

Lead Story: [Executive Recruiters Scrambling to Find Cybersecurity Leaders](#) 1

Ranking: [Hunt Scanlon Cyber Technology Top 40](#) 5

Spotlight: [The Ins and Outs of Finding Cybersecurity Leaders](#) 6

## Executive Recruiters Scrambling to Find Cybersecurity Leaders



Increasingly, organizations of all sizes are awakening to the perils posed by cyber attacks. 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 can be. A recent report by Juniper Research, in fact, predicts that over the next five years, companies will suffer \$8 trillion in damages because of data breaches. And that's to say nothing of the intangibles, like harm to reputation, loss of customer trust, and more.

In recent years, cybersecurity recruiting has probably changed more than any other area of technology recruiting. It plays a key role in the success of every company and industry. Moreover, cybersecurity is critical to protecting the information of hundreds of millions of people all over the globe. So it is that the need for top-level cybersecurity talent is urgently needed, and should continue to be in demand for the foreseeable future.

"Cybersecurity recruiting is similar to recruiting for other IT related positions," said Gary Erickson, managing partner of **Executive Search Partners**. "Because our senior partners are former CIOs, we fully understand what it takes to be a successful IT executive. We help our clients define the requirements for their cybersecurity positions and use these requirements in finding and screening candidates."

Executive Search Partners recruits for a variety of senior-level IT positions. Recruiting for chief information security officers (CISO) is no more difficult than recruiting for other senior-level IT executives. The search firm has been in business for 19 years and has an extensive network of CISOs and directors of cybersecurity.

### Protection from Cyber Criminals

"CISOs are critical in that they protect their company from the attacks of cyber criminals and to ensure that their company adheres to country by country customer data privacy laws," said Mr. Erickson. "However, the demand for CISOs seems to be less than the demand for CIOs. We do not see the same level of turnover in CISO positions as we see in CIO positions."

Chief information security officers protect companies from unauthorized access to their computer systems and their data, according to Mr. Erickson. "Cyber criminals attack a company's computer systems to either steal data or to lock down company operating systems so they can collect fees to unlock them (ransomware)," he said. "CISOs put in place the technology and processes to prevent this unauthorized access. CISOs also ensure that their company adhere to country by country data privacy laws."

### BY THE NUMBERS

According to a survey of 458 CISOs, average salary is **\$463,000**...

...compared to a median salary of **\$342,000** in 2021

Source: CISO Compensation Benchmark Report, IANS Research and Artico Search

"CISOs need to stay on top of the constantly evolving threats to their company systems – from new viruses to rogue employees," Mr. Erickson said. "They need to be up to date on new technologies designed to technically protect the organization's computer systems. And they need to be aware of changing country by country laws regarding customer data privacy and data access."

### Heightened Demand for Cybersecurity Leaders

"Given the geopolitical unrest, changing regulatory requirements, and increasing threat landscape, the demand for cybersecurity professionals has never been greater," said 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. "Cybersecurity is now a topic in every boardroom discussion; consumers globally are more aware of digital theft, and corporations and governments alike are seeking to strengthen their cybersecurity programs," she said.

In response to the escalating Russia-Ukraine conflict, President Joe Biden announced that corporations (cont'd. to page 2)

## CYBER RECRUITING SEARCH NEWS

## Diversified Search Group Acquires Alta Associates



**Diversified Search Group**, a leading search firm backed by private equity firm ShoreView Industries, acquired **Alta Associates**, a Flemington, NJ-based search firm founded by Joyce Brocaglia specializing in cybersecurity, IT risk management, and data privacy, earlier this spring. Hunt Scanlon Ventures,

based in Greenwich, Conn., facilitated the introduction and transaction between both organizations.

"This is a strategic acquisition that will add significantly to our business offering in a key field that touches every client we serve," said Aileen Alexander, CEO of Diversified Search Group. "Cybersecurity, data privacy, and resiliency are top priorities for boards and senior leadership across every sector of our economy. Joyce Brocaglia has been a pioneer in this field, and we are delighted to welcome Joyce and her talented team who bring a shared sense of purpose along with deep expertise, insights, and knowledge of talent that will be valuable to our clients."

Ms. Brocaglia, Alta's founder and CEO, launched the firm in 1986. Since then, Alta Associates has specialized in providing leadership to firms ranging from private equity and venture-backed growth companies to the world's largest and most complex global corporations. Alta Associates' experienced and tenured search executives bring a significant level of expertise and knowledge of talent that will broaden Diversified Search Group's capabilities across industry verticals.

should be on high alert for cybersecurity attacks. "I believe we have never been closer to a cyberwar than we are today," said Ms. Brocaglia. "That means the potential attacks against our nation's infrastructure, financial systems, and the internet itself are all possibilities. The stakes are very high. In addition to all that, reports show nearly a half-million unfilled cybersecurity jobs across the nation. This dilemma is not just at the staff level," she noted.

Alta Associates has seen an increased demand in companies hiring their first-ever CISO. "Many corporations also recognize that the cyber leader who got them where they are today isn't the person who can lead them into the future," said Ms. Brocaglia. "So we are placing CISOs who can elevate the function. We also see an uptick in requests for CISOs and cyber-savvy executives in our board director searches. Boards recognize that having a cyber expert in the boardroom in today's digital world provides a perspective that their traditional retired CEOs and CFOs can't offer."

"Forward-thinking companies are assessing the capabilities of their cybersecurity leadership teams to meet the myriad of challenges they are facing," said Ms. Brocaglia. Gone are the days that this assessment is of the CISO's technical skills. Today Alta Associates is working with companies of every size and in every industry to bring in a new breed of CISO who can build proactive security solutions, holistically evaluate the risks of the organization, and communicate those risks in a language that business stakeholders understand.

## Companies are Digitally Transforming

As companies are digitally transforming, they count on their CISOs to take an active role in ensuring that their organizations move securely into the cloud, according to Ms. Brocaglia. "This requires a new type of cybersecurity leader who is proactive, collaborative, agile, and can understand all regulatory, privacy, and

risk implications and consequences," she said. "Most importantly, they need to be capable of leveraging cybersecurity as a business enabler and differentiator for their organizations. Even if your CISO has the skills mentioned above, they need the C-suite's support in funding headcount, upskilling staff, and providing leadership development programs to build and retain leaders. The time to evaluate and elevate your cybersecurity, risk, and data privacy leaders and the teams that support them is now and not after you've been breached," she added.

"Even though cybersecurity has been formally acknowledged as a discipline since 1970 as threat to businesses and individuals, for decades it has been considered as something that could affect only selected organizations up to a certain extent," said Raffaele Jacovelli, managing director at **Hightech Partners**.

Mr. Jacovelli notes that not only has the demand for experienced CISOs been growing dramatically, but at the same time, as more and more service providers are hiring at every level, the entire cybersecurity ecosystem is under pressure fighting for all sort of talent. (Those roles range from penetration testers up to practice leaders that often manage organizations of hundreds – if not thousands – of specialists generating significant revenues.) "The war for talent is hence getting fiercer in this domain due to the endemic shortage: There is simply not enough people that have the skills, the certifications, the approach, and the experience needed to cover the market requirements," he said.

An industry report estimates that there will be more than four million unfilled cybersecurity jobs globally by 2021, up from one million openings in 2014. Statistics suggest that although employment figures from the U.S. are high, currently there are 314,000 vacant positions that need to be filled immediately. The most alarming cybersecurity talent shortage, though, is seen in Europe, where 48 of hiring managers believe finding a perfect match for this role is a rare possibility. In India, meanwhile, cybersecurity job openings have surged in recent years. But with the high demands of a rapidly growing digital economy, one million such positions are set to remain void.

## Cybersecurity Talent Salaries Soar

Cyber breaches at SolarWinds and Colonial Pipeline have only underscored the importance of putting the right CISO talent in place. That, in turn, has led to intense competition to recruit top cybersecurity leadership who have seen their market values and salaries soar, according to just-released compensation data from **IANIS Research** and **Artico Search**. "This increase in demand has led to turbulent market conditions and CISOs' eagerness to understand their market value and how their compensation compares to that of their peers," said Matt Comyns, Artico co-founder and leader of the firm's cybersecurity recruiting platform.

The firm's CISO Compensation Benchmark report offers objective and comprehensive data from 458 CISOs. The distribution curve for total annual compensation shows a wide gap between top and bottom, with a \$463,000 average and a \$342,000 median. The broad range in the total compensation reflects diversity in the market. It includes CISOs at small companies in sectors with relatively immature cyber programs, as well

(cont'd. to page 3)

as those at Fortune 500 multinationals in highly regulated sectors and an established cybersecurity program.

“Business continuity has become front and center in the last 18 months,” said Artico partner Steve Martano. “COVID-19, combined with the vast increase in widely publicized cyber breaches and ransomware attacks, forced organizations to rethink and reprioritize their security programs. Some companies built out first-time programs, while others enhanced existing programs that were lacking in visibility and resourcing,” he noted.

Prior to 2021, cybersecurity was increasingly a pressing topic in most board rooms, said Mr. Martano. “The advanced attacks and costly public breaches and ransomware events over the last 12 to 18 months have increased the frequency and depth of those discussions. COVID-19 and the work-from-home trend have accelerated the visibility of the CISO and the security apparatus, as endpoint security and vulnerability management became front and center due to the prevalence of remote work,” said Mr. Comyns.

Amidst a challenging talent market where demand still far outweighs supply, companies have boosted incentives to attract top CISOs, according to recruiters, including massive counteroffers and retention packages to keep security leaders they trust. Nearly 75 percent of companies preparing CISO offers are contending against one or more competing offers and/or strong counteroffers from candidates' current employers.

Interestingly, female CISOs out earn their male peers by five percent for base compensation and seven percent for total compensation. What explains that difference? Males still dominate the security function. “This gender gap is not unique to CISOs, as there are fewer women across the entire tech leadership suite,” said Artico co-founder Mercedes Chatfield-Taylor. The gap is most apparent, she said, in some of the most transformative tech functions including security, product and engineering. “Female leaders who break through in these functions command a premium in compensation, as nearly every company requires diversity in their slate of candidates—CISO searches being no exception,” she said. This creates optionality and opportunity for female CISOs to increase their compensation by taking on new roles.

#### Specific Needs

Recruiting in the cybersecurity space is very specific based on the needs of a client, according to Sal DiFranco, managing partner of the global advanced technology and CIO/CTO practices at **DHR Global**. “Security as a general topic impacts and is a priority for all organizations,” he said. “There are nuances to the functional talent needed for different industries. Recruiting for cybersecurity professionals within financial services is much different than looking for those professionals for a manufacturing company, or a software vendor. There are different skill-sets as well as business priorities that are important to take into account when recruiting for these professionals. Factors outside of industry differences that impact recruiting include how global/international the business is, the size, the customer base, as well as the maturity of the current cybersecurity organization.”

(cont'd. to page 4)

## All-star technology search talent with globally connected, A-team support.

At DHR, you're the driver of  
your executive search career.

We're a global firm with a  
boutique touch, right-sized to  
be able to offer both robust  
resources and an agile,  
collaborative culture.

Learn more at [dhrglobal.com](https://dhrglobal.com)

Always Connected.

**DHR**  
GLOBAL

**JOBPLEX**  
A DHR COMPANY

[dhrglobal.com](https://dhrglobal.com) [jobplex.com](https://jobplex.com)



Recruiting cybersecurity executives is a different breed of recruiting, Mr. DiFranco says. "While there is much publication on CISO levels many of their direct reports as well as the technical experts in the cybersecurity are not easily found," he said. "They have more tendencies to be private with their information as well as less responsive to typical recruiters reaching to them. This is why it is important to have networks in the space from the CISO level's down to VPs, directors, and even the leading security architects across the industry. Building the network is difficult but it's where the value of a search firm comes in because these relationships across levels not only lead to candidates but to very strong referrals in the cybersecurity community."

The demand for CISOs continues to increase with more and more security threats and advanced hacking capabilities. CISOs are in demand to build a security organization from scratch, mature an existing organization, or drive innovation for an organization for proactive threat prevention, according to Mr. DiFranco. "The CISO role is becoming increasingly visible at the board level, not only for the Fortune 500 but down to middle market and SMB organizations as well to appropriately protect their assets from unknown threats," he said. "CISOs bring value through a variety of ways. They are leading the technology teams to keep assets safe and protect the company and their employees to threats in the digital age."

Mr. DiFranco notes that the CISO role is not a back-office function. "It is a more forward thinking and business facing role than ever before, and CISOs need to be able to touch all areas of the business and be able to communicate effectively with the business," he said. "The role continues to evolve but we will see more CISOs moving into CIO and CTO roles as well as CISOs sitting on boards in the future as security is a function and topic that is critical to the safety and success of any business."

The information security recruitment sector is more than 30 years old, but the first ever CISO appointment is widely believed to be that of Steve Katz in 1995 at Citicorp (now Citigroup) when the financial services corporate suffered a series of cyber-attacks by Russian hackers, according to Tim Cook, partner and practice lead, cyber at **Acertitude**. "Fast forward to today and most organizations will not only have a CISO, but they will also have been either directly or indirectly affected by a cyber-attack," he said. "This has led to an explosion in demand for cybersecurity executives who are dealing with operational cyber requirements as well as responding to increasing levels of governance and compliance at state, federal, and international levels."

According to statistics published by Statista this year, the number of cybersecurity professionals globally is 4.1 million with over one million in the U.S. alone. However, there is a forecast gap of a further 3.5 million jobs worldwide. "The good news for recruiters is that demand for cybersecurity professionals exceeds supply by some margin which should keep the recruitment sector buoyant. However, the bad news is that many CISOs use their own networks to find good talent as well as solving the in-house shortage of specialist cyber skills by using professional service suppliers," said Mr. Cook. "One of the constant criticisms of recruiters in the cybersecurity

## CYBER RECRUITING SEARCH NEWS

### New Cyber Legislation Ups the Ante for CISO Hires



The Senate recently passed legislation requiring companies to report hacks passed unanimously, as reported by the Wall Street Journal. For CISOs, this means that the communication skill-sets, which are already critical, become that much more important, as scrutiny will undoubtedly increase even more in the event of a breach, said Steve Martano, a partner at

**Artico Search**.

This added scrutiny will come in two forms. Internal scrutiny from executive leadership within companies will increase. This should result in extra support and executive buy-in for CISOs. It will also result in additional pressure for CISOs to build highly-capable security functions and teams that will exceed regulatory requirements to protect a company's assets, products, and services, said Jesse Annunziata, a partner in Artico Search's cybersecurity team.

Externally, scrutiny could result in reputational damage to the CISO in the event of an incident. In turn, this may drive CISOs to become more critical when considering joining a new company or staying at their current employer, as they weigh executive-level risk tolerance and support for budgeting and resourcing into their decision-making, he added. Overall, the increased transparency could be game-changing for CISOs, as it should allow them to react faster to hackers' pivots, added Mr. Martano.

space is an inability to understand what good looks like in cybersecurity leadership. In response to this we have developed a five-level model, combined with psychometrics and AI tools, which help our clients and candidates determine what they are looking for and where they are on the model."

### Reducing Risk

"CISOs reduce risk for their organizations by asking better questions around current and future vulnerability," said Mr. Cook. "The impact a CISO has depends on where they sit on our five-level cyber leader maturity model. A level one CISO brings value by ensuring that process controls such as identity and access management, patching, and adherence to some frameworks such as NIST (National Institute of Standards and Technology) are in place. A level 5 CISO (the highest level on our model) is part of the DNA of an organization, a trusted advisor to the board and senior leadership team, and involved very early on in all crucial decisions (e.g., M&A), the launch of new products and services, big hirings and firings, and anything else that is share price sensitive or has an impact on the reputation and trading ability of the company."

Keeping on top of technology evolutions will not keep an organization safer. "CISOs need to focus on developing and retaining their teams, through advanced training and certification programs as well as soft skills such as communication and resilience training," Mr. Cook said. "A cyber function in the middle of an ongoing cyber attack can be a highly stressful place, and therefore keeping an eye on the mental health of the cyber team is very important. These roles require more general IT and business skills which should be easier to recruit and train for. Another area to consider is incentivizing software engineers to develop code more securely. These kinds of initiatives will widen the talent pool and reduce vulnerabilities."

# Hunt Scanlon Top 40 Cyber Technology Search Firms

<b>Acertitude</b> Kevin O'Neill/Rick DeRose, Managing Partners	(401) 522-5150	<b>JM Search</b> Tom Figueroa/Kevin Kernan, Co-Practice Leaders	(610) 964-0200
<b>Artico Search</b> Matt Comyns, President	(203) 570-7472	<b>Kingsley Gate Partners</b> Umesh Ramakrishnan, Office of the CEO	(972) 726-5550
<b>Bespoke Partners</b> Kristie Nova, CEO	(858) 356-6730	<b>Korn Ferry</b> Tony Rossano, Head of Global Technology Practice	(612)-906-3438
<b>Benchmark Executive Search</b> Jeremy King, President	(703) 728-8506	<b>McDermott + Bull</b> Chris Bull, Managing Partner	(949) 529-2690
<b>Bowdoin Group</b> Paul Manning, Managing Director	(781) 263-5200	<b>McIntyre Associates</b> Jeff McIntyre, President	(860) 284-1000
<b>Carter Baldwin Executive Search</b> Jennifer Poole Sobocinski, Partner	(678) 448-0010	<b>Momenta Partners</b> Ken Forster, Executive Director	(917) 765-3600
<b>Champion Scott</b> Geoffrey M. Champion, CEO	(617) 367-0444	<b>N2Growth</b> Kelli Vukelic, CEO	(800) 944-4662
<b>CIO Partners</b> Joe Gross, President	(770) 971-0324	<b>Odgers Berndtson</b> Steve Potter, CEO	(212) 972-7287
<b>Comhar Partners</b> Bernard Layton, Managing Director	(415) 903-4000	<b>ON Partners</b> Baillee Parker, Partner	(612) 825-4215
<b>Cyber Exec Executive Search</b> Jean-Louis Lam, Managing Partner	(312) 568-6748	<b>The Onstott Group</b> Joe Onstott, Founder	(781) 235-3050
<b>CyberSN</b> Deidre Diamond, Founder and CEO	(857) 415-2650	<b>Quest Groups</b> Joe Kosakowski, CEO	(857) 305-2116
<b>Daversa Partners</b> Joe Patalano, Managing Partner		<b>Riviera Partners</b> Will Hunsinger, CEO	(877) 748-4372
<b>DHR Global</b> Sal DiFranco, Managing Partner	(312) 782-1581	<b>Russell Reynolds Associates</b> Nada Usina, Managing Director	(305) 717-7400
<b>Direct Recruiters</b> Ryan Lange, Partner	(440) 996-0593	<b>Slone Partners</b> Leslie Loveless, CEO	(888) 784-3422
<b>Diversified Search Group/Alta Associates</b> Joyce Brocaglia, CEO	(908) 806-8442	<b>Spencer Stuart</b> Greg Sedlock, Consultant	(203) 324-6333
<b>Egon Zehnder</b> Eric Anderson/Jens Stender, Global Leads	(404) 836-2800	<b>SPMB</b> Kevin Barry, Managing Partner	(415) 924-7200
<b>Executive Search Partners</b> Gary Erickson, Managing Partner	(248) 470-9976	<b>StevenDouglas</b> Steve Kalisher, SVP/Michael Beaton, Director	(954) 385-8595
<b>Heidrick &amp; Struggles</b> Rebecca Foreman, Global Managing Partner	(415) 291-5215	<b>True</b> David Winch, Partner	(646) 741-2585
<b>Heller Search Associates</b> Martha Heller, CEO	(508) 366-7005	<b>Wilton &amp; Bain</b> Erin Callaghan/Chloe Watts, Partners	+44 (20) 7621 3570
<b>Hightech Partners</b> Raffaele Jacovelli, Managing Partner	+32 475 733348	<b>ZRG Partners</b> Dona Roche-Tarry, Global Practice Leader	+44 (20) 8075 8677

## SPOTLIGHT

## The Ins and Outs of Finding Cybersecurity Leaders



*Sophie De Ferranti joined **ZRG Partners** in 2021 as managing director, cyber, and member of the financial services practice. She has served as a keynote speaker on the topic of the war for cyber talent at events in Singapore, Zurich, London, Hong Kong, and Jakarta and participated in TV interviews with the London*

*Stock Exchange on regional compensation trends impacting senior executives within the global financial services industry.*

*Ms. De Ferranti has created a global footprint and highly entrepreneurial approach to executive search and human capital consulting. Her areas of expertise include global wealth management, cybersecurity and digital risk, and human capital management within the financial services/fintech industries. Ms. De Ferranti recently sat down with Hunt Scanlon Media to discuss the cybersecurity sector and the challenges of finding senior leaders for leading organizations.*

### **Sophie, can you provide an overview of cybersecurity recruiting?**

With almost 10 years of executive search and human capital management experience within global cybersecurity, I have witnessed an unprecedented shift during the last 18 months, not only in demand for stellar cyber talent, but also in compensation differentiators particularly in relation to the CISO and global CISO function. What is so fascinating about recruiting within cybersecurity is that it is truly industry agnostic and almost each and every sector, industry, company – irrespective of size, turnover, profitability, headcount, and geography – is exposed to the risks associated with cyber resilience and data security. Mitigating these risks, either through the deployment of advanced infosec technologies, cyber insurance, and, most importantly, human capital, will present the biggest challenge for the immediate to mid-term future as the world emerges from a global pandemic – a pandemic that has served to fuel cyber-crime/dark web activities and that has exposed weaknesses within a new dawn of hybrid and remote working practices. The world, and indeed we in our capacity as recruiters are facing what one may define as a full-on war for cyber talent. And, of greater concern, in the absence of any accelerated, strategic investment in specialized cybersecurity training academies to help stimulate next-generation education within cybersecurity, the talent gap is only set to widen.

### **How difficult is to recruit cybersecurity executives?**

In short: complex. Cybersecurity recruitment in the current landscape lacks succession planning and to some extent stability – the latter which has been fueled by a significant uptick in COVID-related cyber breaches and the associated disruption for those who are assigned to managing an organization's cybersecurity program. In the event of a cyber breach it is often the CISO who "carries the can" and thus a reactive event occurs;

firing and knee-jerk hiring, compounded by a lack of available interim CISO talent solutions. Hence, the tenure of today's traditional CISO (if there is "traditional" one) has been dramatically shortened from an optimal three to five years to just less than two to three. Harnessing top percentile talent should be a primary focus over the next three to five years if the talent deficit is to be realistically benchmarked, and the next generation of infosec/cyber executives identified. Further, one of the key challenges for recruiting senior cybersecurity executives in 2022 and beyond will most likely be:

- Inflated compensation (otherwise known as the "comp pain threshold").
- Diversity (not only gender diversity, but ethnicity, disability, and cultural diversity).
- Increased cybercrime, cyber breaches and the resulting need for enhanced/evolving cybersecurity software solutions.
- An acceptance from C-suite / board members to acknowledge cybersecurity as risk and not purely technology. There is a need to elevate the CISO out of CTO/CIO/COO reporting lines into the realm of the CEO and board. CISOs need the autonomy, resources, and empowerment to act and make decisions accordingly.
- Geographical regulatory differentiators driving the need for enhanced/recognized specialist cybersecurity qualifications which, in turn, determine the credibility and suitability of a CISO.

### **What is the current demand for CISOs?**

The current demand for CISOs (and to some extent senior infosec executives) is accelerating at a staggering 28 to 30 percent year on year. Global statistics suggest that this is set to increase and greater cross pollination across industry and sector specialism will occur (most likely we may see greater public-to-private sector migration) as the private sector lures away top performing public sector CISOs with massive salaries. Based on data captured across nearly 1,000 CISOs surveyed globally in 2020 and 2021 by Cyber-i-Search Solutions in the U.K., the following industries are seeing the greatest demand for new CISO talent: Financial services / fintech; healthcare, biotech, and life sciences; government, public sector, and not-for-profit; professional and technology services; hospitality and tourism; industry, manufacturing, and energy; consumer; and retail/marketing.

### **What value do CISOs bring to organizations?**

The best CISOs not only bring a wealth of highly technical expertise to an organization, oftentimes having originated from within a previous high-tech and infosec orientated role, but the "modern" CISO also now brings a strong commercial acumen with their skill-sets. They are more risk and compliance astute, may play the role of an individual revenue contributor, and are seen to be strategic relationship builders within an organization. They require not only the depth, breadth, and specialism of a range of data security

*(cont'd. to page 7)*

methodologies (e.g. network & cloud security, IoT, application security, identity and access management, security architecture, enterprise crisis management, penetration testing, and more), but are more commonly now empowered with greater governance, risk and compliance responsibilities – all of which elevate the CISOs standing within an organization – irrespective of geography, industry, and size. The CISO should, in today's world of heightened cyber risk, sit firmly within the C-suite thus giving them credibility and the necessary remit to best protect their organization, employees, customers, data, and most of all, their reputation.

*“The CISO should, in today's world of heightened cyber risk, sit firmly within the C-suite thus giving them credibility and the necessary remit to best protect their organization, employees, customers, data, and most of all - their reputation.”*

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

Having interviewed a significant number of CISOs globally – pre, mid and post pandemic — CISOs are calling for greater acknowledgement that cybersecurity really does sit firmly within risk and not just technology. Gone (or soon to go) are the days of the modern CISO reporting into a CIO, or perhaps a CRO or even CTO. There are multiple dotted and fixed lines of reporting that have since emerged which now define the stance and importance of a CISO within an organization – including board level reporting, enhanced autonomy, budget, team build, and an overall bird's-eye view of the actual risk exposure of an organization to a potential cyber breach. A good CISO will build strategic relationships with key internal stakeholders and decision makers on the technology front and will adopt a top-down approach to best protecting the organization's infrastructure, employees, data, and, of course, reputation – the latter of which is always the most difficult to mitigate (and repair).

#### ZRG's Cybersecurity Practice

ZRG's team of technology search professionals has delivered board and leadership projects for Fortune 500, mid-cap, and SMEs as well as private equity, pre-IPO, and venture-backed clients in the technology sector and for tech enabled businesses.

“Cybersecurity is a prevailing strategic priority for most/all of our clients, whether their domain is financial services or consumer/retail or private equity backed manufacturing,” said Larry Hartmann, CEO of ZRG. “We at ZRG are thrilled and emboldened to be positioned at the tip of the spear in advising corporate management teams and their boards on the right talent solutions to develop and enhance robust capabilities along the continuum of defensive and offensive cyber initiatives.

ZRG and a number of its rivals, reports Hunt Scanlon, are positioning themselves to take advantage of a rapidly maturing business need that is expected to come from clients in the U.S., Europe and Asia as the rush to build out global cyber leadership solutions quickens.



## PROVIDING PEOPLE SOLUTIONS

Our global platform of over 400 teammates and our tech-powered solution kit help you build where it matters most – from the top and heart of your organization.

Our core offerings include revolutionary, data-based, executive search focusing on senior leadership, a suite of on-demand talent offerings, and consulting and advisory solutions focused on key issues like culture, strategic alignment, coaching, and sales optimization.

**Providing people solutions for the most complex talent issues.**

**EXECUTIVE SEARCH** **INTERIM SOLUTIONS** **CONSULTING & ADVISORY**



**BETTER DATA.  
BETTER DECISIONS.**

1.201.560.9900

[ZRGpartners.com](https://ZRGpartners.com)

## SPOTLIGHT

## Finding Cyber Talent in a Hyper Competitive Market



*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 to share his thoughts on the competitive cybersecurity recruiting landscape.*

**Matt, what are you currently seeing in the cybersecurity executive search market?**

The cyber market for talent is fierce across the board with demand for security talent far outweighing supply. Practically every organization has open security regulations at various levels, and the market pressure is pushing compensation higher at all levels. At most levels and for most hires, organizations are up against competing offers, counter-offers, and a talent pool that is more attuned with what the market is paying, which is raising salaries upwards.

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

CISOs know they have a myriad of options and in some cases can name their own price; this pressure makes it more difficult to land and retain strong cyber talent. Based on the findings in our CISO survey, two-thirds of CISOs are open to new roles, but last year only 17 percent actually changed jobs – CISOs will have conversations, but won't necessarily make the move. Lastly, in this environment where two-thirds of CISOs report they are satisfied in their current role, it makes more candidates susceptible to accepting counter-offers from their current employers, something that was an outlier event two to three years ago, but we see on a regular basis today.

**Has this led to a higher demand from clients?**

There is continued pressure both from a regulatory perspective and market-driven to have an internal subject-matter expert in security who can not only protect the organization but can manage in crisis. CISO requirements depend on an organization's understanding (or misunderstanding) of the threat environment and their position in an ecosystem. A seat at the executive table, and ability to interface with the board, and be viewed on-par with other C-suite leaders in the organization. Teams and budgets aligned with organizational goals – CISOs can sniff out when a company is trying to do too much in cyber with too little support, and they will withdraw from a process if they get that sense.

**Why are CISOs essential for today's companies?**

Strong CISOs give organizations line-of-sight into tech risk, putting technical and cyber risk into business terms to enable better educated risk-based decisions. CISOs can also work in a commercial capacity, serving as a customer trust leader in front of customers. Typically more mature CISOs bring relationships with law enforcement and an incident response plan.

**What are clients asking for in CISOs?**

Clients are asking for more depth in cloud security and cloud transformation / migration. Additionally, in an increasing crowded cyber-vendor environment, the best CISOs have a pulse on the most impactful technology.

**How active were companies 20 years ago in this functional discipline (cybersecurity) and at what point did you see an uptick begin?**

Twenty years ago the cyber function was a buried IT function, with a focus on network administrator and firewalls / perimeter security rather than tech risk. The Target breach of 2013 kicked off leaders asking questions about security, this was cemented by the Sony breach in 2014, Anthem in 2015, and Edward Snowden's intelligence leaks in the same timeframe. Regulated industries were fastest to adopt newer-age cyber programming, though companies in the aforementioned affected industries also started to ask different questions than they had previously. Financial services started building their own cyber defense and offensive cyber programs to rival those of government intelligence agencies, and often pulling hires from those organizations.

**Who's most in demand at the moment?**

At a high-level, most companies are hiring at all levels, from security leadership to hands-on-keyboard engineers; the more in-demand talent is on the technical side of security. Organizations are continuing to scale, and we've heard clients and HR leaders, CISOs, etc. telling us they need to hire 10-20-50-100-300 people in their security organization as soon as possible.

**There seems to be a pervasive shortage of experienced senior leadership talent who can address the range and complexity of risk management. Why?**

We have to remember that until recently, security leaders were rarely formally trained in risk management, business management, or finance. CISOs who ascended to the top job a decade ago had previously spent a 15 to 20-plus year career entirely buried in the back office of a tech function. They never presented to senior leaders or the board, and everything which they solved from a security perspective came with a tech lens only. This is changing today, as companies provide mentoring to their security leaders, and CISOs spend more time with cross-functional leaders. Still, CISOs are not typically viewed as business partners on par with GCs, CFOs, and GMs...this will likely change over time.

Trust and Integrity  
are Paramount.



## Executive Search & Recruitment

### C-level & Direct Reports

- ❖ Information Technology
- ❖ Cybersecurity | Risk Management
- ❖ Software | Engineering | Technical Sales
- ❖ Private Equity | Venture Capital

**hirewerx** was founded with one goal in mind:

Deliver talent solutions that produce  
the best results for our clients.

Selecting high-performing leaders and  
teams requires assessment using  
data and predictive analytics.

We take pride in our  
thought leadership, domain expertise,  
network, and search execution.

**LEARN MORE**

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

Chicago | London | Singapore

## The Challenge of Recruiting Cybersecurity Talent

"Recruiting cybersecurity executives can be extremely challenging," said Frank Scarpelli, managing partner and chief executive officer 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 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."

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."

### Key Qualifications

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 10)

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.

#### Finding Technology Talent

Chicago-based HireWerx is a boutique talent acquisition solution provider specializing in serving technology and technology-enabled companies. Mr. Scarpelli has dedicated his career to building and scaling companies through strategic business initiatives focusing on strategy, people, process, and technology. With a strong understanding of technology and business, he leverages in-depth knowledge of skills, behaviors, competencies, and effective leadership characteristics to build high-performing teams and recruit top executives.

---

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

---

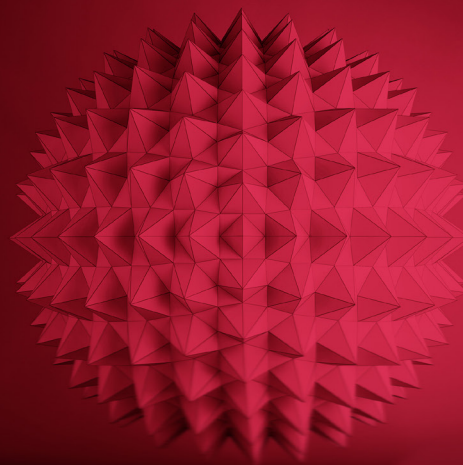
"There is a demand for talent like I haven't seen in over 20 years since the dot-com boom," Mr. Scarpelli said. "Our focus is on technology, so my perspective is influenced by our industry specialization. I don't see any slowdown in demand for the search industry on any level. I see it trending upwards. What's more, the fact that companies are hiring at the management and executive level remotely is really changing the game."

"Many of our clients, including Fortune 500 CPG organizations, were not negatively impacted over the past 18 months," said Mr. Scarpelli. "In fact, they saw booming sales growth. Because the pandemic has boosted digital acceleration, we are seeing rapid adoption of technology, which is what I believe is behind the productivity surge. We are seeing strong movement in the following sectors: medical technology, software, and SaaS, IoT, as well as wireless technology, especially in the area of 5G."

"As a firm, we are always adjusting our services to accommodate our clients' unique needs. I'd say the biggest change has been conducting virtually all of our meetings over video," Mr. Scarpelli said. "It has increased the frequency of face-to-face communication tenfold. And more face time is always a good thing."

**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](mailto:cyber@acertitude.com)

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

## TALENT | TECH TRANSFORMATION



### Enabling Digital Transformation through Talent Acquisition & Development

Whatever technological innovations are ahead, are the people that will make the difference between eventual success and failure.

Be disruptive.

Only tailored executive search and reskilling plans can boost your transformation journey.



HightechPartners

[www.hightechpartners.net](http://www.hightechpartners.net)

## Cybersecurity is the No. 1 Risk Leaders Can't Ignore

Increasingly, organizations of all sizes are awakening to the perils posed by cyber attacks. A new report from **IMSA Search** outlines the threats and dangers cybersecurity attacks and how to prevent them.

The risk of cybercrime to organizations of all sizes is escalating, with significant costs, and can no longer be ignored by business leaders. The Russian invasion of Ukraine, experts predict, will soon reach far beyond that country's borders, and affect us far more than at the gas pump. The Department of Homeland Security is warning citizens and businesses across the U.S. to be on high alert for cyber attacks from Russia. **Cybersecurity Ventures**, a leading researcher and online resource for the global cyber economy, projects global cybercrime costs to increase by 15 percent per year, reaching \$10.5 trillion annually by 2025. And according to global cybersecurity leader Trend Micro Inc.'s Cyber Risk Index Report – an annual survey of 2,800 IT managers and practitioners from the U.S., Europe, and Asia-Pacific – 26 percent of global corporations fell victim to seven or more cyber attacks in the past year, and over 80 percent of these expect such attacks to be “somewhat” or “very likely” to succeed.

Since the onset of COVID-19, the demand for enhanced cybersecurity – and cyber talent – across industries has increased exponentially, with specific needs to address the new realities of a world in pandemic mode. According to a new report by executive search network IMSA Search Global Partners, “As companies shut down and employees worked from home in unprecedented numbers, chief information security officers (CISOs) had to create secure connections for this extensive new remote workforce.” The surge in online commerce during the pandemic also required significant systems upgrades. “CISOs had to reallocate budgets to cover COVID-related costs, putting planned security improvements on hold and possibly exacerbating already identified risks and existing threats,” said the report.

“Prior to 2021, cybersecurity was increasingly a pressing topic in most board rooms,” said Steve Martano, a partner in the cyber practice at Artico Search, a leader in the cybersecurity talent space. “The advanced attacks and costly public breaches and ransomware events over the last 12 to 18 months have increased the frequency and depth of those discussions. COVID-19 and the work-from-home trend have accelerated the visibility of the CISO and the security apparatus, as endpoint security and vulnerability management became front and center due to the prevalence of remote work,” he noted.

That has made competition for top chief information security officers fierce as companies seek to protect themselves from potentially crippling cyber attacks. Newly released compensation data from IANS Research and Artico Search shows a wide pay gap, from small companies with nascent cyber programs to multinationals with well-established cybersecurity teams. Notably, female CISOs are out-earning their male counterparts. *(cont'd. to page 12)*

### Identifying Vulnerabilities, Understanding Consequences

The first step in defending against cybercrime is understanding risks and identifying where your systems are susceptible. Trend Micro's Cyber Risk Index says that the top cyber threats include: ransomware (malware that cryptically blocks access unless a ransom is paid); social engineering/phishing (techniques to trick people into providing personal data); clickjacking (concealed hyperlinks trick people into unintended actions revealing personal data and allowing control of one's computer); fileless attacks (tools built into software that allow attack and leave no code, file, or traceable footprint); botnets (unsuspecting network of computers infected by malware and controlled by a hacker); man-in-the-middle attacks (attacker intercepts communications between users, able to "eavesdrop" or alter the communications).

IMSA notes that certain situations present particular vulnerabilities: In automated buildings, every system and device are unique yet connected, each with its own unique cyber risks; and connected devices are easy to infiltrate. Healthcare facilities are high-value targets, with hackers launching constant attacks; medical records are "best sellers," fetching up to \$1,000 per record on the dark web, according to Forbes.

### Employee Training and Cybersecurity Policy

An essential component of a good cybersecurity plan is an up-to-date, readily available cybersecurity policy. "All employees, from entry level to the C-suite, should understand the policy and be trained to recognize and avoid security risks," said Mitch Berger, managing partner of IMSA Search Global Partners USA and an IMSA board member.

"Many of our clients in the C-suite and HR departments have told us that cybersecurity is now a prominent part of employee onboarding, with hands-on training about online information sharing, passwords and security questions, two-factor authentication for account access, and what to look for in emails and other communications which would signal a cyber threat," he said.

### Prevention is the Best Policy

The effects of any cyber attack can be catastrophic, resulting in business disruption, harm to company or brand image, customer loss, data theft, and in some rare cases, loss of life, according to the IMSA report. The costs can be catastrophic as well. Experts recommend companies get ahead of the problem, addressing vulnerabilities before cyber attacks occur, by implementing the following preventive measures:

- Identify and assess risk areas across applications, devices, and people.
- Implement the ability to automate responses to abnormal activity.
- Adapt systems to remotely resolve issues.
- Create policies and action plans for quick and effective response in the face of an attack
- Empower CISOs with appropriate budgetary and human resources to provide proper planning, training, and continual monitoring and upgrading of systems.



EXECUTIVE SEARCH  
PARTNERS

## Information Technology Search

Founded in 2003 by former  
Chief Information Officers

Executive Search Partners  
understands  
Information Technology

*"One of the top search companies  
in North America."*  
-Forbes



### CONTACT US

[www.execsearchpartners.com](http://www.execsearchpartners.com)  
[gerickson@execsearchpartners.com](mailto:gerickson@execsearchpartners.com)  
(248) 470-9976



## JDG Associates, Ltd.

A recognized leader in executive search since 1973.

Serving the executive recruitment needs of national trade and professional associations, federal and state agencies, and a broad range of research and consulting organizations for nearly five decades.

JDG's founding principle that all organizations must have the right people in the right positions echoes through every search we perform for our clients. Our mission is simple: partnering with our clients to impact organizational growth through a relentless commitment to uncover and deliver the best and brightest leaders of today and tomorrow.

[www.jdgsearch.com](http://www.jdgsearch.com)  
(301) 340 2210

## Top Cyber Searches Making News...

### JM Search Places Head of Cyber Services at Beazley



**JM Search**, a senior-level talent provider serving private equity investors, portfolio companies and Fortune 1000s, recently placed Russ Cohen as head of cyber services at specialist insurer Beazley.

He will be based in Philadelphia. Partner and co-IT executive practice leader, Ben Millrood led the assignment. "As the cyber risk landscape continues to evolve, organizations need to ensure their technology and risk management tools remain a top priority," said Raf Sanchez, global head of cyber services at Beazley. "Beazley has continued to innovate throughout the pandemic to ensure this need is always met, despite changes to working practices and increased ransomware attacks." JM Search's dedicated cybersecurity practice assists public and private equity-backed companies in identifying and recruiting high-performance leaders. Partners Kevin Kernan and Tom Figueroa co-lead the firm's center of excellence for cybersecurity leadership.

### ON Partners Recruits CISO for Bill.com

**ON Partners** recently assisted in the placement of Rinki Sethi as vice president and chief information security officer of Bill.com, a provider of cloud-based software. Spearheading the assignment was partner John Morrow.



Ms. Sethi will lead the global information security and technology functions, overseeing the protection of Bill.com's customer, partner, and employee data assets, and will advise the company on continued innovations in the security and technology space. With a primary focus on technology, consumer, industrial and the life science sectors, ON Partners recruits C-level and board talent for public and private companies, as well as venture capital and private equity firms. Mr. Morrow has 15-plus years in executive search. He has placed over 250 senior level executives in B2B software and B2B2C sectors.

### CIO Partners Called in by PropertySync to Lead CTO Search



**CIO Partners** was recently selected by PropertySync to lead their search for the role of chief technology officer. As PropertySync's exclusive search partner for this role, the search firm will conduct

the initial review of all candidates. Located remotely in the Pacific Northwest, PropertySync's mission is to transform the way title companies interact with their land record data and search process. The PropertySync platform was established from over 15 years of experience witnessing the repeated disappointments produced by alternative title plant software. As a result, the company was founded with the goal of creating the best real estate record management and retrieval system in existence. CIO Partners is focused on technology leadership searches across all industries and corporate sizes, from start-ups to Fortune 100 organizations.

## ...More Cyber Searches Making News

### Prodigy Search Helps Place Director of Security for the MLB Players Association



**Prodigy Search**, a boutique recruiting firm serving the talent needs of media, sports and entertainment organizations, has assisted in the recruitment of Carlos Barron as director of security for the Major

League Baseball Players Association. In this role, Mr. Barron will plan, direct, and coordinate programs relating to the protection, safeguarding, and security of company assets, employees, players, and invitees. Mr. Barron most recently served as director of security and transportation for the Houston Dynamo/Houston Dash/BBVA Stadium. He is also the founder of Salus Security Services. Earlier in his career, Mr. Barron spent nearly 25 years with the Federal Bureau of Investigation, serving as assistant special agent in charge.

### University of California Taps DHR Global to Find CISO

**DHR Global** has been enlisted to find a chief information security officer for the University of California (UC) Office of the President in Oakland. Leading the assignment are 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. The new CISO will report 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.

### CarterBaldwin Recruits CIO for CCRM Fertility



**CarterBaldwin Executive Search** assisted in the recruitment of Wade Lowder as chief information officer for Denver-based fertility service CCRM Fertility (CCRM). Jennifer Sobocinski led the assignment along with Ted Wieber. A seasoned senior healthcare

technology executive, Mr. Lowder will lead the CCRM information technology team through an expectation of significant growth, determining IT strategy and scale. Mr. Lowder joins CCRM from InnovAge, where he was senior vice president of technology and managed the IT strategies, administration and expansion as the company doubled in size. Headquartered in Atlanta, CarterBaldwin provides executive search services in the healthcare, technology, non-profit, consumer services, industrial and media/telecom sectors. Its clients include name-brand institutions, such as KPMG, ADP, Teradata, First Data, Duke University, Pepperdine University, New York Life, Fleet Pride, and Berkshire Hathaway.



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](https://temptingtalent.com)



[enquiries@temptingtalent.com](mailto:enquiries@temptingtalent.com)

Data taken from Tempting Talent's 2022 Compensation Report