CEO	(858) 356-6730
Benchmark Executive Search Jeremy King, President	(703) 728-8506
CarterBaldwin Executive Search Jennifer Poole Sobocinski, Partner	(678) 448-0010
CIO Partners Joe Gross, President	(770) 971-0324
Comhar Partners Bernard Layton, Managing Director	(415) 903-4000
Cowen Partners Shawn Cole, President	(360) 947-2804
Cyber Exec Executive Search Jean-Louis Lam, Managing Partner	(312) 568-6748
CyberSN Deidre Diamond, CEO	(857) 415-2650
Daversa Partners Joe Patalano, Managing Partner	
DHR Global Sal DiFranco, Managing Partner	(312) 782-1581
Direct Recruiters Ryan Lange, Partner	(440) 996-0593
Diversified Search Group/Alta Associates Joyce Brocaglia, CEO	(908) 806-8442
Egon Zehnder William Houston, Global Lead	(202) 774-1300
The Executive Search Group Tim McIntyre, Founder	(860) 652-8000
Executive Search Partners Gary Erickson, Managing Partner	(248) 470-9976
Heidrick & Struggles Matt Aiello, Partner	(415) 981-2854
Heller Search Associates Martha Heller, CEO	(508) 366-7005
Hightech Partners Raffaele Jacovelli, Managing Partner	+32 475 733348
JM Search Tom Figueroa, Co-Practice Leader/Kevin Kernan, Co-Practice Leader	(610) 964-0200
Kingsley Gate Partners Umesh Ramakrishnan, Office of the CEO	(972) 726-5550
Korn Ferry Tony Rossano, Head of Global Technology Practice	(612)-906-3438
McDermott + Bull Chris Bull, Managing Partner	(949) 529-2690
McIntyre Associates Jeff McIntyre, President	(860) 284-1000
N2Growth Kelli Vukelic, CEO	(800) 944-4662
Odgers Berndtson Steve Potter, CEO	(212) 972-7287
ON Partners Baillee Parker, Partner	(612) 825-4215
The Onstott Group Joe Onstott, Founder	(781) 235-3050
Pinpoint Search Group Mark Sasson, Managing Partner	(970) 816-6175
Riviera Partners Will Hunsinger, CEO	(877) 748-4372
Russell Reynolds Associates Angela Jung, Consultant	(305) 717-7400
Slone Partners Cybersecurity Mike Mosunic, Co-Founder	(866) 245-9653
Spencer Stuart Peter Hodkinson, Consultant	(212) 336-0200
SPMB Radley Meyers, Partner	(415) 924-7200
StevenDouglas Jamie Javorsky, Senior Vice President	(954) 385-8595
True David Winch, Partner	(646) 741-2585
Wilton & Bain Erin Callaghan, Partner/Chloe Watts, Partner	+44 (20) 7621 3570
ZRG Partners Lisa Hooker, Managing Director	(512) 501-1515

© Hunt Scanlon Media, Copyright 2023, All Rights Reserved.

StevenDouglas

JOIN OUR TEAM

WE ARE HIRING

We are expanding rapidly and hiring at all levels across the country.

TALENT WE ARE SEEKING

- Top Executive Search Consultants
- Technology Search and Staffing Recruiters
- Finance and Accounting Search Consultants
- Interim Resources Recruiting Managers
- Interim Resources Market Leaders
- Executive Search Researchers/Recruiters

Longevity | Great culture | Highly collaborative

Approaching 40 years in business, privately owned.

Apply Now...

COMPANY HIGHLIGHTS

A Trusted Company Since 1984 - A trusted advisor to companies for over 35 years, starting in Miami in 1984, and now growing to over 20 offices across the United States, as well as a presence in Latin America and Canada.

Top 25 in the U.S & #1 Executive Search Firm in Florida - StevenDouglas is recognized by Forbes as one of America's Best Executive Search Firms and a Top 25 firm on Hunt Scanlon's Top Executive Search Firms in America list making the firm #1 in the southeastern U.S.

Recruiting Experts for Almost 40 Years - Our firm has been connecting clients in an array of high-demand disciplines and industries to premier candidates since 1984.

WHAT STEVENDOUGLAS STANDS FOR

Ethics
Doing things the right way. Upholding consistent best practices, professional standards and integrity with everyone we work with.

Respect
Treating everyone internally and externally with respect and authenticity.

Trusted Advisors
Supporting clients and candidates with knowledge and experience in the industries and areas of expertise that we serve.

SPOTLIGHT

A Look Inside the Competitive Market for Cyber Experts

*A pioneer in the development of the cybersecurity recruiting industry, Matt Comyns co-founded **Artico Search** with Mercedes Chatfield-Taylor to lead the team helping companies protect against cyberwarfare. He built the original cybersecurity search practices at two global firms – Russell Reynolds Associates and Caldwell – filling more than 300 executive level searches in a hyper-competitive market by serving as a trusted advisor for chief information security officers. He developed his vast network as founding CEO and sales executive at tech and media companies in New York, San Francisco, and Beijing.*

*Mr. Comyns recently sat down with **Hunt Scanlon Media** to share his thoughts on the competitive cybersecurity recruiting landscape.*

Matt, since we last spoke can you tell me what you are seeing in cybersecurity recruiting?

Despite the market turbulence, many organizations of all sizes and funding levels are looking to hire security professionals at various levels. CISO recruiting remains important to funds that have invested significant capital in portfolio companies; many companies that are weathering the turbulence well continue to increase the size of their budgets and teams irrespective of the macro conditions. Candidates actively seeking a new role have options and many end up with multiple offers; this consequently leads to the continued upward pressure on compensation for high-caliber candidates – this is especially true of security professionals on the technical side of security (security engineering, security architecture, incident response, etc.)

How difficult is to recruit cybersecurity executives?

In a market this competitive it is always a challenge to recruit, so relationships are critical. Recruiting cyber executives is all about trust – does the candidate pool trust the recruiter, do they develop trust with a hiring manager and critical stakeholders? To stay ahead, we spend a lot of time in the trenches with the candidate pool so they know we have their best interests at heart and try to find them a position that works for all parties – it's not about filling a role, it's about finding a long-term match for the business and the candidate.

What is the current demand for CISOs?

Heading into 2023 we're seeing demand down from where it was a year ago, but up from where it was two to three months ago. Companies that are scaling remain in the market for CISOs, particularly if there's a departure or there is external pressure from investors to formalize or mature a program.

What value do CISOs bring to organizations?

Mature CISOs have elevated themselves from tech executives to business risk executives, so the value a strong security leader can bring to an organization is significantly greater than it was 10 or even five years ago. At this point in the CISO journey, security leaders are not only conducting security due diligence, but many are identifying acquisition targets for complementary tech, something mostly unheard of in the not-too-distant past. CISOs serve as the quarterback during an incident, and likely have a playbook to manage responses; they are the face of security internally as well as with customers

What do CISOs need to know moving forward as technology continues to evolve?

CISOs need to keep a pulse on the latest vendor trends and technologies. They need to know what their own company development pipeline looks like, and how it compares from a security perspective, and if they're at a security product company, from a product differentiation and end-user solutions perspective. The threat environment continues to get more complex, so understanding what industry peers are facing, and how they are mitigating these threats is essential to the success of their programs.

"CISOs serve as the quarterback during an incident, and likely have a playbook to manage responses; they are the face of security internally as well as with customers."

Can you share some search work you have done for cyber security executives?

CISO searches for technology portfolio companies of a16z and Vista as well as privately-held multi-billion Cox Automotive. Team build work for pre-IPO companies like Justworks, as well as team-build work for companies like Mandiant (acquired by Google this year), Chubb Insurance, Charles Schwab, JPMC, Clear Secure, among others.

What do you see for this sector in the next five to 10 years?

The security transformation is likely a 30-year journey and we are heading into year 10 since the Target breach of 2013 that brought security to the forefront of business risk. Our data (coming out of our Artico Search / IANS 2022 CISO survey) indicates that budgets and compensation continue to increase, we expect that trend to continue. Over the next five to 10 years, we'll likely see a heavier push to automate tasks as companies continue to battle for talent.

Any other trends that you would like to share?

We're also seeing many cloud-forward and cloud-native companies merging the CIO and CISO roles into one, we expect that trend to continue and be adopted in more places as more companies move away from traditional tech stacks and into the cloud. CISOs will continue to get more reps in front of boards and leadership teams, and we would expect that over the next decade they will likely be viewed as true business risk executives at even more companies than they are today.

SPOTLIGHT

A Look Through the Eyes of an Executive Recruiter at the Cybersecurity Sector

*As a partner at **SPMB**, Radley Meyers works with a variety of leading technology and tech-enabled-services companies, placing senior-level executives at venture capital-funded, private equity-backed, and publicly traded companies. A key area that he brings extensive knowledge and expertise to is SPMB's security and data-related search work.*

Mr. Meyers leads both functional searches (CISO, CDO, and VPs defining security and data strategy), and also builds out executive teams at top security software and data companies. The comprehensive nature of his work—on both the software vendor and the operating side—gives him a unique and in-depth understanding of today's market that, in turn, helps drive successful outcomes for his clients. Mr. Meyers recently sat down with Hunt Scanlon Media to discuss what he is seeing in the supply and demand for cybersecurity leaders and how their role has evolved in recent years.

Give us an overview of the market for cybersecurity recruiting.

The market remains extremely hot for security professionals, which is no surprise given the high profile headlines around security events we see on an almost daily basis. So, while hiring has slowed for other executive functions, savvy companies are ramping up their efforts around security hiring — and are also upleveling their existing security team and resources to get more from the function. In fact, I am seeing a lot of companies look at their CISO and think: How can we broaden the role of security in our organization? The answer to this question varies depending on the company — but I've seen CISOs take over IT, data, product, engineering, and sales teams. Again, a CISO's remit depends heavily on the industry and future vision of the company, but there is no question that the role is expanding meaningfully and quickly.

Any other trends that you are witnessing?

The other theme worth noting is companies are exploring hiring a true CISO (vs. a director or "head of") much earlier in their growth cycle. Historically, an upcoming IPO triggers the hiring of a CISO. Comparatively, earlier stage companies/startups tend to leverage more junior security leaders as they begin to scale. However, given the themes noted above paired with the complexity around international/global growth and the regulatory requirements tied to that growth, companies are bringing more tenured talent in-house earlier on in their growth journey.

Why is this sector so important to all companies and organizations?

The rise of the CISO and companies prioritizing the importance of the broader security organization has been encouraging, and perhaps long overdue. Historically, the most highly regulated industries like healthcare and financial services have prioritized security and helped lead the way. Today, in a digital first world, there is so much information and data at risk that every company, big or small, is having to evaluate their security posture and mature their security programs accordingly. Customers and consumers want to know that their data is protected and that by being a customer or a partner they are not at risk. Having a security leader who is capable of building a strong program, and also has the ability to convey this strategy to customers is both critical and highly sought-after. Security is no longer (and probably never should have been) a "behind the scenes" function; instead, it is now fully entrenched in the sales, product, legal, and technology organizations. As companies continue to recognize the damage that security events have on their brand (and bottom line), the more investment they will make into the function.

What are some challenges you are seeing in the market for these top executives?

The market is evolving quickly, but certain things are going to take some time to catch up — one of which is the wide spectrum with regard to compensation. You're seeing CISOs with similar job scopes, within the same industry, at similar scale with drastically different compensation models. I believe the next shoe to drop, that will help establish more compensation consistency, is an updated reporting structure for CISOs and security executives.

Are CISOs today reporting directly to the CEO?

Today a small percentage of CISOs report directly to the CEO. However, this number is growing steadily as companies see the value in their security executive having a direct line to the CEO. It no longer makes sense to have your CISO buried two to three levels below the CEO where their influence and impact is minimized. Security executives need a seat at the table in order to protect their organizations and their customers from the onslaught of cybersecurity threats that only continue to grow year after year. This notion is being reaffirmed by the SEC and their proposed new cybersecurity disclosure rules for public companies that stress the importance of cybersecurity expertise and inclusion on boards as a critical part of corporate governance and board oversight going forward.

What is the current demand for CISOs?

The demand is as high as it's ever been — and for good reason. Given the massive implications of high profile cybersecurity events like SolarWinds and Log4j, or even the news cycle surrounding Uber and Twitter security leadership, boards are hyper aware of the need for top-tier security leadership. That said, there is a finite number of "been there, done that" CISOs available today who fit the modern CISO profile, meaning that they can effectively work with product, sales, IT, etc. The demand definitely outweighs today's supply, which creates a bit of a void, but it also puts even more pressure on companies and leaders to develop a strong bench of future security leadership. This requires investment and commitment to growing and maturing security programs at most companies that have reached a certain scale across all industries.

TEMPTING TALENT

Salary offers that Executive Search professionals need to consider moving roles:

+26%
Delivery/Recruiting Professionals

+28%
Business Development professionals

+32%
Leadership Professionals

Tempting Talent can help secure the very best Executive Search talent for your business

temptingtalent.com

enquiries@temptingtalent.com

Data taken from Tempting Talent's 2022 Compensation Report

Expanding the Role of CISOs on Boards

Not since 2002 and the passing of the massively consequential Sarbanes-Oxley Act, when the Security and Exchange Commission (SEC) required America's boards of directors to appoint chief financial officers and form audit committees, has there been such a critical impending change to board skill-sets and reporting. The SEC has once again identified a serious gap in board expertise, governance, planning, accountability, public disclosure and response – this time in the areas of cybersecurity and risk assessment – and is making regulations to address them. The changes are expected to be finalized by the end of the year.

The SEC's proposed amendment requires boards to begin reporting about material incidents and providing updates; initiating and reporting on policies and procedures to identify and manage those risks; reporting on their impact to the bottom line; reporting their resolution; and notifying investors about those incidents. Thus far, the SEC has only talked about the specific outcomes they want to see implemented and not provided specifics about how companies can best satisfy the new requirements.

DHR Global has been actively focusing on what the right cybersecurity expertise encompasses at the board level, how it will dovetail with other board positions such as the chief information officer, and is recommending its clients get ahead of the new rules by recruiting highly qualified chief information security officers (CISO) to take their seats at the table as board directors. "Thanks to the SEC's new cybersecurity requirements and the growing threats evolving from digital technology and the use cases and business models they enable, there is a huge opportunity for CISOs to broaden their roles into the boardroom," said the search firm in a new report.

The Ideal CISO Board Member

According to DHR's proprietary research, to date only seven of the 500 largest public companies in the U.S. have an experienced CISO currently sitting on their corporate board of directors.

"Among our clients we are increasingly seeing that cybersecurity is becoming a new agenda item at every board meeting," said Heather Smith, partner in the board and CEO practice at DHR. "Our research shows that the vast majority of boards do not have a CISO among them. As such, non-technical board members are called on to provide guidance on cybersecurity risk. It's becoming apparent that there is a specific cybersecurity skill-set that we are recruiting for to meet both the current need and the impending SEC requirement."

"The ideal board CISO provides a competitive advantage and brings relevant, recent experience from the last two years, has a long lens when it comes to the latest cyber vulnerabilities and a strategic, proactive outlook, and is able to communicate effectively regarding what risk management entails at the board level," said DHR's Kathryn Ullrich, managing partner in the advanced technology practice. "They understand IT security but also the company's strategy and how IT should support that strategy."

What has caused this massive threat and critical omission at the board level? Digital technologies and *(cont'd. to page 10)*

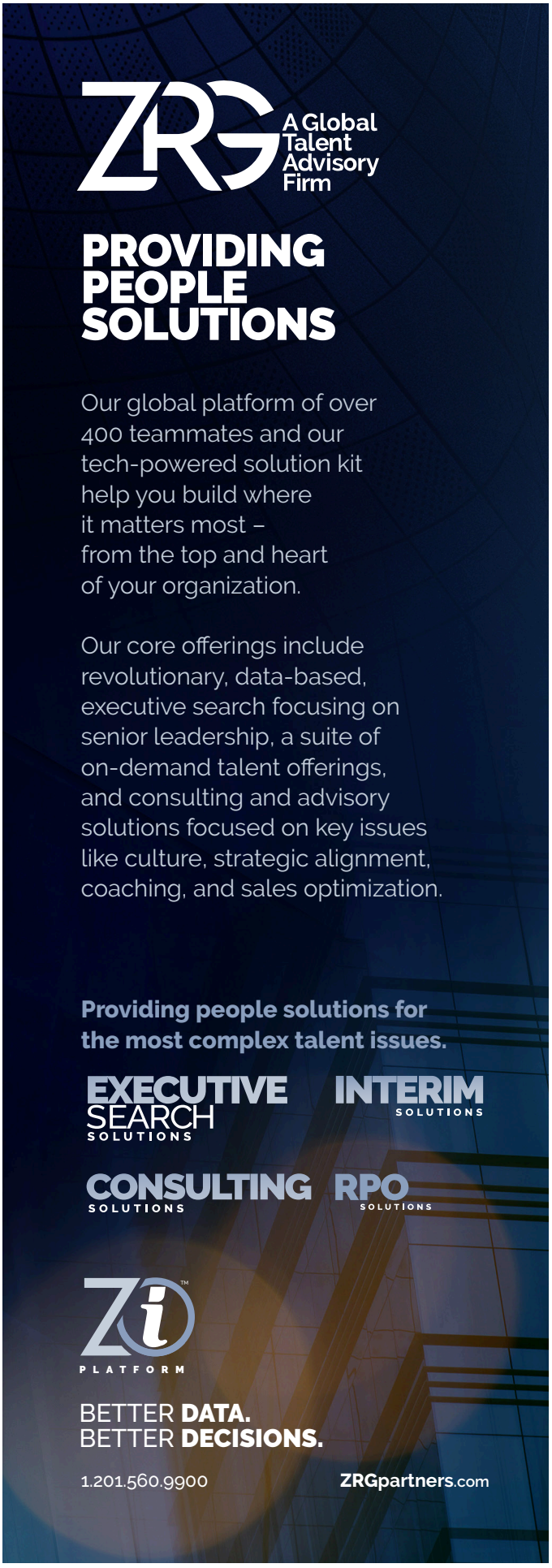
their impact on the modernization of networks and infrastructures are at the heart of the issue, according to DHR. "Already in play, these changes have been sped up out of necessity by business closures and remote workers due to COVID, workplace re-openings, and a newly hybrid workforce, supply chain disruptions, applications and operations moving to the cloud, a slew of new internet of things devices and multi-domain networks in which operations technology and information technology networks are merging – all have meant that there are many new and ever-evolving avenues for hackers to take into the heart of economies, businesses and everyday life," said the report. According to the World Economic Forum, 70 percent of economic growth is now being driven by digital technologies.

The numbers, says DHR, are startling: Cyber-attackers can breach 93 percent of company networks, according to new research from Positive Technologies; cyberattacks in 2021 increased by 50 percent when compared to 2020, as reported by cybersecurity firm Check Point; cybercrime cost U.S. businesses more than $6.9 billion in 2021, the FBI told Newsweek in March 2022; and 29 percent of CEOs and CISOs and 40 percent of chief security officers admit their organizations are unprepared for a rapidly changing threat landscape, reports Thought Lab from their 2022 cybersecurity study.

"Today's cybersecurity threat takes many forms and can vary by industry," said the DHR study. "Among this year's top issues according to CSO Magazine: ransomware, cryptomining/ cryptojacking, deep fakes, video conferencing attacks, XDR (extended detection and response across endpoints, email, identity and access management, network management and cloud security), operational attacks against IoT and OT, and supply chain attacks such as the recent Solar Winds breach."

In its study, DHR points to a wide range of potential targets:

- **Education:** Outdated technology, massive stores of data, and hybrid campuses are putting education at risk. Data breaches, phishing, and ransomware are the top methods for attack here.
- **Healthcare:** In healthcare, it is the vast number of new medical and IoT devices now on the network that are most at risk with hackers targeting patient care devices and causing distributed denial of service attacks demanding ransom and holding hospitals hostage.
- **Manufacturing:** In manufacturing, as multiple OT, IT, and cloud networks connect for the first time, the lack of end-to-end security is causing issues as new, wireless endpoints and legacy systems suffer from weak encryption impacting production and distribution.
- **Energy:** In energy, it is inefficiencies in identity and access management and a lack of system integration that causes vulnerabilities in the supply chain.
- **Financial Services:** Financial services continue to be threatened by data breaches from ransomware, phishing, web application and vulnerability exploitation and denial of service attacks.



Slone Partners Launches Cybersecurity Practice

Life sciences-focused search firm **Slone Partners** has launched Slone Partners Cybersecurity, a national talent recruitment firm that delivers diverse commercial, operational, and technical cybersecurity specialists and leaders for companies in all business verticals and health systems. The firm is a successor to Wolf Hill Group, which was founded as a joint venture with Slone Partners in 2019.

Adam Slone, founder of Slone Partners, will continue to advise both companies and be actively involved in guiding Slone Partners Cybersecurity as a value-driven organization committed to its clients. Leslie Loveless will remain CEO of both firms, while Tara Kochis will remain president of both firms.

"Slone Partners Cybersecurity will draw upon the expertise, experience, and networks that have positioned Slone Partners as one of the nation's top executive recruiting firms in the life sciences and healthcare industries," said Mr. Slone. "We are fully prepared and excited to deliver on our mission of securing critical cybersecurity talent who build and protect amazing organizations."

The renamed firm has more than 75 years of combined recruiting experience among its founders and is well positioned to understand and meet the cybersecurity talent needs of high-performing organizations in a competitive market, said Slone Partners. While the firm will engage in searches for leadership positions including board members, CEOs, CISOs, and CTOs, it is also designed to support companies seeking specialists for their cybersecurity teams, including analysts, engineers, program managers, threat hunters, and security officers.

"Slone Partners Cybersecurity will draw upon the expertise, experience, and networks that have positioned Slone Partners as one of the nation's top executive recruiting firms in the life sciences and healthcare industries," said Slone. "We are fully prepared and excited to deliver on our mission of securing critical cybersecurity talent who build and protect amazing organizations."

"We look upon this name change as an opportunity to extend our reach and enhance the impact that we can have in the cybersecurity market," said Ms. Loveless. "The scarcity of cybersecurity talent is a serious challenge for companies in all sectors and health systems, and Slone Partners Cybersecurity is uniquely designed to address those needs."

"The cyber threat landscape is changing rapidly, the risks are expanding, and organizations are having to revamp their operational infrastructures to keep up," said Ms. Kochis. "That includes building robust and diverse cybersecurity teams that are trained and empowered to develop and implement the initiatives needed to manage those risks. As a company, we are sincere advocates of the power of diversity, equity, and inclusion to make great companies even greater, and that is baked into all of our cybersecurity recruiting strategies.

Creating Value through Optimizing Talent.

hirewerx
talent solutions

Executive Search
Talent Advisory & Consulting

Private Equity & Venture Capital

- Strategic Hiring
- Recruitment Strategy
- Private Equity Leadership
- Interim Management Resources

HireWerx was created with one goal in mind:

Deliver custom talent solutions to produce optimal results for clients.

We take pride in our domain expertise, process, execution, and speed.

LEARN MORE

10 S Riverside Plaza
Chicago, IL 60606
hirewerx.com | 312-690-4950

AMER | EMEA | APAC

The Burgeoning Demand for Cybersecurity Talent

The impact of a cybersecurity breach – be it from cyber criminals, business competitors, terrorist organizations, or foreign nations – is unsettling to say the least. In terms of dollars alone, the average data breach cost $4.35 million in 2022, an increase of 2.6 percent over last year and 12.7 percent since 2020, according to a new report by IBM. And for critical infrastructure organizations – like those in the financial services, industrial, technology, energy, transportation, communication, healthcare, education and public sector industries – that number jumped to $4.82 million — $1 million more than the average cost for those in other areas. And let's not forget the damage to reputation and trust, shutdowns, harm to the potential sale of a business, lawsuits, even legal penalties that can leave a company reeling.

All this has made finding top cybersecurity talent a growing imperative for organizations everywhere. And it's not just the senior-most leadership roles like chief information security officers that are in demand. Search firms are being asked to build out teams, which in some cases can number in the hundreds of new hires. That's good news for recruiters who specialize in the field. A growing challenge, however, is finding the people to fill the roles that are vital to keeping organizations safe. And because it's a relatively new field, building pipelines continues to be a work in progress.

"While companies may be reducing headcount in these uncertain economic times, they are not including cybersecurity talent in their cutbacks. I have one private equity client with 100 portfolio companies who told me recently that they have cut the technology budget by 20 percent, But they're growing the cyber budget by 20 percent."

"It's difficult in different ways, depending on the level of the role," said James Shira, global and U.S. chief information and technology officer for professional services network **PwC**, speaking about the stresses of recruiting cybersecurity talent. "But it's difficult across the board. For the executive-level type searches, it's difficult because the skill-set for the role is not just technical. And those non-technical, more subjective type qualities in an executive role are much more important for a CISO now than they were a decade ago."

The War for Talent

For the next level down, such as a director role, it's a similar challenge. "But then the focus there also needs to be not just those executive-level qualities but also what is that person's ability to lead and deliver change," said Mr. Shira. "When you go to the more junior-level roles, it's a little easier, although not easy. In that case, below the director level, there's a broader *(cont'd. to page 13)*

population of available folks. But in that space, there is never enough. And there's a lot of what I'll call talent wars occurring between different organizations. So it's not uncommon to find someone who's a manager-level person, with like five or six years of experience, and that person calls you after you think that they're going to join you, and they say, 'Oh, well, my incumbent employer offered me your offer plus X.' There's a bit of that occurring more at that level."

Matt Comyns, president and co-founder of **Artico Search**, a pioneer in the development of the cybersecurity recruitment industry, says the problem of finding cybersecurity talent is especially acute with large enterprises. "We've been having this really hockey stick, rapid growth in cybersecurity over the past six to eight years, " he said. "And in that time, you've seen, for example, large financial services companies literally transforming their teams where they have doubled, tripled, quadrupled in size."

Mr. Comyns cites one major financial services player he has worked with that five or six years ago had a cyber team of about 300 people. That number is now 600. "You also have banks that had teams in the hundreds; now it's multiple thousands of people. Same with Google and all these other places. For these really large programs, there are thousands of people globally on their security teams. In fact, I'm talking today with a very large global bank, and I was just told that they have 500 open headcount – 500, right now. So all of these companies are still ramping up. And at the same time, as you can imagine, when the whole market is ramping up everybody's getting poached at the same time. So not only are you filling the open headcount that you've identified to round out your team, but you have to replace those who are leaving."

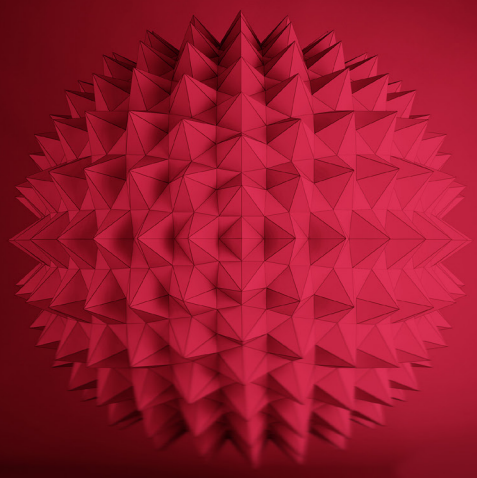
What Downturn?

Cybersecurity roles are largely recession-proof. While companies may be reducing headcount in these uncertain economic times, they are not including cybersecurity talent in their cutbacks. "I have one private equity client with 100 portfolio companies who told me recently that they have cut the technology budget by 20 percent," said Mr. Comyns. "But they're growing the cyber budget by 20 percent. This is just one of those things – you've got to take care of this problem of security. You might say, 'Oh, can you do more with less?' But no matter how you slice it, this is an expanding area, even in this market. We have yet to hear any chatter whatsoever that people are freezing hiring in cybersecurity."

Even lower level hires are in demand, so much so that not long ago fast-growing Artico Search signed on three respected recruiters from information security boutique L.J. Kushner & Associates in the wake of its acquisition by BG Staffing. "They had a particular expertise and focus on this next level down hiring," said Mr. Comyns. "And I said, Gosh, all of these Fortune 500 companies are coming to me more and more, saying, 'Hey, can you do a handful of roles below the CISO? Can you do even more roles below that?' I'm getting mandates now that I never did before. In the last six months, I've gotten mandates for five or six searches at a pop from one organization. This is definitely happening. It's definitely a trend. And because a rising tide lifts all boats it's not just the CISO who's getting paid; everybody's getting paid."

acertitude.
brilliant people at work®

Unleashing cybersecurity.



Cyber-attacks are the biggest threat to business, and one of the biggest specialties at Acertitude.

Our world class team combines insights from the most sophisticated market for cyber talent in the US with the fastest growing one in the UK.

Our proprietary maturity model for what goods looks like in cyber leadership benchmarks CISOs, their teams, and cyber practice leaders.

Secure your business. Get in touch.
cyber@acertitude.com

CISO & Cyber Searches | Cyber Advisory Boards
CISO Master Classes | Cyber Leader Maturity Model
Cyber Leader Development

DIVERSIFIED SEARCHGROUP

We invite you to join a people-centric firm collectively dedicated to our purpose.

Cultivating new leadership for a changing world

DIVERSIFIEDSEARCH
Alta ASSOCIATES
BioQuest
GrantCooper
KOYA PARTNERS
StorbeckSearch

DIVERSIFIEDSEARCHGROUP.COM/CAREERS

Forbes
POWERED BY STATISTA
AMERICA'S TOP 10 EXECUTIVE SEARCH FIRMS 2022

A MEMBER OF ALTOPARTNERS

Top Cyber Searches Making News...

Odgers Berndtson Seeks Chief Cybersecurity Officer for U.S. House of Representatives

Odgers Berndtson, has been enlisted to find a chief information security officer for the Office of the Chief Administrative Officer of the U.S. House of Representatives. Partners Diane Gilley, a member of both the firm's technology practice and CIO and technology officers practice, and Jon Barney, head of the U.S. aerospace, defense, and national security practice, are spearheading the assignment. The CISO role requires a visionary, positive leadership focused individual with sound knowledge of cybersecurity fundamentals for risk management, incident management/response, and offensive engineering. The ideal candidate is a thought leader, a consensus builder and bridge builder between the cybersecurity office, its policies and strategy with the members, committees, and leadership offices at the House.

SPMB Recruits Chief Revenue Officer for Xage Security

SPMB, an executive search firm that helps find transformative executives throughout Silicon Valley, has recruited Darron Makrokanis as the new chief revenue officer of Xage Security. Todd Greenhalgh and Nick Hoffmire led the assignment. "Darron's track record of scaling software and cybersecurity companies will help Xage broaden its impact across sectors as the urgent need to cyber-harden critical infrastructure industries continues to accelerate, the search firm said. "Xage is on a mission to protect the world's most vulnerable organizations from potentially devastating hacks," said Duncan Greatwood, CEO of Xage. "This means we need to continue to scale across both the public and private sectors Darron's impressive track record scaling software and cybersecurity companies will help us broaden our impact across sectors."

DHR Global Recruits CISO for University of California

Chicago-based executive search firm **DHR Global** recently placed April Sather as the chief information security officer (CISO) for the University of California (UC) Office of the President in Oakland. The assignment was led by Kathryn Ullrich, managing partner in the search firm's Silicon Valley office, and Ed Flowers, managing partner, chief human resources and diversity practices, in Atlanta. As CISO, Ms. Sather reports to the university's chief information officer, said DHR Global. The individual will be accountable for and bear shared responsibility for information security across the University of California system. The position collaboratively leads the development and implementation of a shared vision for information security across all UC locations that measurably reduces the university's cyber risk.

...More Cyber Searches Making News

JDG Associates Tapped by the Andrews Federal Credit Union To Fill VP of IT Security Role

Rockville, MD-based executive search firm **JDG Associates** has been retained by the Andrews Federal Credit Union to lead its search for a vice president of IT security. Andrews Federal is seeking an inspiring, transformational leader who will be responsible for evolving and driving its security strategy across corporate systems, networks, branches, and third-party SaaS applications to safely serve its members around the world, said JDG Associates. Reporting to the CIO, the VP of IT security will partner with senior leadership across Andrews Federal to gain alignment and drive forward a strategy and operating model for the Security program. This will involve identifying and acquiring the key personnel, processes, and technologies best suited to improve Andrews Federal's security posture.

Acertitude Recruits CEO for Industrial Defender

Acertitude has recruited Jay Williams as the new CEO of Industrial Defender, a provider of OT cybersecurity technology in New York City. The search was led by Acertitude's technology team and co-led by Rick DeRose, co-founder, managing partner, and leader of the technology practice, and Tim Cook, partner and leader of the firm's cyber practice. "Jay's outstanding track-record of managing P&L, setting winning growth strategies, and working strategically with OT cybersecurity professionals in a variety of industries is a great fit for Industrial Defender's vision for the future," said Mr. DeRose. "We look forward to seeing Jay's impact on the business and continuing our strong partnership with the board and the rest of the Industrial Defender team." Acertitude notes that Mr. Williams is a highly regarded cybersecurity executive with 30 years' experience in operational environments and industrial control systems and 25 years' executive leadership experience.

Hudson Gate Partners Recruits Chief Technology Officer For Mogo

Hudson Gate Partners recently recruited Brad Shapcott as the first chief technology officer of Mogo, a NASDAQ-traded digital payments and financial technology company in Vancouver, British Columbia. Ryan Kellner, Hudson Gate's head of technology recruiting, was retained to lead the search. "We are very excited to have Brad join as our inaugural CTO," said Greg Feller, president of Mogo. "Brad has a wealth of industry experience and we believe he is the perfect person to lead our technology organization to the next level, and to execute on our biggest new product introduction." Mr. Shapcott brings to Mogo three decades of software and IT expertise with global experience in numerous demanding leadership roles.

HUNT SCANLON CULTURE AWARDS FORUM

Designing a Sustainable Culture Blueprint

MARCH 16, 2023
THE PLAZA ■ NEW YORK

Come join corporate culture leaders, business transformation experts, DE&I leaders, chief talent officers, heads of HR, and executive recruiters as they examine how companies are leveraging culture.

BUY YOUR PASS NOW

PREMIER SPONSORS
walking the talk
ZRG A Global Talent Advisory Firm