RUTHERFORD

How to Identify the Best

Head of Compliance

November 2020

rutherfordsearch.com

RUTHERFORD

How to Identify the Best

Head of Compliance

There was a time when a Head of Compliance was often referred to disparagingly as a "business prevention officer". Nowadays the reality – and expectations of the role – are very different. Whilst it has never been sufficient to adopt a box-ticking mentality in this function, the evolving role now requires a raft new skill-sets to add to some perennial pre-requisites. So, what exactly are the skills, qualifications and attributes you should be looking for from potential candidates for a Chief Compliance Officer ("CCO") role?

Whilst every firm will have a different risk profile, many consistent attributes still remain crucial for the contemporary CCO. Far from being a heavy-handed enforcer, today's Head of Compliance can actually go far beyond meeting regulatory requirements and help to drive your business. And to do so, they need a portfolio of skills and experiences that range from deep and broad technical knowledge of their subject and the regulatory environment through to excellence in communication, relationship building and technology.

CCOs should obviously have all the usual educational qualifications and personal qualities you would expect from any senior role, plus some attributes that are essential to this position. These include an analytical and well-structured mind, an open and non-political but rational approach, and talent at fostering relationships with internal and external stakeholders, regulators and their peers. We have found that the most successful CCOs by tenure share similar qualities in testing; high "emotional quotient", self-awareness and calmness under pressure.

RUTHERFORD

We look for social diversity - not always go for the 'Harvard types'. People who are considered 'outsiders' are often instinctively sceptical and their exclusion means they don't have that sense of entitlement. They can see through the conceits and have a neutral mindset.

Buy-side COO

How commercially aware are they?

A high-calibre CCO should make a significant contribution to your long-term commercial success by promoting ethical standards and proposing both compliance and commercial solutions. Your new compliance officer may well be taking on an explicitly investor-facing role but even if they are not, increasingly the credibility of this function is at the forefront of many client and external stakeholder's selection processes. It is therefore crucial to identify the CCO's appetite for risk, and to check whether it is in line with your own business strategies.

Check too that the CCO has experience in or knowledge of the relevant products and asset classes, as well as the full breadth of jurisdictions in which you operate. Make sure that candidates are fully aware, not just of your day-to-day activities, but of the overall direction of your organisation.

Look for a combination of strong influencing skills and the ability to get the business on-side when they need to with an entrepreneurial attitude towards solutions.

Crucially for smaller firms and something that has led to a number of CCO departures is a compliance officer who can balance the strategic and commercial business advice work with an appetite for the day-to-day compliance work. Many leadership compliance roles necessarily sacrifice time spent on core compliance activities like filings and monitoring. It is vital that you are transparent about what the balance between the business advisory and strategic work is versus the more process-orientated needs of your firm. Find out the candidate's 'operational ceiling', i.e. where they see the balance between tactical work and the more everyday tasks. For smaller firms, some understanding on how much access to external resources a potential CCO would expect or need may also be helpful.

For some, it may be important that your organisation is embracing Environmental, Social and Governance (ESG) investing. Either way, a CCO who is uncomfortable with your approach to regulation, ethics and culture overall could quickly move on. Scenario-based questions can help identify possible issues here.

Agile Partners

Meeting regulatory requirements is only part of the job. In fact, an Accenture 2019 Compliance Risk Study called for a new generation of compliance officers to become agile partners. It found the primary driver of transformation in compliance to be business growth, in areas such as open banking and blockchain transactions, plus inorganic growth from mergers and acquisitions.

These were viewed as five times more important as managing external regulatory change.

In other words, your new CCO should be helping to drive your business, not just to protect it. So find out what they are capable of in terms of adding value.

RUTHERFORD

We avoid the 'city types' with the bluster they acquire. We need to always remember that at the end of the day, this isn't our money. In fact, it belongs to public employees, firemen, police officers. Not us.

Buy-side COO

Management Partners

The bigger your business, the more stakeholders your CCO will have to deal with. This means that their ability to forge strong relationships at many different levels becomes even more important.

If you have a large compliance team then effective delegation will be essential, along with the ability to manage a wide variety of people. A CCO should demonstrate a proven people management capability with evidence of building, retaining and developing high performing teams. You may wish to drill down on previous team size here but we have found management philosophy to be more revealing. Functions will likely be more siloed, which can make them less dynamic. It's essential that your prospective CCO can help them to communicate with each other seamlessly. Experience of navigating group politics may be an advantage in larger corporates, as discussed in one of our *Leadership Series* article.

SMF16/CF10

The requirement for a CCO to have held previously the old CF10 or SMF16 function will depend on the risk profile of each firm. Whatever they identified themselves as previously or do currently, for this position, it is absolutely essential that they are the right person to be called SMF16 – your designated compliance officer. This has been a requirement for all regulated firms since December 2019.

Some smaller firms may be able to get away with a "ghost compliance officer" , i.e. someone who is essentially "double-hatting" or part time in the role. As this earlier blog article shows, the consequences need to be considered carefully. Either way, these traits will remain essential.

The most successful CCOs by tenure also correlate strongly to those that take on the Control Function or Senior Management Function within six months. The experienced compliance officer will be unwilling to take on SMF16 in a permanent capacity without working at your firm for a period of time to gauge the culture and controls in place themselves. Mismanagement of expectations around when the SMF16 will pass to the CCO has been the catalyst of many an exit and a balance needs to be struck between allowing the compliance officer to establish the lay of the land and building enough credibility with senior management to trust the compliance officer to take it on.

Credible CCOs will also expect the risk-profile of the role to be matched by a commensurate level of control and ability to affect change. They may not need to be on the Board, Ex-Co, Risk-Co, report to the CEO or have a "seat at the table", but if they are not looking closely at senior management's willingness to support potential action as well as querying resources available to them to implement change, then that is a flag. This is taking on the personal risk liability without understanding what they are accepting.

Where holding the SMF16 function is a requirement for the role, you should make this explicit to prospective candidates so that if for whatever reason they are not accepted by the regulator, then it is understood that makes their continued employment untenable.

RUTHERFORD

I want my Chief Compliance Officer to just know what the right thing to do is, and to have a strong sense of their 'true north' - the compass analogy being that what may only seem like a few degrees today will become a huge deviation over a period of time.

I want them to just know that complimentary £10K Wimbledon tennis tickets are a no go!

Buy-side COO

Some questions to ask and characteristics to look for

Does their personality and approach match the role? They should come across as principled, diligent and fair. Qualities such as these are important, not just in themselves, but in providing an example to those they work with and setting culture.

How proactive are they? An ideal candidate should always be looking to be on top of new regulations and to develop the best ways of meeting changing requirements. Today's compliance regime has evolved greatly from what it was even five years ago. Fast-forward another five years and the chances are it will again be far removed from what is expected today.

How strong is their international outlook and worldwide regulatory knowledge? Both are important and, depending on the nature of your operations and your global presence, they may be of critical importance to your organisation, particularly in the context of Brexit.

Is there "executive credibility" or gravitas? Are they capable of effectively communicating with both partners (at a strategic level) and staff (at an operational level)? For larger organisations, can they represent compliance effectively on relevant committees or other internal bodies?

Can they produce internal policy documents for identifying and following current and future requirements? Can they draft and interpret legislation? Will legal skills be required? Can they talk to the business, technologists, coders, traders or PMs?

Can they cultivate good working relationships with the regulators? How would they handle investigations if breaches occur or are suspected?

Will they be able to develop good relationships with their peers in similar firms to ensure your organisation is at the forefront of best practice?

If you are not convinced by the answers to questions like these, chances are that the regulators won't be either.

Taking the lead with technology

An ability to harness the potential of technology in compliance has never been more important since the Covid-19 pandemic, which accelerated the trends we spoke about in our August 2020 article RegTech – The Future of Compliance. The modern CCO must be adaptable and embrace issues around ensuring a compliance culture remotely. As well as automating mundane compliance tasks, technology can do more and more in the compliance sphere – and the authorities are requiring not just more automated data capture, but their proper analysis.

Since the first lockdown firms have been ingesting new risks that were inconceivable a few months before. Whether 2021 is a 'new normal' or nearly BAU, what seems likely is that the efficiency benefits in terms of physical footprints, as well as the employee benefits of working at home, will play out in increased appetite for remote-working. A CCO will need energy and creativity to navigate the question of how to surveil in an environment of dislocated and disassociated teams. Questions like, how to imbue the right culture if you are onboarding people that you have never met? What culture might an experienced trader import? How do you teach an inexperienced trader the 'reflexes' of your organization when they are not around their supervisors who can see their body language and how they behave? How are we confident that our controls and supervision continue to operate effectively? The industry may feel that nothing has gone massively wrong, but is that because nothing has gone wrong or because we are not seeing it? Who will get hit?

A CCO candidate must also be able to demonstrate some knowledge of RegTech. The extent of this will depend on the organization. A bank might prize technology change implementation experience where a private equity firm or a boutique investment bank may not.

Many firms still use multiple compliance software solutions. These often don't talk to each other well, if at all, and can generate overlaps as well as gaps. As with people, so with technology – your would-be CCO should ideally be comfortable with handling multiple systems and being the link between them. Better still, are they in a position to be able to take a lead on securing the right technology, and in maybe consolidating your RegTech into a single platform?

By being capable of harnessing technology correctly, they can also lessen the pressure on your in-house teams – helping to increase effectiveness, save costs and reduce staff turnover.

Diversity

Anyone who meets all or most of the above criteria should of course be considered for the position. But as we highlighted in a September 2020 blog article, just 15% of those who held a CF10 or SMF16 job title this year were women. All else being equal, you should therefore pay real attention to the diversity of those on your shortlist. Apart from anything else, failing to embrace inclusiveness could have a negative effect on a firm's diversity of thought and competitiveness.

Making an offer

There is a lot to consider when hiring the right CCO, but we are here to help you hire the best talent – and that includes sending you the best candidates only. Our recruitment consultants themselves come from compliance, legal and financial backgrounds, so they know what to look for in order to find the right Head of Compliance for you.

About Rutherford

Located in London and New York, our team has been providing specialist legal and compliance executive recruitment to the financial services sector for over a decade. Our purpose has always been the same: to bring the best available talent to our valued clients, through deeper market knowledge and the cultivation of trusted long-term relationships.

We pride ourselves on understanding our clients' needs and finding that crucial cultural fit.

Contact us

RUTHERFORD

How to Hire the Best

General Counsel

February 2021

rutherfordsearch.com

How to Hire the Best

General Counsel

From a senior management perspective, the position of General Counsel is vital to ensure that your firm gets the best legal advice to support the business in meeting its strategic objectives. The role has evolved however, from strictly lawyering through advising and drafting; the modern GC will now lead and manage your legal department and be corporate officer to the executive management team, facilitator of corporate governance, they will act as a representative of your firm when dealing with third parties including outside counsel and they will be a key negotiator for strategic transactions.

For larger corporations, the GC may play more of a manager or advisor role, whereas GCs in smaller organizations may be required to not only lead, but also do the legal work. In either case, the General Counsel's possible contribution to your business has never been broader or significant and that potential for them to add value has only increased as a result of the pandemic. Your GC represents your organisation and as such they must take ownership of a wide array of liabilities, discrete business operations, and all past, present and future projects a corporation undertakes. As a business critical hire it is essential that considerable thought is applied to securing the best Head of Legal available to your organisation.

How

Any senior legal interviewer will actually have had many years of experience in selling. Making a case for various views; persuasion and debate are inherent skills to them. On familiar territory (like their career history) they are unlikely to be flummoxed by conventional interview formats or questions – they tend to interview well.

This will present a challenge in differentiating between top candidates. It is vital that your interviewers are prepared and experienced enough to challenge answers and drill down into the detail of key areas like product or specialist technical knowledge through to job transitions. At this point interviewers need to be pushing back on the first and second answers, looking to develop a deeper picture of what the candidate has really been doing. Expect easy rebuttals to hard questions so it will be necessary to pick away at times, even at the risk of seeming the pedant.

The added advantage of this will be identifying another key job requirement, handling pressure. Lawyers are often the best interviewers of Lawyers so for larger firms see if there is someone at the right level in Group or elsewhere and for smaller firms consider asking a trusted Partner from your panel of law firms.

What

Particularly where SMEs are concerned, it is vital that there is a consensus between prospective employee and employer with regard to their responsibility jurisdiction. Where there is a separate Compliance or Operational Risk resource, ensure a clear understanding of where the sole counsel's purview begins and ends. The sheer scope and variety of work the SME Lawyer might be expected to undertake has infinitely expanded during the pandemic and this means that it is important for both parties to understand the likely shape of the workload accurately. From time-to-time one would expect the senior legal professional to turn their hand to new and perhaps unforeseen areas where their legal experience would be an advantage (such as an office lease negotiation) but it is also sensible to outline access to external resources where necessary. Your new General Counsel will be looking to insource a number of responsibilities currently with private practice to save the firm legal fees. Both SMEs and larger corporates should be explicit with candidates about their external cost-saving goals and even look for them to outline suggested ways this could be achieved.

We have talked elsewhere about the qualities required in a Chief Compliance Officer but it is worth reinforcing that, particularly where the General Counsel will sit above the Chief Compliance Officer, the delineation of roles needs to be very clearly understood. Similarly, where it is desirable that your new Lawyer will hold the SMF16 we suggest you refer to this link and satisfy yourself that these criteria are met. Whilst "double-hatting" legal and compliance roles is common, many a clash has arisen over the old CF10 now SMF16 and where the function should sit. Some Lawyers are entirely happy SMF16s and regulatory experts (particularly in US firms), but it can cause consternation in the most senior pre-existing Compliance Officer if there is a reluctance to relinquish it, matched by inadequate regulatory understanding. Note the dual-function incumbent will also usually expect a higher compensation to reflect the increased personal risk-liability, albeit this could be offset by the Compliance saving. At the SME, all skills being equal, ask yourself if your General Counsel will have the capacity to pick up the compliance and reporting requirements. At the larger firm this will turn on the adequacy of your existing Compliance Department. A thematic discussion around issues like information security, Covid-19, Brexit or ESG will also highlight where candidates are and are not comfortable.

Where

The practice lawyer will have to demonstrate a different set of soft skills in an in-house role. In reality a lawyer or even Partner may not see the diversity of backgrounds and the slightly more nuanced stakeholder management that exist in-house. On a day-to-day level they will be exposed to parts of the business that they were not previously, meaning they will have to adapt stylistically and demonstrate a range of communications skills. What worked best for a blue-chip PLC client at practice might not work with the CTO, CFO, or the Board at a challenger bank. Can they deliver the message to your business? If they have not worked in-house previously you must be certain that they can adapt to a more pragmatic and dynamic environment. Can they determine an acceptable level of commercial risk? Can they be proactive, not reactive? Can they give a straight answer succinctly?

Assuming there is alignment on commercial risk, where our counsel will be supported by a competent compliance member, they will be able to offer a valuable resource to draw on supporting the compliance function or offer a separate check and balance. These days a strong grasp of the regulatory landscape is vital for all senior financial services lawyers but in many organisations it is compliance that is sitting out with the business, spending time with them, and getting to know their issues. Legal tends not to sit on the desk with the business in the way that compliance usually does. Where there is no full-time compliance resource it is essential that Legal fills that gap and can provide real-time decisive advice. Look for pragmatic, balanced, and direct responses to scenario questioning to see how they are measuring risks.

The practice lawyer in particular may also have misconceptions about your firm's culture that need elucidation. For some, the move will at least in some part be driven by a hope for better work-life balance. Whilst this is often achievable it is important to reinforce that some companies will have working days significantly longer than 9am-6pm, particularly where trading hours or US calls need to be fielded. Be transparent about your requirements in both the short and long-term to avoid the need to re-hire your lawyer in six months.

Some firms will consider Partner hires in their top in-house legal role but they can present challenges; without recent secondments they may be in equal parts over-specialised and institutionalised. Only some larger organisations will have the specific level of infrastructure and support to accommodate them. Often, after 8-10 years/PQE that benchmark becomes less useful and instead the focus will be on specific experience - but keep in mind that it retains an optical relevance for lawyers themselves if you are hiring someone above them. For smaller firms it is vital to understand a candidate's "operational ceiling" and competency-based questions are vital to determine if a prospective employee will be willing to be hands-on enough; look for signals of how involved they have been in the detail of deals or cases.

Do not assume senior private practice lawyers have extensive management experience. Ad-hoc case-by-case management is sometimes closer to project management and not quite the same as line management - it may be worth digging into this further. General Counsels must be legal leaders, motivators, coaches and developers of legal talent within their corporation. Of course, there will be a lot of transferable skills and in both private practice and in-house candidates look to understand the type and level of lawyers they have managed as well as their approach to developing a team. Does this fit with your culture?

Although in-house lawyers do not usually have to worry about chargeable hours, they still work against demanding deadlines. They are often pulled in a number of different directions and responsible for a wide range of issues so it follows that they must be highly organised and able to prioritise in a different way to in-house. Adaptability will be key.

The private practice lawyer will also need to adapt to an environment where they serve and facilitate the business – they are not the business anymore; they are a cost centre. That need to adapt will have to extend to departmental resourcing, expenses and staffing constraints. Can they think of themselves as an employee of your firm first and a lawyer second?

Who

Underlining all of the above is a fundamentally high emotional quotient and a lawyer's ability to empathise, communicate and build relationships with all areas of the business. Look for the executive credibility to sit on the leadership team and advise the Board, to pull along the business with important decisions and reassure investors. Sole General Counsel may also be unfamiliar with being the only lawyer in an organisation and competency-based interview questions will also reveal resilience and an ability to work effectively autonomously. Look for an extensive external network of peer lawyers that will provide the candidate with moral and professional support and benefit the business by ensuring your General Counsel sees the bigger picture. A lawyer’s professional network will become increasingly vital in providing both the mental health benefit of informal support but also ensure they are at the forefront of trends in the market. The sheer breadth of an in-house legal role will often exceed a lawyer’s direct expertise so resourcefulness and creativity are also vital. Look for signs of an intellectual energy in the candidate to dive into new and unfamiliar legal areas.

Often legal expertise is a given in the eyes of the hirer, but there must also be a focus on what else a lawyer can bring to the table. That energy should extend to advocacy of technology and the solutions it can – and as crucially, cannot – provide. As goes the world, the pandemic has increased the need to have tech-savvy lawyers with a level of understanding and interest in how technology can improve a department or business. On an individual-professional level they will need to have embraced the tools required to manage geographically dispersed legal staff, like Zoom, Slack and Teams.

The senior lawyer is now also seen as being at the forefront of driving the diversity and inclusion agenda and their responsibility for risk and governance has made them natural stewards of the social responsibility and sustainability themes. At the conclusion of the interview, you should ask yourself if you can see the candidate setting the example here.

> **“We avoid the 'city types' with the bluster they can acquire. We need to always remember that at the end of the day, this isn't our money. In fact, it often belongs to public employees, firemen, police officers. Not us.”**
>
> Buy-Side CCO

It is instructive to talk to a candidate about their day one, week one and month one. It is essential that there is a humility. Early on they must walk around, visit all areas of the company, and embrace the values, culture, ways of doing business. They must establish who are the right people to talk to. They must understand the strategy and mission of the company.

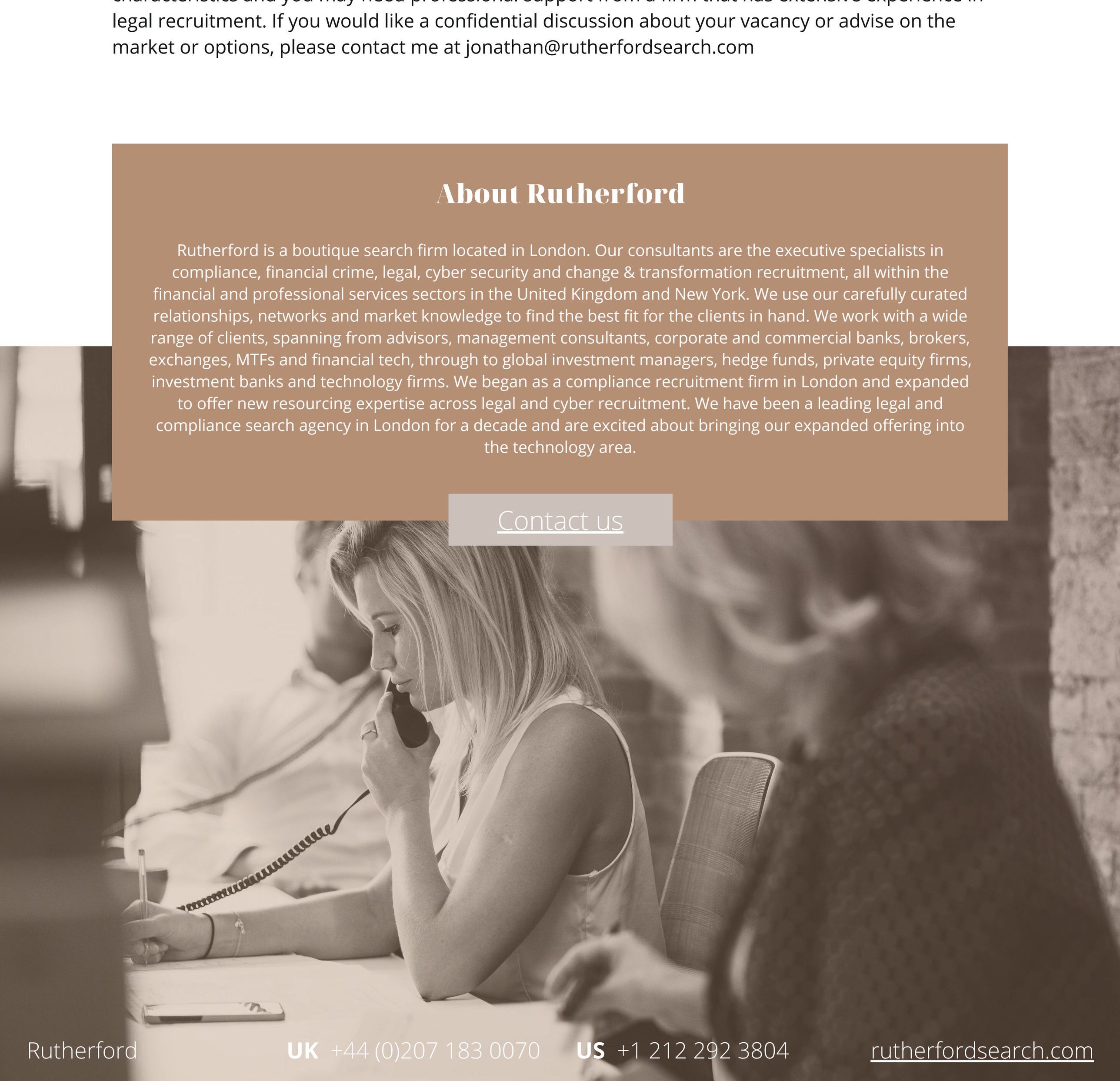
The General Counsel must balance sophisticated evaluation and judgement with decisive course of action and inherent leadership qualities to attract and retain the best legal staff or properly manage external resources. You will need to satisfy yourself that they will be proactive in the guardianship of your business as well at the furtherment of its strategic goals. They will need gravitas and integrity.

It is striking that when we talk about the perfect attributes for your organisation's General Counsel that so few of them are technical, or apparent on a CV. At this level, a cultural fit turns on subtle characteristics and you may need professional support from a firm that has extensive experience in legal recruitment. If you would like a confidential discussion about your vacancy or advise on the market or options, please contact me at jonathan@rutherfordsearch.com

About Rutherford

Rutherford is a boutique search firm located in London. Our consultants are the executive specialists in compliance, financial crime, legal, cyber security and change & transformation recruitment, all within the financial and professional services sectors in the United Kingdom and New York. We use our carefully curated relationships, networks and market knowledge to find the best fit for the clients in hand. We work with a wide range of clients, spanning from advisors, management consultants, corporate and commercial banks, brokers, exchanges, MTFs and financial tech, through to global investment managers, hedge funds, private equity firms, investment banks and technology firms. We began as a compliance recruitment firm in London and expanded to offer new resourcing expertise across legal and cyber recruitment. We have been a leading legal and compliance search agency in London for a decade and are excited about bringing our expanded offering into the technology area.

Contact us



RUTHERFORD

How to Hire the Right

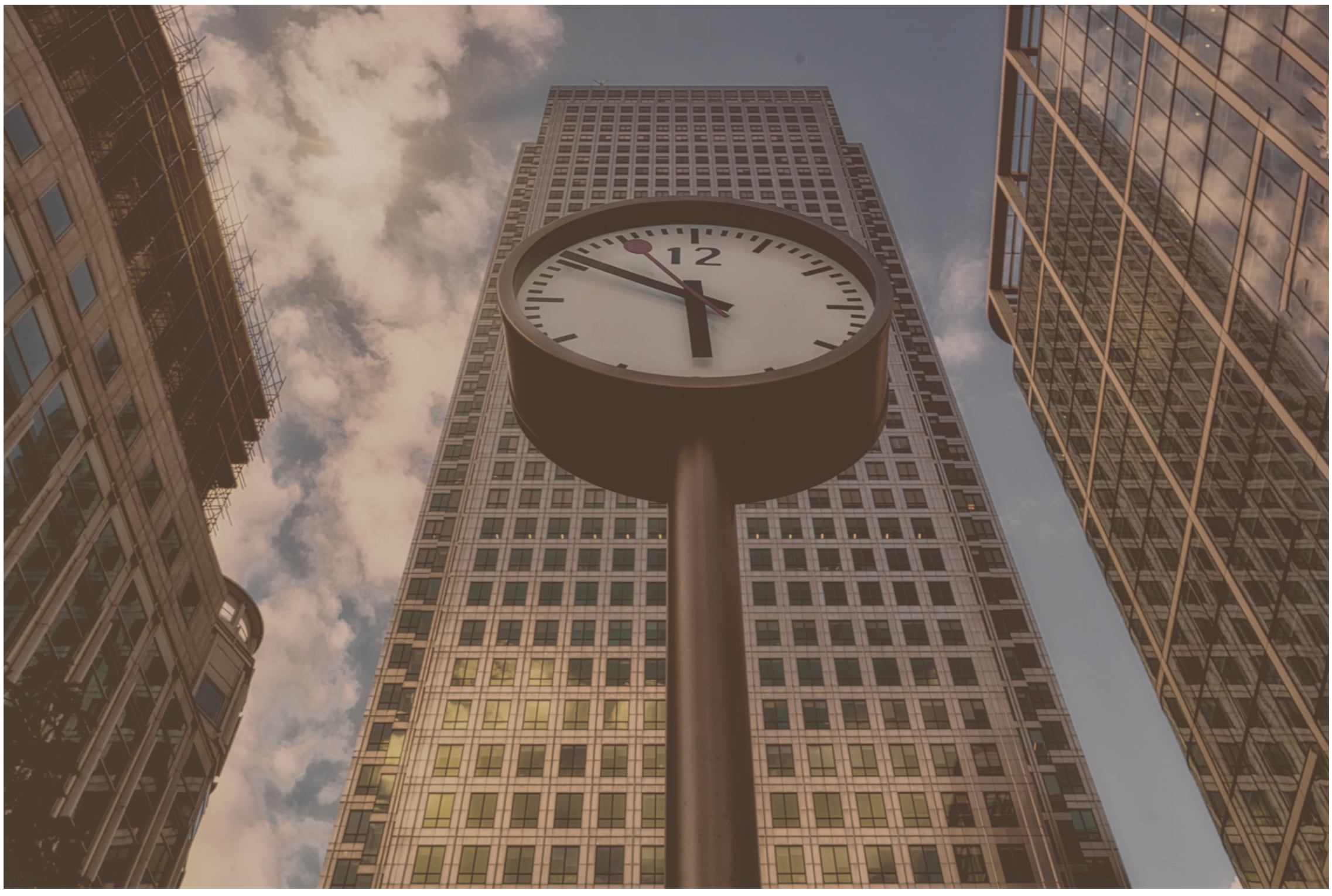
Chief Information Security Officer

for your business

March 2021

rutherfordsearch.com

RUTHERFORD



How to Hire the Right

Chief Information Security Officer

for Your Business

As the professional world grapples with COVID-19, certain sectors have not been quiet. Information Security (InfoSec) and Cyber Security risks have surged over the last decade, and the past 12 months have seen that growth accelerate and evolve. As a result, organisations have to cast an even beadier eye on their InfoSec and Technology Risk policies, and make sure that they have the right people and resourcing in place to try to handle the threat.

Over the course of the second and third national lockdowns in the United Kingdom, the Rutherford Cyber team sat down - virtually - with over 100 Chief Information Security Officers* (CISO) across multiple sectors of the British and Irish economies to discuss the crucial elements to consider when hiring such an important position. The following guide is informed by those conversations, and those held with other C-level peers with oversight of the CISO function - traditionally Chief Operating Officers (COO), Chief Risk Officers (CRO), Chief Information Officers (CIO) and Chief Technology Officers (CTO). From identifying the right kind of CISO for your business to offering the right compensation, the present guide will cover a few salient points that are easy to dismiss.

**NB: If your business has a flat management structure, or doesn't stick to traditional titles, there are a couple of other titles that equate to CISO - Head of Information Security or Head of Infrastructure being the most common.*

RUTHERFORD

Identifying the business requirement for a CISO

Does your organisation need a CISO? Arguably not if your business is down the “S” end of the scale of enterprises (under 20-30 pax if you need an arbitrary figure). That also depends on whether or not your business uses, generates or even just handles a lot of data. It is not a legal requirement to have a CISO – but there are serious ramifications to businesses that do not have one, or at least a nominated individual who is in charge of the Information Security aspects of the business, especially if their internal practices are not up to scratch.

A lot of smaller firms will wrap the CISO role into a business operational risk or a technology position. Again, depending on the demands of the business – probably not an issue for smaller, independent retailers and hospitality firms – be wary though, of equating InfoSec with cyber, and cyber with technology. Gone are the days when InfoSec was “an IT” issue. It is now a critical business risk – according to IBM and the Ponemon Institute, the average cost of a data breach in 2020 was US$3.86m globally. That rises slightly to $3.9m in the UK and almost trebles to $8.64m in the USA. That is a substantial write-down against any business. Those costs are normally down to incident response and loss of custom (temporary and permanent). They have grown significantly due to the constant evolution of malicious cyber incidents, as well as the steps that regulators and watch dogs are now taking in the aftermath of breaches.

As costs of breaches to businesses have grown, regulators are building stronger frameworks that businesses must abide by. One of the best known changes has come about from the European Union’s “General Data Protection Regulation'' (GDPR). Whilst the US doesn’t have a single, overarching, GDPR equivalent due to its federalized nature - although the Biden Administration might change this - California is leading the way with the California Consumer Privacy Act (CCPA). In Europe, and the UK for now, the regulator can levy a fine on any business that is breached (due to a lack of adherence to the basic data protection regulations) up to €20m or 4% of global annual turnover – **whichever is greater**.

If you think that your company can risk not having a senior internal stakeholder, empowered to make organisational-wide changes, to protect against technology risk threats (in this instance manifested in the form of data breaches) because it is discrete and flies below the radar, think again. Back in late 2018, Hiscox released data that suggested a small business in the UK is hacked every 19 seconds – since then the threat has only increased and anonymity is no longer a reliable defense.

Hiring a Head of Information Security or CISO does not mean your business will become safe from cyber threats overnight. If anything, in the modern workplace, it is almost impossible to completely eradicate the threat of cyber breaches. However, taking the time to embrace the critical function that a CISO has to play in an organisation, and the fact that no system is foolproof, will go a long way to reducing the overall operational risk to your business.

Strategic Hiring

Does a CISO count as a strategic hire, and what role do they have to play in a Change and Transformation fashion within your organisation? The answer to the first question would appear to be blindingly obvious - but the issue here is whether or not the Executive Committee have genuinely committed to the idea of the function and resourced it accordingly. The second requires the hiring manager to have a strong idea of the outcomes they want to achieve with the hire. Whilst the two ideas work in tandem, it is important to know that even though every hire is part of the Change and Transformation process, not every hire is a strategic one.

What signifies a “strategic hire” then? By its very definition, any hire that is labelled a strategic hire is one that enables the company to achieve a specific goal in a significant way. It doesn’t matter which business function you are hiring into – that maxim applies across the board.

You might be asking yourself – why is a CISO a strategic hire?

In many firms, CISOs are now at a C-suite or C-1 level. As InfoSec has grown in importance, its place in a firm’s business risk and continuity planning has also grown. A CISO is not a Chief Technology Officer in all but name. Rather, it is a wholly separate function that both enables and protects a business. We mentioned GDPR-related risks earlier – and the associated fines that can be levied. These are just one of many different threats to the business – others include fraud, financial crime, industrial espionage, extortion – the list goes on. These threats, and the inherent risks they could bring – let alone the associated damage – to your organisation, highlight the importance of this position.

If you have identified the overriding priority that the CISO needs to focus on or deliver – then you have the strategic reason behind the hire. You will now need to identify the appropriate candidate and incentivise the right talent to apply.

NB: Do not make the admittedly understandable mistake and think that the candidate with the most post-nominals is the best fit for the job. It sounds obvious, but if you are hiring this role for the first time, or with a specific transformation goal in mind, it bears repeating. Qualifications and certifications can be earned in-house or gained by more junior hires.

What Type of CISO Do You Need?

Within information security and wider technology facing roles, it is not just enough to hire a candidate with all the professional qualifications and certifications. After all, most penetration testers - offensive cyber security professionals (Aka Red Teamers or White Hat Hackers) employed by you, or more likely your third party service provider - would point out that many of the best testers, in the UK at least, are not Tiger Scheme or CREST accredited. Instead, you will need to identify whether or not your business requires a certain level of qualification - for audit, regulatory or client-facing reasons - and, more importantly, if the person leading the new function fits with your wider company culture, or is capable of creating a new and more security-conscious culture.

In many organisations, the InfoSec function is seen as some form of internal company police. This mentality often stems from a set up whereby InfoSec becomes siloed from the main business, and used as a final line of defence that is upheld at the end of a business process. By actively, or inadvertently, separating the function from your business as usual operations, it can be extremely difficult to create an internal culture which brings InfoSec practices into the heart of your standard business processes. If you believe your organisation is suffering slightly from that scenario, then the candidate you chose needs to be able to break down internal barriers and lead stakeholder engagement at all levels within your firm. This is addressing a cultural issue, as much as an InfoSec one.

If your firm has a good InfoSec culture already established, the requirement for the CISO may be in one of two other areas. Whilst we mentioned that qualifications aren't always the critical requirement for the role, that will depend on the nature of the function, and/or regulatory and compliance needs. The larger the InfoSec function, the less need there is for the CISO to have all the qualifications required by your industry/the regulatory body that oversees your sector. Good deputies can be trained up to achieve necessary qualifications – if desirable over a longer period of time and not time sensitive. If your firm is missing a critical qualification that is mandated by a regulator or law, then you may not only need a CISO who holds the necessary qualifications, but also additional employees with the relevant ones.

The other side of hiring the right CISO will depend on how much external engagement the function may need to handle. As the nature of our interaction with the internet, data and all other things digital has changed ever since the dawn of the world wide web, so has the cyber threat environment. In recent years, even more so during the COVID-19 pandemic, the threat level online has increased at an almost exponential rate. It is no longer the case that businesses can maintain good corporate security by having devices and portals which physically stay in protected spaces like office buildings and company campuses. The wholesale move to remote working has forced companies to re-evaluate their systems and practices as they now have to look at the threat present outside of the company's real estate. Additionally, regulators are cracking down on firms who have previously taken a light-touch approach to cyber threats, or have failed to resource the function properly. Regular high profile breaches continue to take place and a lot of well-respected names have been on the wrong end of an S166 from the Financial Conduct Authority.

Who Should You Hire?

Underlining all of the above is a fundamentally high emotional quotient and a CISO's ability to empathise, communicate and build relationships with all areas of the business. Look for the executive credibility to report directly to the leadership team and advise the Board, to pull along the business with important decisions and reassure clients and regulators.

The resourcing for the function, including headcount, will impact the kind of CISO you can attract. Some organisations have extensive in-house teams that report to them, whilst much leaner ones will have the majority of headcount being subordinated to the Technology function or outsourced to a trusted third party provider. Regardless, your CISO needs to have a good network within the InfoSec community. An extensive external network of peer CISOs will provide the candidate with moral and professional support and benefit the business by ensuring your hire sees the bigger picture, and can keep the firm on the front foot against new cyber threats. This helps ensure they are at the forefront of trends in the market. As Information Security finds its own space between Technology and Risk, a CISO with the ambition to evolve the function, and take on additional compliance and regulatory mandates will be the most desirable option. This is not a stagnant role that can be filled by a carbon copy candidate: intellectual desire to move the function forward and make it into a business vertical that enables rather than holds back your business will be crucial.

With the move of the InfoSec function away from the Technology vertical, it may be the case that the direct reporting line does not have the subject matter expertise that would come with a CISO – unless the company has a Chief Information Officer. In this instance, the desired candidate must have the ability to drive the InfoSec conversation in a way that all stakeholders can understand. Third party peer review can be essential in helping identify the necessary technical requirements, as well as the strategic experience, to ensure that you do not have capability gaps once a candidate has been identified and brought in. It is important to note though that no CISO can do everything required of the function – particularly if they're in a lean one. A candid conversation with interested parties will identify possible areas that will need additional resourcing.

Hiring managers also need to be willing to consider candidates from outside their immediate space. Firms that fall into the category of Critical National Infrastructure, or have a strong regulatory environment, can be strong contenders. Other good sources are professional services, managed service providers or cyber-focused software vendors. You do not have to hire a CISO with 20 years of financial services experience just because your firm operates in that space. Likewise, a lot of good, ambitious CISO candidates did not go to an Oxbridge institution, and a significant number of the best do not have a higher education certificate at all. The key takeaway here is this: there is no one path that makes a good incumbent for the role.

It is also worthwhile keeping an eye on internal talent and those looking to take a step up at another peer/or larger organisation. This can be for the role of the CISO itself, or as a Deputy CISO. Succession planning is key and doesn't have to be a painful process. The new CISO can mentor internal potential, or help lead the process to bring in additional capability. You do not necessarily need a standalone Deputy position, but that will largely come down to the size and scope of the organisation, as well as the complexity of the security function and technology platforms it has oversight of.

The Right Compensation

Since the idea of the CISO has entered its current format – the last 15 years or so – compensation for the role has gradually begun to improve. Four to five years ago, the average CISO salary in London hovered around the £150,000 a year mark. As the scale of the cyber threat has increased, the function has also matured. When earmarking resources for the role, it should be at a similar level to other C-Suite members or "C-1" level roles in your organisation. Within larger financial services firms, the average has crept up to over £200,000 in 2020/2021.

Strong compensation packages alone will not equate to the right CISO, and there is no hard and fast rule that you must pay close to a quarter of a million sterling a year to find the right candidate, but the average pay is only going in one direction for the position. A point of order – whilst "London weighting" has a not inconsiderable impact on that figure, those kinds of packages are now the norm, not the exception. Some UK-based firms are compensating their InfoSec leaders to the tune of seven figures, in an attempt to rival the traditionally better-heeled competition in the United States, and not lose their best to New York, Charlotte, Boston and California.

Conclusion

There is no one type of CISO to be found on the market. This makes the hiring process that much more challenging. However, clear trends in the sector can be used to streamline the process and reduce the headache! Finding a CISO that matches your firm's requirements doesn't need to be painful. Through the identification of the business requirement for the role - or for replacing an outgoing CISO - you can reduce a time consuming process. This is a Change and Transformation hire - so you need to find the candidate who will do more than just lead the team on a business as usual setting. A good handle on InfoSec Strategy, threat awareness, industry best practice, upgrades to operating systems and cloud migrations - the list continues - will put the team in a position where they can continually evolve.

In the new world of heightened cyber threats, the value of the function lies in having the right team in place to enable the business to grow in a safe and risk-mitigated fashion. It is no longer possible to remove the risk of malicious cyber activity from your firm's risk considerations, but carefully considered hires, and the right kind of resourcing will lead to a safer business operating environment. A CISO does not have to possess all the cyber certifications to be good at their job. They also cannot run the function without adequate junior and senior resources - both internally and externally. Outsourced security service provision can be a game changer when coupled with the right internal team - but it must be backed by strong internal practices.

With a network of CISOs across multiple industry vectors, Rutherford is well positioned to reach out to the leading professionals within the InfoSec space. If you are considering hiring a CISO or InfoSec lead for the first time, or looking to fill a newly vacated role, do get in touch for a discrete consultation.

About Rutherford

Rutherford is a boutique search firm located in London. Our consultants are the executive specialists in compliance, financial crime, legal, cyber security and change & transformation recruitment, all within the financial and professional services sectors in the United Kingdom and New York. We use our carefully curated relationships, networks and market knowledge to find the best fit for the clients in hand. We work with a wide range of clients, spanning from advisors, management consultants, corporate and commercial banks, brokers, exchanges, MTFs and financial tech, through to global investment managers, hedge funds, private equity firms, investment banks and technology firms. We began as a compliance recruitment firm in London and expanded to offer new resourcing expertise across legal and cyber recruitment. We have been a leading legal and compliance search agency in London for a decade and are excited about bringing our expanded offering into the technology area.

Contact us