ESR
Executive Search Review
A HUNT SCANLON MEDIA PUBLICATION No. 1 2016

CYBERSECURITY RECRUITING SPECIAL ISSUE

Scrambling for Cybersecurity Leaders is Big Business for Recruiters

In the mid-1990s, when Joyce Brocaglia took on her first assignment to help build an information security operation for Citibank, it was a very different world. No one knew how much the Internet would grow and ultimately transform society. Technology was more primitive. Data was less accessible. And the massive connectivity we now taken for granted was a distant dream. Yet that initial call from the banking giant, sparked by the audacious theft of $10.7 million by a Russian hacker and his accomplices in 1994, would be one of the seeds that ultimately grew into cybersecurity's rise as one of today's hottest sectors in executive search.

On The Hunt

Back then, it was all new terrain. Citibank had hired its first chief information security officer, Steve Katz, who wanted to go beyond technical security alone and deal with threats from the more encompassing perspective of business risk. Ms. Brocaglia and her colleagues at **Alta Associates** helped Citibank build out its core information security group of perhaps 30 people. But in the bigger picture of protecting corporations from cybercrime, that was just the beginning.

Unprecedented Demand for Cyber Talent

Citibank's broader approach would reverberate down through the years. These days, it is more relevant than ever. "When we do searches today for cybersecurity officers we are still transitioning organizations from that old fear, uncertainty, and doubt mindset into a newer way of thinking," says Ms. Brocaglia. "It's a much more collaborative, strategic approach to figuring out how information security can actually add value to an organization in terms of generating revenue, protecting brand and protecting reputation." Cybersecurity, she said, "has gone from being a completely back-office role that was often

Hunt Scanlon CYBER 20

Company Name	Practice Leader	Contact Information
680 Partners	David Feligno	david@680partners.com
Alta Associates	Joyce Brocaglia	joyce@altaassociates.com
Benchmark Executive Search	Jeremy King	jeremy@benchmarkes.com
Bridgen Group Inc.	Julie Bridgen	jbridgen@bridgengroup.com
Caldwell Partners	Jim Bethmann	jbethmann@caldwellpartners.com
DHR International	Peter T. Metzger	pmetzger@dhrinternational.com
Diversified Search	Tony Leng	tony.leng@divsearch.com
Egon Zehnder	Kal Bittianda	kal.bittianda@egonzehnder.com
Heidrick & Struggles*	Phil Schneidermeyer	pschneidermeyer@heidrick.com
Indigo Partners	Veronica Mollica	vmollica@indigopartnersinc.com
JM Search	Tom Figueroa	figueroat@jmsearch.com
Kaye/Bassman - Sanford Rose Associates	Alexander Ross	aross@kbic.com
Korn Ferry**	Jamey Cummings	jamey.cummings@kornferry.com
Russell Reynolds Associates	Matt Comyns	matt.comyns@russellreynolds.com
SI Placement	Kathy Lavinder	klavinder@siplacement.com
Spencer Stuart	Anthony Laudico	alaudico@spencerstuart.com
SPMB	Andy Price	andy@spmb.com
TD Madison	Dean Madison	dmadison@tdmadison.com
Work&Partners	Alan J. Work	ajw@workandpartners.com
ZRG Partners	Stephen Spagnuolo	sspagnuolo@zrgpartners.com

*Matt Aiello, practice co-leader; based in Washington, D.C. **Aileen Alexander, practice co-leader; based in Washington, D.C.

buried way down in an organization to a much more highly central and strategic function that is really getting a lot of interaction with the board and with outside organizations."

Certainly, much has happened over the two decades since that landmark breach at Citibank, both in terms of cyberattacks and hunting for professionals to protect companies from such intrusions. As cyber breaches and their consequences have grown more expansive and menacing, information security talent is in unprecedented demand. In many ways, the changes feed into an even broader trend toward specialization in executive recruiting and the rise of boutiques.

Collateral Damage

One of the problems all recruiters have been encountering is a candidate pool that includes professionals with weak career paths to becoming top cybersecurity leaders. Ideal candidates, they say, are generally well-versed in many parts of a business – not just in technology. But candidates possessing this cross-section of corporate experience can be like finding needles in a haystack.

Nevertheless, cyberattacks are growing in magnitude, complexity and frequency, and these massive security lapses have left many companies vulnerable. The growing list of major businesses that have been compromised has forced leaders from organizations of all sizes and across industries to pay heed: JPMorgan Chase, Target, Anthem, Sony Pictures, and Home Depot are just some of the bigger players to have been hobbled, not only by the intrusions themselves but by collateral damage to their corporate reputations and the weighty costs of recovering. As such, many cyberattacks have never been publicly reported. In some instances, companies have lied about breaches even occurring. And given the complexity of the systems in question and inadequate protections, it's anyone's guess how many intrusions have gone undetected.

BY THE NUMBERS

Why Demand for Cyber Leaders is Intensifying

Over **500,000** cyber attacks globally every day

Cyber spending will hit **$86 billion** this year

Source: Gartner

One study, by the Center for Strategic and International Studies, a Washington, D.C. policy research group, and McAfee, the technology security firm, puts the annual cost of cybercrime to the world economy at more than $400 billion and perhaps as much as $575 billion, to say nothing of the immeasurable ripple effects on businesses, communities, and personal lives.

Fueling the threat is the ever-expanding inter-connectedness of web, cloud, social, and mobile technology. There's also uncertainty about who these shadowy hoodlums might be, their motivations, intentions, and when they might strike. Certainly nation states like Iran, North Korea, and China have been implicated in a number of cyberattacks. Freelancers in Russia and Eastern Europe have done considerable damage, as have corporate competitors and whistleblowers. Even an adolescent hacker with too much time on his hands can cause damage. Who can say whether the perpetrator seeks to upend the economy, pilfer intellectual property, take revenge for a perceived insult, or is just bent on wreaking havoc?

All of us have access to information like never before. And we're communicating through vast networks that are linked in one way

The Global CISO

Why U.S. Leaders Must Think Beyond Borders

To compete for the top cybersecurity jobs on a world stage, home-grown CISOs need to take a more international approach to professional development. This advice comes from Kal Bittianda, who heads up the cybersecurity recruiting practice at **Egon Zehnder**, one of the largest global talent providers. At Zehnder, Mr. Bittianda has a unique vantage point to see what companies are looking for in their next CISO – and what the CISO talent pool is offering. He conducts executive search and provides leadership development services to help companies leverage technology to drive growth, transformation and innovation, while managing emerging leadership opportunities and challenges, such as cybersecurity and big data.

Here are three things that he says cybersecurity leaders in America can do to stay in step with a wider world:

Keep your bags packed. American cybersecurity leaders aren't only reluctant to consider job offers outside of the country; many won't even look beyond their metropolitan area. Increasingly, American CISO candidates will be taking themselves out of consideration for prime appointments unless they are prepared to relocate in the same way that other senior executives are expected to in the course of their careers;

Get mentored. If you are at a company with international reach, a good way to develop a global sensibility is to be mentored by someone for whom it is an essential part of their job. That might be the head of a business unit, or someone like the CFO, general counsel or head of compliance, who has to operate across a range of regulatory regimes and sensibilities;

Look outside the office. If your company doesn't have the global footprint that can provide exposure to different cultural and regulatory systems (and even if it does), consider a volunteer leadership role for a non-profit or professional organization with an international mission. In addition to broadening your perspective, you will be expanding your network in ways that may bring unexpected benefits down the line.

"The expectation that cybersecurity leaders can work across borders as do their counterparts in other functions is just emerging," he says. "But it will surely gather momentum as economies become truly global." Although developing a global perspective is a long-term undertaking, he added, current and future CISOs who start now can help ensure that their professional development keeps pace with the needs of the talent market. "It's an alignment that makes for better security for everyone."

or another. "As a result, more people are exposed to the risks and there's more value in hacking into an account or phishing an account," says Kal Bittianda, who heads the cybersecurity search practice at **Egon Zehnder**. "There's more commercial value, whether it be for individual hackers or crime syndicates, and then of course there's political activism and country-to-country activity as well. All of that means that the level of activity is a multitude of what it was 20 years ago and the number of people affected by it is pretty much everyone who's connected online."

In the early 2000s, a major change in the types of attacks began to emerge. Nation state attacks were coming with more sophistication and frequency. "The market's been coping with this level of sophistication for the last 15 years," says Matt Comyns, who heads the global cybersecurity recruiting practice for **Russell Reynolds Associates**. "However, if you talk to veterans of this field they will also tell you that the last three to five years in particular have seen tremendous scale of attacks – their volume and complexity has increased dramatically." Therefore, he says, "the awareness at companies around the world has increased significantly, highlighted by the consequences of the attacks on Target and Sony, in particular."

Top Cyber Recruiting Specialist

Cyber Expert Matt Comyns

Matt Comyns is global cybersecurity practice leader at **Russell Reynolds Associates**. He recruits chief information security officers (CISOs) and next level down top lieutenants in information security for large global corporations and fast-growing private companies. He also recruits cybersecurity consultants for leading professional services firms and top executives for cybersecurity technology companies.

Cybercriminals come in all shapes and sizes. And efforts to fend them off are in many ways just getting started. "It's almost multi-sector if you want to put corporate-speak to it," says Stephen Spagnuolo, who was hired last spring to help launch **ZRG Partners**' cybersecurity and defense-intelligence search practice. "You have entrepreneurs. You have emerging growth players. You have large corporates, the nation states. And the numbers don't really matter. One bad dude could do a lot of harm to many points for a long time. It's not a numbers game. It's a will and commitment game. And it's going to take an entire generation to even approach battlefield balance."

ZRG Partners, with headquarters in Rochelle Park, NJ, is a mid-sized search firm that conducts assignments across a broad range of industries, including aerospace and defense, consumer, cybersecurity, financial services, and healthcare, among others. Its recent cybersecurity recruitment and advisory work has seen a search for a CEO of a prefunded cybersecurity company, a COO and board member for an early stage cybersecurity services firm, and a head of business development for an emerging growth cyber analytics software firm. ZRG today has offices around the U.S., as well as in Canada, Switzerland, the Netherlands, China, and Hong

Kong. Clients in these locations all need need cybersecurity talent as much as their American counterparts.

The need for cybersecurity executives reaches across virtually all industries. Information security analyst jobs are expected to grow 36.5 percent by 2022, according to the U.S. Bureau of Labor Statistics, with 27,400 new jobs being added. Areas like financial services, defense, and high technology have long focused on cybersecurity. But retail, healthcare, entertainment, utilities, and others have stepped up their efforts and are now seen as bolstering their defenses in the face of security breaches. All of these sectors recognize that information security is the ultimate competitive advantage. "Any B to C business is focusing very aggressively on it now, in a very public fashion," says Mr. Bittianda. "B to B businesses are doing it behind the scenes."

Demand is picking up just as risk and security executives are being elevated to the C-suite – turning security breaches into a C-suite problem. It is this convergence that is the result of what is now seen as a highly visible leadership need as well as a strategic imperative for every company.

High demand and limited talent supply lines are leading to bidding wars throughout the security sector, says Mr. Comyns, as cyber-security transforms from an independent, functional focus to a full-fledged integrated business sector. With the shift, talent demands have come to exceed the available supply by a widening margin.

It would be tough to ignore the growing number of cyberattacks and the damage they have wrought for their corporate victims. "I think that growth can be completely attributed to the growing cyber threats as well as companies becoming more aware of threats and the challenges that are associated with addressing them both from an internal and external perspective," says Marci McCarthy, CEO and chairman of **ISE Talent**. "When you start putting a price tag on some of these breaches, from credit monitoring and class-action lawsuits as well as personnel changes and then potential loss of customers and trust, you're looking at a severe wakeup call for boards of directors, management teams and shareholders alike."

ISE Talent, based in Atlanta, focuses only on recruiting information security executives and professionals. The boutique firm, which spun out of T.E.N., a national technology and security executive networking organization run by Ms. McCarthy, was officially launched early last year. The firm has conducted searches for chief information security officer (CISO) / VP equivalents as well as security team members like security managers, security engineers, cyber analysts, and enterprise security architects. Among its clients are Fortune 1000 businesses as well as security solutions providers.

In short, all the commotion means that business over the next few years and beyond should be brisk for executive recruiters who specialize in finding cybersecurity talent and have an established network of candidates and sources. Newcomers, on the other hand, may find it less than welcoming. "There's a considerable amount of barriers to entry," says Ms. McCarthy. "You can't just have an IT search firm, then wake up one day and do information security searches. The security profession is about trusted relationships."

Stunning Admission

The Unprepared CEO

Half of the CEOs recently surveyed by **KPMG** admitted they were not fully prepared for a cyber event. Yet, cybersecurity was named by 20 percent of respondents as one of the top five risks – right behind the related issues of third party and supply chain risks. For technology firms, information security edged out all other risks as the most pressing threat. How prepared are you for a cyber event? "Any CEO who really understands risk knows that cyber is possibly the most unpredictable risk there is," says Malcolm Marshall, KPMG's global head of cybersecurity. "It's more unpredictable than a flood or tornado." Many CEOs might believe they are well prepared for a cyber event because they have invested so heavily in detecting and preventing an attack, adds his colleague Greg Bell, KPMG's U.S. cyber leader. You still have to demonstrate due care on prevention, he said, "but until recently, there has been too much attention focused on prevention and not enough on protection and response."

Plans to appoint a cyber security executive/team

Have taken preemptive steps	50%
Planning to take steps in the next three years	29%
No planned action	21%

Scrambling to Play Catch-up

As companies scramble to play catch-up in cybersecurity, too few qualified candidates are available to fill all the openings for roles like CISO, directors of information security, chief technology officers, and heads of information technology – driving up compensation, in some cases igniting bidding wars, and oftentimes leaving critical roles unfilled. A number of companies, in fact, avoid publicizing or even discussing their openings for fear of attracting cybercriminals who might consider them vulnerable. Search firms, too, report a burgeoning number of calls for candidates with cybersecurity expertise, especially chief information officers, to serve on boards.

There's also been movement away from more traditional roles like chief security officer, which predominantly handles physical security, and the CISO, which focuses on information technology protection, says Jeremy King, president of **Benchmark Executive Search** in Reston, VA. More corporations are developing a new role, chief risk officer, to oversee the full range of risk exposure. "Bank of America went this direction in the wake of its big breach and more companies are following suit," he says. In fact, Mr. King expects the role to be among the hottest in the cybersecurity sector in the next few years.

Board risk committees, meanwhile, are already a way of life in the financial services industry, but Mr. King expects other industries will follow suit. The biggest challenge is that corporate leadership must come to terms with the enormity of the cyber threat. "It seems like the best way to focus attention on this will be for CEOs to step

out front," Mr. King says. "We believe that boards are taking these threats seriously and will begin to assign an individual on the board to oversee all risks. Physical security, IT security, personnel security and certain aspects of compliance and legal are all components of risk. But with most new corporate initiatives, they do not bubble up but work top down. Companies need a holistic enterprise risk management framework tailored to their business and applied rigorously by management while routinely overseen by the board of directors."

Peter T. Metzger, vice chairman at **DHR International**, who specializes in recruiting for cybersecurity, is emphatic that companies must make systems protection a top priority. "This should be one of the top three agenda items at every board meeting every quarter," he says. "When you talk about a risk analysis, this is you-bet-the-business every single day."

Don't Expect to Stamp Out Cyber Threats

Despite a long history of attacks, and largely because of them, financial services companies are probably the most advanced in their cyber protection capabilities. Their people are frequently tapped by firms looking for top cybersecurity talent.

Turnover can be high for many cybersecurity roles. Supply and demand is a major consideration. "There are not many of these folks out there who are operating at the top level," explains Tony Leng, a managing director at **Diversified Search**, who heads the firm's San Francisco office. "There are some. What you find is that they get poached one firm to the other."

Recently, Diversified recruited a head of cybersecurity risk management for a major West Coast utility, a CISO for a major healthcare provider in the Northeast, and a CISO for a Fortune 200 consumer products company. Based in Philadelphia, Diversified is among the top 10 search firms in the U.S., with offices in nine cities.

David Feligno, vice president with **680 Partners** in New York, says the demand for talent reaches into the information security vendor market as well. "The cybersecurity industry is extremely competitive," he says. "As a recruiter, you have to latch onto companies that you can tell a good story with, that are performing well within the market, that have teams that are extremely innovative, very collaborative, and that are culturally a place that people would want to go."

That said, it is a candidate's market. "They have a lot of opportunities available to them," says Mr. Feligno. "So getting candidates excited, getting them into the vendors that we work with and keeping them there, getting them through the process, and then closing the deal is certainly a tough thing to do."

680 Partners, founded in 1999, is a boutique search firm that helps find senior managers for a range of technology, software, Internet, and e-commerce companies. In addition to cybersecurity vendors that Mr. Feligno has known over his professional career, his firm is introduced to many others through PE-VC firms with whom the firm has longstanding relationships. "We've worked on sales, marketing, operations, software engineering, support, professional services, product management, product marketing, and executive positions to oversee one of those particular departments as well," says Mr. Feligno.

For industry in general, client companies often erroneously expect their cybersecurity teams to completely stamp out cyber threats. Company leaders can sometimes be too quick to cast blame when their firm is breached, turning cybersecurity leaders into fall guys when in truth they were doing the best they could with the budget and resources they were given. Furthermore, no one can repel every attack. Cybercriminals are too numerous, too wily, and too relentless. And they always have new schemes and techniques in the works. "The burnout factor of the security executive is quite high," says Ms. McCarthy, of ISE Talent. "There's an expectation of, 'You're going to solve our problems, tell us what our problems are, and then when something does happen you are the scapegoat.'"

DHR's Peter Metzger, who operates out of the firm's Washington, D.C. office, says that when breaches occur – and they are inevitable, he says — company leaders should take stock of themselves. If they have failed to take proper precautions in terms of talent and action, it is they who hold the responsibility. "What the shareholders ought to do is fire the CEO and some of the directors if this happens," Mr. Metzger says. "If it's shown that they're not taking it seriously enough, then there's a problem."

Trusted Advisor

DHR International, headquartered in Chicago, is the sixth largest U.S. search firm and its growth has been rapid in recent years. Like many of its rivals, the firm has expanded into assessment and leadership development. The firm's CEO, Geoff Hoffmann, said: "Clients these days demand an integrated approach" to talent management. "As their needs evolve, we are being looked upon to find answers in specialization and advisory services."

The firm's assignments in the cybersecurity sector include recruiting a senior partner who had led the cyberrisk practice at one of the big four consulting firms for the world's largest health insurance provider. DHR also recruited a top cybersecurity leader for a Fortune 50 American manufacturing company that had been breached by China. That mandate involved significant U.S. government oversight, says Mr. Metzger, and was preceded by extensive consultation to ensure that all parties understood the scope of the project.

Corporate culture also carries a big part of the load to keep businesses safe from intrusion. Employees have to buy into security policies if protection efforts are going to be effective. Companies with a laissez faire culture must alter some of that thinking, say recruiters, at least when it comes to cybersecurity. Disgruntled workers can also cause a lot of difficulties, both directly and indirectly. A simple lack of diligence can open the doors of the kingdom to cyber marauders.

"At the end of the day, it's the cultural outlook," says Julie Bridgen, managing director and CEO of the **Bridgen Group** in Brantford, Ontario. "You have to have people who want to protect the organization." Indeed, any sensitive information that is compromised has the potential to be harmful. Carelessness can be a big factor. Even emails and Twitter posts can cause problems. "You can have a whole room of people who spent a year coming up with their company's forecast for the future, and then in a sweep of an intrusion they can have to rethink an entire year's worth of planning," says Ms. Bridgen.

The Bridgen Group, formerly affiliated with the Canadian search firm Donaldson & James, this winter became partners with Vicinage, an international network of nearly 500 CISOs, based in Annapolis, MD. The Bridgen Group specializes in cybersecurity searches for senior to C-level executives and response teams. The firm recently recruited a senior team leader for the cybersecurity assessment and analysis group, who reports to the director of cybersecurity, of a St. Louis-based company. Among the roles that Bridgen Group helps fill are CISO, board positions, chief information officer, forensics experts, and security software developers.

Manhunt for Cyber Specialists

Bridgen Group Goes Covert

Bridgen Group identifies C-level security professionals and cyber threat response teams for clients nationwide. Cryptanalysts, disaster recovery analysts, forensics experts, security architects, virus technicians, web penetration testers, intrusion detection specialists, security software developers, source code auditors, and security engineers are just some of the cybersecurity specialists the firm hunts for nationwide.

Few companies have a formal risk management process in place, says Mr. King, of Benchmark Executive Search. "But the more important question might be: How many companies have created a culture of security, implemented policies, and allocated real resources for implementation?" he says. "Risk management is very complex. It takes strong people, processes, technology, and almost ruthless commitment by an organization's top leaders."

Finding good cybersecurity talent can be a challenge. Too few people specialize in this area, and the market has moved rapidly in just a short period. There's simply more demand than the market has been prepared to handle, for senior roles as well as junior positions. "To further exacerbate the pressures on the human capital pool, companies are requiring these people to do a lot more than they did previously," says Russell Reynolds' Matt Comyns. "Their roles have expanded tremendously. So not only do we not have enough people doing it, but now we're asking incoming leaders to do more. So to get people who can handle the new role and responsibilities and do that at scale to keep up with demand is very challenging."

Pay is Inconsequential

Given the new and evolving nature of top cybersecurity roles, recruiters oftentimes tap candidates from related and tangential fields to fill these positions. Many have IT backgrounds, including management experience in security. Some come out of internal audit positions. Others have government and military histories in places like the Department of Defense, the U.S. Cyber Command, the NSA, or organizations like the FBI.

With demand for cybersecurity talent high, supply low, and companies urgently seeking to fill a myriad of positions, compensation is skyrocketing. "I watched one person go from making $200,000 a year to $650,000 in three years," says Mr. Comyns.

Information security leaders at major companies typically earn upwards of $500,000 to $600,000 a year, including base salary,

bonus, and long-term incentives, Mr. Comyns says. And while many companies are still struggling with the reality that an annual range of $250,000 to $400,000 for a top-fight cyber executive might be, in fact, no longer enough, Mr. Comyns says that 10 percent of the market will pay a good deal more than $600,000 a year to lure the right executive. Perhaps they've come to realize that some top banks and Fortune 50 companies have already settled on a new reality: you have to pay up for the best. Mr. Coymns says stand-out cyber security leaders can make $1.5 to $2 million a year.

Mr. Comyns recently recruited chief information security officers for a Fortune 100 company, one of the largest global retailers, a leading global automotive supplier, and one of the largest online / offline brokerages as well as a chief technology officer for a global multi-channel media company.

Mr. Metzger says that he's pointed out to clients on numerous occasions that high pay for cybersecurity talent is inconsequential compared to the devastation that an attack can produce. "If you want to protect your bank, what difference does it make?' he asks. "One breach can mean multiples of that compensation package. And the reputational loss is enormous."

Talent CSI

Forensics Investigator Turns to Talent Acquisition

Kathy Lavinder founded **SI Placement** in 2000 after working as director of complex investigations with IGI, a preeminent corporate intelligence firm. After a decade there, she turned to the challenges of talent acquisition. She now focuses on finding high caliber investigators with capabilities in fraud detection and prevention, anti-money laundering, financial misconduct, electronic investigation, forensic accounting, business intelligence, due diligence, and litigation support), and senior level security management experts.

Sometimes, too, clients resist a recruiter's suggestion to consider candidates from a business that has suffered a major cyberattack. Public perception is at stake, after all. "My contention is that's probably the best place to go because there have been some serious lessons learned," says Mr. Leng. "But they're worried about that image."

Clients must understand, too, that proper security involves far more than simply finding a talented individual and hiring that person. They have to have given thought to a bigger plan. "They will say, 'I want to hire a CISO and here's a laundry list of things we want to do and what we want to pay them,'" says Ms. Brocaglia of Alta Associates." And we'll say, 'Well, you're either going to have to pay them more, or expect less.' They're often unrealistic. We'll ask them, 'When they come on board are you going to let them build a team?' And they'll say, 'I don't know.' 'What's their budget going to be?' 'I don't know.' 'What's the organization going to look like?' 'I don't know.' And we'll say, 'Well, maybe you guys need to think about this.' Oftentimes, that leads to some drilling down with clients to try to answer those hard questions."

"What I try to explain to them is that the market is so competitive that unless you really have a mission, a direction, and most importantly the support of your senior executive board, you're not going to attract the kind of person that you need to do that important job because they're not going to step into a situation that they know is going to be difficult and have the bottom fall out from underneath them," she says.

Continued Gap in Cyber Talent Expected

In other words, companies must be prepared to pay for more than just a top cybersecurity leader. Teams of people are often needed to handle the expanding tasks at hand. The price tag may be high, but it's impossible to get around the necessity. "This is a total re-think for companies around the cost of doing business securely," says Mr. Comyns. "It's an ocean change. It's a new way of doing business. I don't know how else to say it. Unfortunately, it's a significant cost added to your business. It's the cost of doing business in today's world. And the sooner companies embrace that the better off they're going to be."

The best candidates for top cybersecurity roles, say recruiters, go beyond the technological skill base. The best cybersecurity leaders in place today seem to share one common trait: strategic perspective. And, they communicate well with top leaders. They also possess an open mind in an evolving world. "I tell all my clients, 'I'm going to find you somebody who can do this job today,' but really the currency of business nowadays is speed," says Diversified's Tony Leng. "And so your business is going to change. The world of hacking and theft and cyberrisk, that's going to change. So you need to hire the right level of leader who is able to understand the change and move effectively with the times and pivot and understand what's going on, constantly."

One thing is certain: Look for greater corporate awareness of cybersecurity in the years ahead. "We're going to see a continued gap in cyber talent," says DHR's Mr. Metzger. "We're going to see an increase in spending. We're going to see an increase in data analytics, which is very important in this field. And we're going to see a further proliferation of cyberattacks. This is a big business both defending and attacking right now."

As recently as seven or eight years ago, CISOs were much different from today, says Mr. Bittianda of Egon Zehnder: "They were introverted. There was a big focus on just technology skills. And they used to be more often than not the 'Dr. No' type who said, 'No, you can't do this; it will breach security.' Today what we're finding is someone who is much more extroverted, someone who can influence the board and the CIO, someone who is more of a facilitator, and someone who takes an interdisciplinary approach. So we're already seeing that pool of talent evolving in terms of who will be successful. Going forward, I think we're seeing it change even more, where they need to take much more of a multi-functional approach and risk-management type of approach."

The bottom line, says Mr. Bittianda, is this: "The CISO you're going to want to hire today is not the person you would have hired five years ago and will likely not be the same person you'd hire five years from now. So we look for things such as potential for

How Boards Should Tackle Cybersecurity

A 5-Point Checklist:

Boards increasingly understand that cybercrime is a risk management issue that affects the entire organization and requires board oversight. However, although directors know that they need to stay informed about cybersecurity, keeping up with it in the complex, rapidly evolving world of IT is often a challenge. Here are five recommendations from **Spencer Stuart** on how boards should tackle cybersecurity:

1. Acquire a high level of understanding of how your organization uses technology and potential vulnerabilities
2. Ask for a comprehensive annual review of your security program
3. Have an independent audit conducted
4. Review the breach response plan
5. Bring experts onto the board

someone to evolve as a way to figure out who may be the most effective hire." Mr. Bittianda's recent assignments have included a global search for a CISO at a top-five global enterprise software company, head of IT security for a Fortune 500 manufacturing firm, and a board director for a fast-growing cybersecurity business, among others.

Recruiters in this sector, almost across the board, speak of the satisfaction of helping companies find talent and solve their cybersecurity challenges. Most consultants in cybersecurity seem to feel they are truly making a difference. "I've combed the world to try to understand how people are approaching this, how people are thinking about it, and it is a full-time job to stay on top of it and then help companies think through it," says Mr. Comyns. "I've done other types of recruiting, where I've walked in the door and they're always happy to see you and partner with you. But in this functional area it's a whole different ballgame. Many of my clients lean forward across the table to hear what I have to say."

For recruiters focused on this sector, the business of finding cybersecurity leaders and teams of cyber professional talent to back them up has been exceptionally strong in the U.S. Increasingly, companies around the world are following suit. No one believes demand will ebb anytime soon.

"Starting last year we began to see the market pick up in Europe and now we're seeing the market pick up in Asia," says Mr. Comyns. "I'm probably going to be spending some time in Latin America and places like the Middle East. This is a global phenomenon." He says the U.S. is clearly more advanced in its investment against the challenge but it still has a long way to go. "We're years away from a mature market here in the U.S. And the rest of the world is many years behind us." Demand for human capital in the space will continue unabated, he says, for at least five to 10 years, but probably much longer than that. Others concur. "I think we're in the early innings of a doubleheader in terms of U.S. and global cybersecurity and security awareness," says ZRG Partners' Mr. Spagnuolo.

Q&A

Cybersecurity Recruiting Pioneer Looks Back, and Ahead

Alta Associates has risen over the past 30 years to become the most prominent boutique search firm specializing in the cybersecurity function. Founding CEO Joyce Brocaglia is a highly sought-after strategic advisor to her clients in the areas of information security, risk management and privacy. In the following interview, she discusses the evolution of the information security sector and the holistic approach she uses to find risk management leaders – and where the pitfalls lurk.

What events led you to settle on recruiting security and IT risk talent? I know you were retained by Citigroup in 1994 after the Russian incident where they hacked into the bank's computers. Was that your starting point?

Not exactly. My starting point was IT audit. Believe it or not, that was a hot growth area at the time. But yes, in 1994 the Russians hacked into Citigroup's computers and the bank then hired their first ever chief information security officer, Steve Katz. Steve then contacted me to build his information security organization. We knew that IT auditors were already looking at data centers and applications controls, and those people combined with folks coming out of the government and military made ideal candidates for what became the first ever information security organization for Citi. So fast forward 20-plus years and here we are.

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

Twenty years ago when we were recruiting information security officers the world was really a different place in terms of technology and the amount of data that employees, customers, and partners had access to. At the time the role was very focused on securing main frame systems and the perimeter. So we looked for people that were highly technical. There was a substantial pickup about four years ago when companies were starting to replace their existing technology leaders. A 'new' executive chief information security officer (CISO) evolved; one that had a much more holistic approach to risk management and who really enabled businesses by providing value and articulating solutions in a language that made sense to business leaders. Companies were asking us to find executives for them that really could become the face of their information security organization; who could increase the credibility of their department; who could influence their culture; and then constructively partner, sell and deliver their security initiatives globally to diverse businesses with various risk policies. So I would say, initially, that was the push of having a kind of an 'ah ha' moment where companies realized, the position itself needed to be re-elevated. I also think another driving force was the increased volume and complexity of cyber threats. So many companies were starting to see these types of attacks on their organizations. The result was that senior-level positions were being created because the board and the audit committee were starting to ask harder questions and regulatory requirements were demanding more compliance. These newly-created positions, therefore, began to really take more of a front office spot as opposed to just a back office technology function.

Obviously industries like financial services that need to protect the personal records of millions of individuals is clearly a prominent sector in need. What other industries are active?

Financial services is probably the most evolved for obvious reasons: They have been moving large amounts of data and money for years and are huge targets to nation states and individual hacker attacks. There have been many high profile breaches where millions of credit card customers' information has been compromised. These breaches were a wake-up call to many major retailers who thought that being compliant to regulatory requirements was enough to be secure. But now they are dealing with enhanced PCI requirements and they have received advice from consultants and auditors who were quick to point out there were vulnerabilities and risks in their policy-oriented security programs. They advised them to build more robust and formalized security organizations that quite often required them to bring on a first time CISO or elevate their current role by hiring someone who has much more strategic and leadership skills. Healthcare is another industry that has had a huge uptick in terms of their focus on information security, governance, IT risk, compliance and privacy. With the threat of cyberattacks on the U.S., the importance of protecting our energy grid and other utilities is more important now than ever. So the energy sector is really increasing its focus on information security as well.

Who's most in demand at the moment?

At the senior levels it is the chief information security officer. A lot of companies have developed what we call business information security officers. In essence it's akin to being the right-hand person to the CISO and aligned to each of the business lines for that company. We see a lot of companies utilizing that person as a liaison relationship manager as a means by which to get security embedded into organizations through various business lines in kind of a partnership approach. For example, we are currently working for a financial services company, conducting a search for their chief information risk officer and, at the same time, we are currently placing candidates as business information risk officers in each of their divisions. We also are seeing a lot of companies that are looking for very strong architects – not architects from the general IT area – but carrying a specialty network security or applications security. So these are people who have both deep technical expertise and are actually able to design the framework and define the technical requirements to effectively drive a solution across the enterprise. These are some of the top positions that we are most frequently asked to find.

Have there been many newly-created positions as a result of this activity, and if so, what are they?

Recently, for a large Fortune 100 healthcare organization, we conducted a search for a chief data officer. They work cross-functionally throughout an organization to re-evaluate the data as an asset, versus a side effect of the business like finding a timeline to store data, how to classify the data, how to share it, how to store it and how to leverage it. And, as you can imagine, they will work closely with the CISO, with the chief privacy officer as well as with the digital marketing team, enabling them to securely leverage the information. With a new value placed on data analytics, companies are hiring data scientists as part of the overall information security strategy around big data. Due to very stringent regulatory requirements, some of our clients are now separating the role of the chief information security officer and the head of IT risk. Many companies are now hiring an enterprise technology risk officer who manages the strategies, programs, governance and the oversight of everything to do with IT risk. So, again, they would partner with the information security officer. But I think it is important to note that it is not as much the newly created position that is important but, rather, the elevation of the roles in IT security and risk. These are positions that were once VP or director are now being graded as a senior vice president and those that were senior vice president are now being extended the opportunity to move into a C-level position. The majority of the head of the security and risk roles that we are placing all have the responsibility to present to the board of directors and to their risk and audit committees and they actually lead task forces or committees themselves.

"A driving force is the increased volume and complexity of cyber threats."

- Joyce Brocaglia, CEO, Alta Associates

Where are we all heading?

Our theme for the Executive Women's Forum National Conference is 'Big Data, Big Risks, Big Opportunities.' I think that really highlights the future of security as well. There is currently what I would describe as negative unemployment in our field, which reflects the current demand for cybersecurity professionals. The estimates are about 1.4 million information security jobs will be in existence by 2020, and there are statistics that show the demand for information security is growing 12 times faster than the overall market demand. This year alone there was a 46 percent increase in the number of breaches and 43 percent of companies were hit by an attack. And 60 percent of those companies were hit twice or more. There is a saying that there are two types of companies: Those that have been attacked and those that don't yet know they've been attacked. I don't see that as changing but only increasing. As I mentioned earlier, with the Internet and the connectivity of the world today, the complexity of the role of the information security officers and their teams is only going to continue to expand and grow.

SPOTLIGHT

Risk Management Starts with Pinpointing Vulnerabilities

Benchmark Executive Search, based in Reston, VA, is making its mark as a sought-after recruiter for both federal market and commercial companies in search of cyber talent. Jeremy King, the firm's founder, has worked extensively with VC/PE backed firms that serve the government, building strong ties with leaders in intelligence, defense, and national security. Benchmark's focus has been on helping start-ups, emerging growth and mid-cap companies find top executives with government backgrounds and strong connections in the defense and national security markets in areas like information technology, military communications, homeland security, and cyberwarfare, among others. Terrorism and cyberattacks are ratcheting up the call for hiring in these areas, he said, and the sector is thriving.

Benchmark is now directing its energy to Fortune 1000 companies, many finally awakening to how destructive security breaches of all types can be – from physical damage and real costs to reputation loss and customer recovery. Mr. King is now calling for industry to re-evaluate its approach to risk management. "Previously siloed risk-management functions must be reinvented, strengthened, and funded more aggressively," he says. "Success will require unprecedented cooperation from board directors and those in the C-suite."

Hardening People as Well as Networks

Mr. King advocates a stronger "culture of security," strong executive leadership, and greater resources to manage network vulnerabilities with urgency and continual innovation. Top companies, in particular, must be vastly more vigilant about comprehensive risk management. "Fortune 1000 corporations face a clear imperative: decisively improve internal risk management assets, leadership and performance – or risk suffering at your company's or shareholders' peril," says Mr. King.

In many respects, risk management starts at the top of these companies, and the key will be vigorous attention and collaboration between boards of directors and the C-suite. Of particular concern in keeping companies safe is the human element. "With an estimated $94 billion dollars to be spent on cybersecurity in the next decade, it is surprising most corporate investment in security today is directed to hardening networks rather than people," Mr. King says. "Most organizations have not taken the time to map the vulnerability points of their employees or done a comprehensive risk management assessment."

Predictions for 2016

Based on what he and his colleagues have gleaned from clients, advisors, and their network of security talent, Mr. King makes four predictions for 2016:

- Public companies will increasingly empower a single leader or group to take charge of their integrated risk and security strategies;
- Chief risk officers (CROs) will see a greater role at public companies and be regarded as peers to the COO. "With the COO having P & L, profit and loss, responsibility, the next generation CRO will have a new kind of P & L – prevention of loss," says Mr. King;
- Boards will increasingly follow the federal Sarbanes-Oxley Act compliance mandates, which among other things led to most public companies establishing a chair of the audit committee. "Soon we will see more public, and some private, companies implement a chair of the risk or cyber committee, or both, on their boards," Mr. King predicts;
- Public companies will undertake more extensive risk assessments to pinpoint where they are most vulnerable to attack. This would include facilities, communications, networks, and employees. "This new level of threat intelligence is partly due to increasing global corporate espionage and intellectual property theft," he says.

Q&A

A Shifting Problem

Jeremy King has nearly two decades of cybersecurity knowledge and access to a vast network of the nation's top cybersecurity experts. Here, he describes the corporate risk and security leadership needs of companies now in the crosshairs of a talent dilemma.

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

It is no small task for any organization to achieve consensus about what must be done, what organizational assets must be integrated into their broader risk-management mission and even a standard organizational structure to determine how the CRO, CIO, CSO and CISO fit together. Not to mention the cost of the mission, measured in both dollars and management focus.

Is everyone approaching the talent problem the same way?

For Fortune 1000 corporations convinced that they need enhanced security, it is not easy to find the right leaders to design and manage an effective program. And at the other end of the spectrum, most small organizations are not addressing the complexity of the challenge – nor can they justify the costs.

Is the problem priority or focus?

Both. Corporate security is today's biggest talent management challenge and it needs to be given the highest priority and focus. Our experience tells us that the core skills and expertise gained from public sector leaders can be leveraged to inform private sector actions and strategies. In the end, only people can create strategy, policy, processes and implement the right technologies. The risk to preserving enterprise value is too high not to have an A-team to navigate the new landscape of threats.