Caldwell

STATE OF THE CYBER TALENT MARKET

A Caldwell Whitepaper

CONTENTS

STATE OF THE CYBER TALENT MARKET

By Matt Comyns

ABOUT THE AUTHOR

Matt Comyns is managing partner of the firm's Cyber Security Practice. His focus is on recruiting chief information security officers and next-level-down top lieutenants in information security for large global corporations and fast-growing private companies, as well as cyber security consultants for leading professional services firms and top executives for cyber security technology companies.

Matt has been on the ground since hacking and cybercrime started showing up on the radar of major corporations, and has successfully recruited more than 100 high-ranking executives in this burgeoning space.

Matt Comyns
+1 203 348 9593
Stamford
mcomyns@caldwellpartners.com

THE STATE OF THE CYBER TALENT MARKET

It has been a little over three years since the Target breach—the watershed moment when cyber security changed overnight from an issue that lived in the murky realm of *I suppose it's a concern, but there are more pressing matters,* to an issue at the top of the priority list for companies and industries across the board.

I feel fortunate to have had a front row seat as the aftermath of that event has unfolded. I worked on my first CISO search approximately six years ago, and have since worked on more than 100 cyber security-related executive searches and talked with hundreds of other companies about their cyber programs and human capital challenges.

Cyber programs certainly existed "pre-Target," however, the dialogue and environment changed dramatically after the Target breach and the infamous Sony incident a year later.

Outside of government, defense contractors, financial services, technology, and telecom, there was not a lot of investment in cyber. As other industries (energy, consumer, manufacturing, retail, health care, etc.) began to "get religion" on the topic, we started to see the kind of supply and demand disconnect that can best be likened to Dutch Tulip Bulb mania or 1999 Dotcom Bubble hype.

In 2016, even the most dutiful of cyber executives lost their way in the face of multiple and increasingly lucrative job opportunities. It was a psychology study in bad human behavior—particularly troubling since these are the people we are relying on to protect us!

In these cyber execs' defense, they saw life-changing offers and no end in sight on the demand side. It is easy for them to justify their decisions, because there will seemingly always be another company out there willing to overlook any perceived bad judement. They're sort of right. The US and the rest of the world are nowhere near maturity in the development of their cyber programs, and it will be quite a few years before the market normalizes.

So now what?

I am sympathetic to companies that are committed to hiring top talent and building leading cyber security programs in this overly inflated market—I have watched many executives and talent teams do EVERYTHING right and still get disappointed.

CYBER PROGRAMS CERTAINLY EXISTED "PRE-TARGET," HOWEVER, THE DIALOGUE AND ENVIRONMENT CHANGED DRAMATICALLY AFTER THE TARGET BREACH AND THE INFAMOUS SONY INCIDENT A YEAR LATER.

Here are some things to keep in mind when running these competitive search processes:

PRESENCE

Besides supply and demand, the biggest complaint is "these people are too techie" and lack the executive presence and communication skills needed to present to the board and C-suite. Remember—before Target, most cyber functional experts were lower in the IT org chart and had limited responsibilities. Just because cyber risk went from 0 to 60 in two seconds flat does not mean the human capital pool kept pace with that change.

The job requirements of the new next-generation CISO or head of information security have expanded tremendously to deal with more complex challenges, including helping CEOs and boards put cyber risk into the proper business context. There are some qualified cyber experts who meet these new criteria, but they can name their price in this market. Comp packages at the high end of the market now run north of $2 million all-in, so bring out your checkbooks if you want it all. The other option is to go with a top athlete who can grow into the role in time or repurpose another high-level IT executive and train and support them to become new age cyber execs.

COMPENSATION

Compensation is all over the map. As I mentioned, the high end now trades north of $2 million all-in, and the low end is closer to $250k. That's a big gap. As with other things in life, you get what you pay for.

I see many highly qualified cyber executives in the $500k to $700k all-in comp range, but you will have to motivate them to move. The typical bump in pay of 15% to 20% won't necessarily do the trick anymore, no matter how great your company and opportunity. This is especially true when you factor in the kind of unusual counteroffers we're seeing.

What is talent worth to a company? They often don't know until it is walking out the door. I will give you my most painful example of 2016...a terrific cyber executive at a bank was making $900k all-in. My client pulled out all the stops and put together an offer of $1.55 million all-in. The candidate's existing company countered with an offer to beat $1.55 million ***and*** created a new hybrid role that incorporated fraud, cyber, physical, etc., and consolidated 3,000+ people under him—approximately four times as many people as he had previously managed! Until the supply side is fixed, we are all in for a compensation headache to get top talent in this area.

Another recent example is a conversation I had with a talent officer at a reputable company who said to me, *"Look, I get it. We are in a bubble market. Well, at my company we don't play that game,"* to which I politely replied, *"I understand, but I have news for you...you're in the 'game' whether you like it or not. I wish that weren't the case, but it's today's reality."* The happy ending on this story is that the company hired a top-notch step-up candidate at a reasonable price. You can get what you want, but you need to be creative.

DIY OR CYA?

Competition in hot markets is inevitable, and that was certainly the case in cyber security recruiting over the past year. It seemed like anyone who could spell cyber security was purporting to be an expert recruiter, only to run full steam into conditions that made it tricky for even the most experienced cyber recruiters. Caveat emptor.

The thing that caught me by surprise, though, was how many Fortune 500-type companies were tackling CISO searches themselves. The DIY trend is part of the broader trend in executive searches, with in-house teams—emboldened by tools like LinkedIn and Google—feeling confident enough to hire on their own and save on search fees. If you believe half of what I've told you thus far, you likely concluded that going it alone is a high-risk proposition.

It's not just about identifying the right names, although good specialist cyber recruiters will definitely augment your list of potential candidates. It's also about having a dedicated outside partner reaching out to the market on your behalf and using every available edge to land these highly sought-after executives. Having a trusted relationship with the top candidates, being aware of the competitive searches in the market, and running a tight process are all keys to success.

With boards and C-level execs elevating cyber risk to one of the top enterprise risks they are dealing with today, why wouldn't you take proper precautions and partner with a specialist recruiter on these searches?

I will leave you with a catchy phrase that will serve you well: when dealing with cyber, think CY(b)A.

With boards and C-level execs elevating cyber risk to one of the top enterprise risks they are dealing with today, why wouldn't you take proper precautions and partner with a specialist recruiter on these searches?

WHAT DOES GOOD LOOK LIKE?

The most common profiles include backgrounds in IT, professional services, military/intelligence agencies and developers, but with the proper training and support, stellar CISOs can grow from virtually any plot. That said, the candidates must all have solid business acumen, executive presence, great communication skills, strong influencing skills, nimbleness and, increasingly, the ability to manage large internal and external teams. The CISO must also be able to engage with the outside world of regulators, the media, and industry trade associations.

OUT-OF-THE-BOX CANDIDATES?

If you are willing to re-purpose trusted executives at your company, look at your CTO, head of infrastructure, head of application development and the like. Legal and audit are also places you might look. 12-24 months of training/education can go a long way with these leaders. Look to top universities like Columbia University *(Disclosure: I am an advisor to Columbia's masters in technology management with a concentration in cyber security)* or the Sans Institute, which will customize a cyber program for your leader(s).

Another way to bring a greener executive along quickly is to build a cyber advisory board (see below) that can partner with the executive to design a strategy, build a road map, and create a metrics dashboard for the board and CEO to measure the progress of your cyber program.

THERE IS NO SILVER BULLET

This is often the toughest part for companies to stomach—even if you pitch a perfect game and land that top talent, they might only be with you two to three years in this market. Having a Plan B is of critical importance, so start your succession planning now. Within six months, a new CISO should be identifying his/her top successor candidate and creating a development path to get there. That includes socializing that person with C-level execs and the board. The other important thing to know is that vendors/partners (Big 4, Accenture, IBM, Cisco, cyber boutiques like SecureWorks or Optiv, etc.) are critically important—outside expertise will keep you current and help you scale.

CREATIVE SOLUTIONS

Given the state of the industry and the market, I strongly believe that companies would greatly benefit from adding specialist advisory boards of outside cyber experts—a cyber advisory board.

Some companies have taken the plunge and added a full-time cyber expert to the board; however, most are gun shy about adding a director who may be too narrow in scope and unable to speak on broader business issues. An advisory board option is more flexible—these people can help you continue down the cyber maturity path and offer valuable external market perspectives.

For example, imagine having five cyber experts who might be current or recently retired proven blue chip CISOs, threat intelligence gurus, chief privacy officers, legal and/or regulatory experts, supply chain/third party risk management experts, intellectual property experts, high-volume transaction experts, geographic specialists, etc. You get the picture.

Depending on your business needs, you could design a cyber advisory board to offer maximum value. This new team's responsibilities would include educating the board, C-level executives and functional heads, and could also serve as mentors/advisors to your CISO, especially if you go with an out-of-the-box choice. It may, in fact, be a better solution AND more cost effective. We have prequalified leading experts who are excited to participate in Caldwell's advisory board program—stay tuned for more announcements on that front.

Vendors and consultants are still relevant and valuable, but a cyber advisory board provides a deeper level of expertise and consistency, not to mention saves you a lot of money. Lastly, a cyber advisory board will go a long way toward satisfying the regulators who are putting more and more pressure on companies to demonstrate their commitment to cyber best practices.

THE JOURNEY AHEAD

Cyber risk is here to stay, and it's a journey to maturity. Large enterprises don't change overnight, so if you have not started the journey, start now! If you have made progress, know that it is a multi-year process and that the market is still figuring itself out.

We are likely a decade away from a consistent understanding of how companies deal with this new enterprise risk. And remember, you can't have enough friends in this space—sharing, partnering is good. That includes a human capital partner who can help you make sense of what type of leadership is needed and where those leaders are.

HOW CALDWELL CAN HELP

Engaging Caldwell is the key to finding best-in-class talent across industries and gaining market intelligence.

Our partners fully understand the nuances of this fast-evolving marketplace, and the issues companies face in attracting and retaining these in-demand leaders.

Our service offerings span from chief information security officers searches and interim solutions to assessment, development, benchmarking, briefings, advisory boards and beyond.

OUR SERVICE OFFERINGS

Buy	– CISO Searches
Interim	– Part-time solutions
Access-Develop	– Proprietary and psychometric testing along with training and development solutions
Advise	– Board and C-level briefings
Map-Benchmark	– Real-time compensation surveys and organizational structures
Grow	– Cyber advisory boards

Caldwell

WE BELIEVE TALENT TRANSFORMS™

As a leading provider of executive talent, we enable our clients to thrive and succeed by helping them identify, recruit and retain their best people. Our reputation–nearly 50 years in the making–has been built on transformative searches across functions and geographies at the very highest levels of management and operations. We leverage our skills and networks to also provide agile talent solutions in the form of flexible and on-demand advisory services for companies looking for support in strategy and operations. With offices and partners across North America, Europe, Latin America and Asia Pacific, we take pride in delivering an unmatched level of service and expertise to our clients

caldwellpartners.com