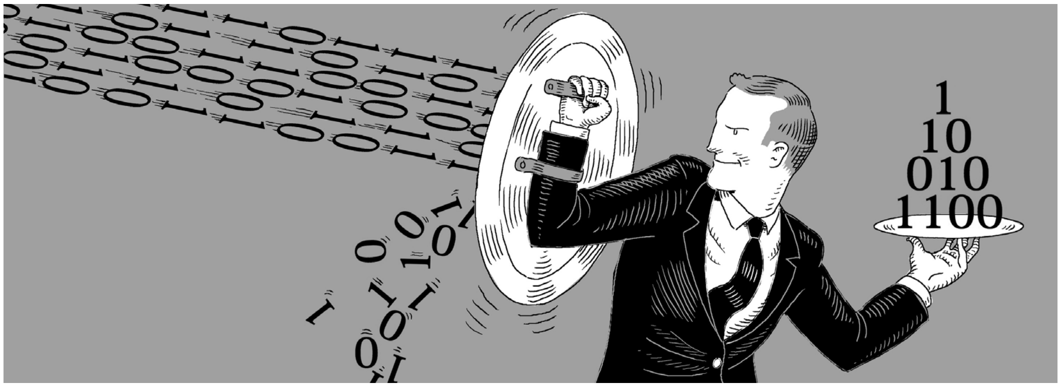
RUSSELL REYNOLDS ASSOCIATES
Leadership, Succession and Search

Global Leadership

New Threats, New Leadership Requirements: **Rethinking the Role and Capabilities of the Chief Information Security Officer**

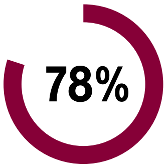


Cybersecurity (or, often, the lack of it) now dominates headlines—and for good reason. The recent spate of large-scale security breaches demonstrates the scale of the threat, the potential for harm, and the vulnerability of many organizations' systems and networks.

Indeed, the breaches occurring in December 2013 alone were jarring. During the peak of the holiday shopping season, hackers invaded Target's systems, stealing information on more than 100 million customers.[1] Only weeks after Target's breach was publicized, luxury retailer Neiman Marcus announced that more than 1 million customers' credit and debit cards had been compromised.[2] And on New Year's Eve, hackers attacked Snapchat, a rising star in social media, exposing the usernames and phone numbers of 4.6 million users.[3]

But a focus exclusively on headline-grabbing breaches holds the potential of distracting leadership teams from the larger trend. The evidence on hacker activity clearly demonstrates that cyberattacks are persistent, pervasive and penetrating. In fact, Cisco's *2014 Annual Security Report* states that *all* the networks of the world's 30 largest multinational companies indicated the existence of malicious traffic. Cisco went on to recommend that "all organizations should assume they've been hacked."[4]

Given the scale of these threats, cybersecurity is now a key item on the agendas of boards and executive teams. And these discussions are not theoretical. As BP Chief Executive Officer (CEO) Bob Dudley recently noted, "We see as many as 50,000 attempts [at cyberattacks] a day."[5]



percentage of initial intrusions rated as "low difficulty"[6]
Source: Verizon

percentage of the world's largest 30 companies with indications of malicious traffic.[4]
Source: Cisco

[1] Harris, Elizabeth A., et al, "A Sneaky Path Into Target Customers' Wallets", *The New York Times*, 17 January 2014.
[2] Harris, Elizabeth A. et al, "Neiman Marcus Breach Affected 1.1m Cards", *The New York Times*, 24 January 2014.
[3] Kosner, Anthony, "4.6 Million Snapchat Usernames and Phone Numbers Captured by API Exploit", *Forbes*, 1 January 2014.
[4] Cisco Systems, *Cisco 2014 Annual Security Report*, 2014.
[5] Tomaso, Michael, "BP Fights Off Up to 50,000 Cyber-Attacks a Day: CEO", CNBC, http://www.cnbc.com/id/100529483.

Global Leadership addresses the key issues companies face in identifying, assessing and retaining successful leaders and leadership teams.

Global Leadership

Previously considered a technical issue confined to the backwaters of information technology, the topic is now central to the strategic and operational discussions of leadership teams.

Commonly, though, these boardroom discussions are rendered deeply uncomfortable by a single, inescapable fact: Most breaches are both predictable and preventable. According to Verizon, 78% of initial intrusions are rated as "low difficulty."[6] And, all too often, it's not until a law enforcement agency notifies an organization that its customer information is available on the black market that a company is aware of having been breached. While hackers are undeniably becoming increasingly sophisticated, research reveals that the majority of successful attacks cannot be attributed to the ingenuity of the attackers. Instead, successful attacks often result from a lack of readiness in large organizations.

"Cybersecurity threats have evolved at a much faster pace than the skills of the executives (and teams) that hold responsibility for deterring those threats."

Perhaps most critically, this vulnerability is not simply a function of gaps in technical infrastructure. Rather, many companies are finding that talent gaps—most notably among chief information security officers (CISO) and their broader information security departments—are more troubling than technical gaps. Painful experience has taught many firms that the nature of cybersecurity threats has evolved at a much faster pace than the skills of the executives (and teams) that hold responsibility for deterring those threats.

This (ominous) leadership and talent gap should force all organizations to rethink the shape and structure of the chief information security officer role, as well as the capability requirements for the executives who occupy the position. To this end, this paper is designed to provide organizations with a sharper perspective on:

- The (fast) changing responsibilities of the CISO role.
- The fundamental skills, competencies and experience necessary to succeed in the CISO role today.
- How the smartest companies are competing for and attracting top cybersecurity talent.
- How those same companies are positioning CISOs (and their teams) to succeed.

NEW THREATS, NEW LEADERSHIP REQUIREMENTS

Beyond confronting a surge in criminal hacker activity, CISOs now face a wide array of risks that have significantly increased the complexity of their role. Indeed, CEB, a global research firm, recently documented a daunting list of emerging challenges confronting CISOs, with risk generated by the near ubiquity of mobile devices; the growing global scope of information assets; the rising difficulty of complying with new regulations; and the specter of state-sponsored attacks.[7]

The fast-evolving nature (and heightened intricacy) of the risk environment is forcing firms to redefine the core requirements of the CISO role.

[6] Verizon, 2013 *Data Breach Investigations Report (DBIR): Sophistication*, 2013.
[7] CEB, *Risk Intelligence Quarterly*, Q1 2014.

As a first step in this direction, many organizations are elevating the level (or altitude) of the role itself, ensuring that the CISO is positioned either as a key direct report to the enterprise chief information officer, chief risk officer or general counsel.

While this elevation of the role is necessary, it is also insufficient. "Moving the box on the org chart" is essential for signaling the importance of the function and extending connectivity to the executive team, but such action is unlikely to make a difference unless expectations for the role are simultaneously redefined.

As companies raise the profile and prominence of the CISO role, they also must require that the responsibilities of top cybersecurity executives change in five important ways:

- ***From Urgent Responders to "Urgent Responders and Proactive Innovators":*** The quickly changing nature of the threat environment means that CISOs must develop a clear vision of how the tactics of hackers will evolve. Visionary leadership is now a core requirement of the role, with leading executives demonstrating real skill at developing sophisticated scenario plans.
- ***From Methodical Managers to "Methodical Managers and Agile Adapters":*** The CISO role always has demanded relentless attention to process and detail. While still necessary, this emphasis on process sometimes lulls executives into basic routines. To avoid this trap, CISOs today must demonstrate real agility—a willingness and ability to pivot and respond with alacrity to changes in the threat environment.
- ***From Compliance Managers to "Compliance Managers, Educators and Influencers":*** The vast majority of cyber vulnerability occurs outside the direct reach and control of the cybersecurity department, with routine employee behavior often generating the greatest risk exposure. Leading CISOs recognize that the scale of this challenge (i.e., influencing the day-to-day actions of thousands of individuals) requires a sharp focus on education and influence. Rather than simply deploying perfunctory compliance training sessions on the "why, what and how" of information security, these executives engage directly with line leaders to build a culture of vigilance.
- ***From Tactical Operators to "Tactical Operators and Strategic Leaders":*** Perhaps most critically, CISOs now must operate strategically, ensuring clear (and clearly visible) alignment between business strategy and cybersecurity strategy. Top CISOs have an influential and compelling voice at board meetings and in executive committee discussions. And CISOs articulate cybersecurity strategy not as a simple cost of doing business but, instead, as a crucial enabler of business outcomes.
- ***From Technicians to "Technicians and Talent Magnets":*** Frequently (unfairly) stereotyped as hidebound technicians, leading CISOs engage actively and outwardly in the talent market. These executives take as a given that their ability to stay ahead of threats will largely be a function of the capacity to attract, develop and retain the best cybersecurity talent—and they allocate their time and energies accordingly.

> **"Core leadership and general management competencies — rather than technical ability — stand as the clear differentiators of the very best cybersecurity executives."**

WHERE DO LEADING CISOS COME FROM?

Of course, organizations cannot simply redefine CISO expectations and hope that their CISOs are up to the task. Instead, companies must take a hard look at the core capabilities of the individual occupying the CISO role. Many executives in the role today are fully ready and able to adapt to the changes in the environment. But our experience suggests that more than one-third of sitting CISOs lack the fundamental competencies needed to meet the demands of these new role requirements.

But can a CISO's readiness be predicted based on the nature of one's on-paper profile (e.g., educational credentials and career experience)? At first glance, the educational background and career experience of CISOs differ notably from one executive to the next. In turn, organizations often struggle to define the ideal characteristics of their future CISO.

"Organizations accustomed to positioning cybersecurity as a niche role in IT will experience sticker shock when first learning of the compensation requirements of top CISO candidates."

Given this challenge, Russell Reynolds Associates undertook an effort to understand the career path and profile of 20 leading CISOs. Our analysis sought to answer two basic questions:

- Is there a consistent, discernible CISO profile among the best executives in this field?
- Do the best executives in this field cluster around a single, dominant profile?

The answer to our first question was a clear "yes." While these 20 executives exhibit a range of backgrounds, their profile fits into four distinct categories:

- **Profile 1: Corporate Cybersecurity "Lifers":** Often holding a technical degree in engineering or computer science, these executives typically begin their career in the cybersecurity function of a large organization and climb their way to the top.
- **Profile 2: General Technologists:** Frequently holding a technical degree in engineering or computer science, these executives normally begin their career in corporate IT (e.g., applications development) and migrate to a specialization in cybersecurity.
- **Profile 3: Military or Law Enforcement Professionals:** Less commonly holding a technical degree, these executives begin their career in the military or law enforcement, gaining technical expertise via experience and rising to a senior cybersecurity role before migrating to a senior position within the cybersecurity function of a corporation.
- **Profile 4: Cybersecurity Product Specialists:** Less commonly holding a technical degree, these executives begin their career with a vendor of cybersecurity products. Similar to CISOs with military or law-enforcement backgrounds, product specialists also tend to gain technical expertise via experience and rise to a senior role before migrating to a senior position within the cybersecurity function of a corporation.

Notably, however, the distribution of the 20 executives in our analysis was fairly even across each of these four profiles. And our broader experience indicates that all four of these profiles are also found in abundance in the larger CISO population outside our group of 20 leaders.

Taken together, these facts provide an answer to our second question. The differentiating feature of the best CISOs is not a single, common set of educational credentials or career experiences. Of course, both matter foundationally. However, our analysis demonstrates that executives falling into any one of these four profiles of education and experience can reach the top of the cybersecurity field.

WHAT DIFFERENTIATES LEADING CISOS?

What, then, distinguishes leading CISOs from average CISOs?

Our work in the field suggests that core leadership and general management competencies—rather than technical ability—stand as the clear differentiators of the very best cybersecurity executives.

This is not to say that technical ability can be cast aside. To the contrary, technical competence is a core feature of the profiles of nearly all leading CISOs. That said, technology know-how also is a core feature of the profiles of nearly all average (and less-than-average) CISOs. In other words, technical competence is required but is insufficient, in and of itself, for success in the CISO role. Technical skills are table stakes, not differentiators.

"Too often, the first meeting between the CISO and the executive team occurs when the CISO is called into an emergency session to brief the firm's leaders on a significant breach."

Instead, the most effective CISOs are bringing new sets of capabilities to the position. Beyond a necessary (and relentless) focus on results, the following competencies stand out as key differentiators of the most effective executives in this role:

- ***Business Acumen and Analytics:*** Leading CISOs develop and demonstrate a deep understanding of their firm's competitive strategies, business models and underlying economics. These executives are intimately familiar with their firm's key strategies for acquiring and retaining customers. These leaders can insightfully describe their firm's cost structures and understand the tradeoffs associated with sales and marketing channels. Armed with this knowledge, top CISOs ensure that cybersecurity strategies reflect not only the threat environment but also the strategic imperatives of the business.
- ***Creativity and Innovation:*** Leading CISOs have an appreciation for proven playbooks and practices, but top executives also bring a zeal for creativity and innovation to their role. They recognize that "failure of imagination" often is the root cause of security breaches, and effective CISOs pride themselves on being more creative than hackers.
- ***Business-Relevant Communication:*** Leading CISOs are as comfortable describing how their company makes money as they are in explaining cybersecurity architecture. A depth of business acumen enables these executives to convey cybersecurity strategy in the native tongue of operating executives. And by communicating in business-relevant language, these executives ensure that their departments (and investments) are viewed as core features of business strategy, not simply burdensome costs of doing business.
- ***Relationships, Influence and Presence:*** Leading CISOs excel at building relationships from the C-suite to the shop floor. Top executives recognize that cybersecurity hinges on culture as much as systems, and CISOs energetically engage in the task of establishing connections to key influencers across the organization. These leaders also demonstrate the executive presence required to build and maintain credibility in the boardroom and executive suite.
- ***People Leadership:*** Leading CISOs challenge the assumption that technical leaders, by definition, lack people-leadership skills. These executives over-invest in acquiring, developing and retaining top talent. They ensure that their teams are fully aligned and engaged with the core mission of the cybersecurity function. And top leaders measure their long-term success by the ability to develop a bench of successors capable of stepping into the CISO role.

The most notable feature on this list is that, at first glance, most of these competencies look remarkably soft. But, as aforementioned, our experience demonstrates that hard technical skills are not differentiators of top performers in this role. Instead, top CISOs are distinguished by their unique ability to define a vision, secure support for that vision with the board and the C-suite, marshal the resources and talent required to translate that vision into reality, and engage the broader employee population in becoming champions for information security (rather than merely being in compliance with security policies). Put simply, as the role gets harder, this "soft stuff" matters more.

ATTRACTING THE BEST CISO TALENT

The changing nature of the CISO role forces organizations to rethink their approach to attracting and developing cybersecurity talent. Old methods likely will produce talent that is best suited to address old challenges. As enterprises consider creating, filling or (over time) managing succession for the CISO role, they must creatively confront the realities of the external market.

Demand far outstrips supply for the new model of top CISO talent. In particular, individuals with both technical credibility and core leadership capability are exceptionally scarce. To successfully attract candidates who fit this profile, organizations must consider four tactics:

- **Sell the Vision for the Role, Not Simply the Day-to-Day Responsibilities of the Job.** Top CISOs tend to be satisfied with their current role. They also have the luxury of an abundance of career options. As a result, these executives are not especially likely to be lured away by the "same job in a different company." Rather, they will gravitate toward a unique opportunity to simultaneously stretch their capabilities and demonstrate impact against meaningful objectives. With this in mind, companies must craft a credible vision for the CISO role before approaching the market. Unlike a standard job specification (with a laundry list of responsibilities and desired qualities), a vision for the role is a simple statement of the compelling, concrete objectives that the CISO will be expected to achieve. The content of this vision certainly will vary from firm to firm, but the importance of a clearly articulated "vision for the role" is an essential tool across firms.
- **Ensure Direct Engagement of the CEO in the Recruitment Process.** Top CISOs will consider roles within only those organizations that demonstrate a strong strategic commitment to the importance of cybersecurity. And no amount of reassurance from the chief information officer, chief risk officer or general counsel is likely to convince these executives that cybersecurity maintains a prominent place on the CEO's list of priorities. This message must come directly from the CEO, who should play a visible role in the final assessment and recruitment of the finalist candidate.
- **Demonstrate Flexibility on the Scope of the Role.** Top CISOs rarely are empire builders, but they do require their organization to provide them with the latitude necessary to confront the staggering array of threats in the security environment. In turn, these executives frequently will aim to negotiate on the scope of the role itself. Organizations naturally are reticent to bend the boundaries of jobs, but companies should not shun this discussion. A lack of willingness to engage in this conversation will often repel the most talented candidates.
- **Prepare to Pay for Top Talent.** Talent scarcity is unsurprisingly leading to rising compensation for the top CISO role. Total annual cash compensation in the range of $400,000 to $600,000

is increasingly normal for this position, with leading executives at top firms now often commanding total annual compensation packages of more than $1 million. Organizations accustomed to positioning cybersecurity as a niche role in IT will experience sticker shock when first learning of the compensation requirements of top CISO candidates. And, to be sure, astute CEOs and chief human resources officers will not allow headlines to lead them to overpay for the role. That said, compensation for this role should be set according to market benchmarks rather than anchored on the compensation of the previous CISO.

POSITIONING FOR SUCCESS

Cybersecurity no longer can remain a technical discipline confined to a centralized group within IT. Instead, cybersecurity now must stand as a broad organizational capability. For efforts to succeed, employees across the organization must be fully equipped, engaged and enabled to deter potential security threats.

At the same time, this broader organizational capability must be driven by a highly influential, central cybersecurity function. And the structure and positioning of the cybersecurity team will significantly influence its ultimate success or failure.

While there is no one-size-fits-all model for structuring and deploying an information security function, our experience suggests that the following factors frequently prove critical:

- **Reporting Altitude:** CISOs invariably will struggle to demonstrate executive influence when their title or reporting line suggests "backroom administrator." At a minimum, the CISO must be a prominent member of the chief information officer's, chief risk officer's, or general counsel's leadership team.
- **Board and C-Suite Exposure:** CISOs must maintain a consistent presence at meetings of both the board and the executive committee. Too often, the first meeting between the CISO and the executive team occurs when the CISO is called into an emergency session to brief the firm's leaders on a significant breach. Without a consistent rotation in front of these groups, CISOs will lack the influence and connectivity needed to ensure a forward-looking approach to cybersecurity.
- **Distributed Deployment:** Advances in an organization's cybersecurity readiness are unlikely to occur exclusively via missives and policies issued from a central, isolated group. Information security professionals must be deployed within the business units they serve. And just as CISOs must maintain a continuing presence with enterprise leadership teams, business unit cybersecurity professionals must build strong connections to the leadership teams (and broader employee bases) at their decentralized locations.

IN CONCLUSION

Leading companies recognize that their ability to confront rising cybersecurity risk is largely driven by the quality of talent within the cybersecurity function, with a particular emphasis on ensuring that the CISO role is held by an executive who is as comfortable in the boardroom as in the IT backroom. Companies lacking this type of CISO leadership will grow increasingly vulnerable. And as recent experience demonstrates, these vulnerabilities are unlikely to go unnoticed by cybercriminals.

Leadership, Succession and Search | Russell Reynolds Associates is a global leader in assessment, recruitment and succession planning for Chief Executive Officers, boards of directors, and key roles within the C-suite. With more than 300 consultants in 42 offices around the world, we work closely with both public and private organizations across all industries and regions. We help our clients build boards and executive teams that can meet the challenges and opportunities presented by the digital, economic, environmental and political trends that are reshaping the global business environment. **www.russellreynolds.com**. Follow us on Twitter: **@RRAonLeadership**

Americas

Atlanta
1180 Peachtree St., NE
Suite 2250
Atlanta, GA 30309-3521
United States of America
Tel: +1-404-577-3000

Boston
One Federal Street, 26th Floor
Boston, MA 02110-1007
United States of America
Tel: +1-617-523-1111

Buenos Aires
Buenos Aires Plaza
Manuela Sáenz 323
Seventh Floor, Suites 14 and 15
C1107BPA, Buenos Aires
Argentina
Tel: +54-11-4118-8900

Calgary
Suite 750, Ernst & Young Tower
440-2nd Avenue SW
Calgary, Alberta T2P 5E9
Canada
Tel: +1-403-776-4192

Chicago
155 North Wacker Drive
Suite 4100
Chicago, IL 60606-1732
United States of America
Tel: +1-312-993-9696

Dallas
200 Crescent Court, Suite 1000
Dallas, TX 75201-1834
United States of America
Tel: +1-214-220-2033

Houston
600 Travis Street, Suite 2200
Houston, TX 77002-2910
United States of America
Tel: +1-713-754-5995

Los Angeles
11100 Santa Monica Blvd.
Suite 350
Los Angeles, CA 90025-3384
United States of America
Tel: +1-310-775-8940

Mexico City
Torre Reforma
Paseo de la Reforma
115-1502
Lomas de Chapultepec
11000 México, D.F.
México
Tel: +52-55-5249-5130

Minneapolis/St. Paul
225 South Sixth Street, Suite 2550
Minneapolis, MN 55402-3900
United States of America
Tel: +1-612-332-6966

New York
200 Park Avenue
Suite 2300
New York, NY 10166-0002
United States of America
Tel: +1-212-351-2000

Palo Alto
260 Homer Avenue, Suite 202
Palo Alto, CA 94301-2777
United States of America
Tel: +1-650-233-2400

San Francisco
101 California Street
Suite 2900
San Francisco, CA 94111-5829
United States of America
Tel: +1-415-352-3300

São Paulo
Edifício Eldorado Business Tower
Av. Nações Unidas, 8.501 11°
05425-070 São Paulo
Brazil
Tel: +55-11-3566-2400

Stamford
301 Tresser Boulevard
Suite 1210
Stamford, CT 06901-3250
United States of America
Tel: +1-203-905-3341

Toronto
Scotia Plaza, Suite 3410
40 King Street West
Toronto, ON
M5H 3Y2
Canada
Tel: +1-416-364-3355

Washington, D.C.
1701 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20006-5810
United States of America
Tel: +1-202-654-7800

Asia/Pacific

Beijing
Unit 3422 China World Tower 1
No. 1 Jian Guo Men Wai Avenue
Beijing 100004
China
Tel: +86-10-6535-1188

Hong Kong
Room 1801, Alexandra House
18 Chater Road Central
Hong Kong
China
Tel: +852-2523-9123

Melbourne
Level 51, Rialto Towers
525 Collins Street
Melbourne, VIC 3000
Australia
Tel: +61-3-9603-1300

Mumbai
Unit 9(A), Grand Hyatt Plaza
Santacruz (East)
Mumbai 400 055
India
Tel: +91-22-6733-2222

New Delhi
203, Eros Corporate Tower
Nehru Place
New Delhi 110 019
India
Tel: +91-11-4603-4600

Seoul
16F West Tower
Mirae Asset Centre 1 Building
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82-2-6030-3200

Shanghai
Room 4504, Jin Mao Tower
88 Century Avenue
Pudong, Shanghai 200121
China
Tel: +86-21-6163-0888

Singapore
2 Shenton Way
#08-01 SGX Centre 1
Singapore 068804
Singapore
Tel: +65-6225-1811

Sydney
Level 40 Aurora Place
88 Phillip Street
Sydney NSW 2000
Australia
Tel: +61-2-9258-3100

Tokyo
Izumi Garden Tower 14F
1-6-1 Roppongi
Minato-ku, Tokyo 106-6014
Japan
Tel: +81-3-5114-3700

Europe

Amsterdam
World Trade Center
Tower H, 18th Floor
Zuidplein 148
1077 XV Amsterdam
The Netherlands
Tel: +31-20-305-7630

Barcelona
Edificio Prisma
Avda. Diagonal, 613, 2˚A
08028 Barcelona
Spain
Tel: +34-93-494-9400

Brussels
Boulevard St. Michel 27
B-1040 Brussels
Belgium
Tel: +32-2-743-12-20

Copenhagen
Kongens Nytorv 3
DK-1050 Copenhagen K
Denmark
Tel: +45-33-69-23-20

Frankfurt
OpernTurm
60306 Frankfurt am Main
Germany
Tel: +49-69-75-60-90-0

Hamburg
Stadthausbrücke
1-3/Fleethof
20355 Hamburg
Germany
Tel: +49-40-48-06-61-0

Istanbul
Cumhuriyet Cad. No 48
Kat: 4/B Pegasus Evi
Elmadağ 34367 Şişli
Istanbul / Türkiye
Tel: +90-212-705-3550

London
Almack House
28 King Street
London SW1Y 6QW
United Kingdom
Tel: +44-20-7839-7788

Madrid
Calle Miguel Angel, 11, 7°
28010 Madrid
Spain
Tel: +34-91-319-7100

Milan
Via Mascheroni, 5
20123 Milan
Italy
Tel: +39-02-430-015-1

Munich
Maximilianstraße 12-14
80539 München
Germany
Tel: +49-89-24-89-81-3

Paris
20 rue de la Paix
75002 Paris
France
Tel: +33-1-49-26-13-00

Stockholm
Hamngatan 27
SE-111 47 Stockholm
Sweden
Tel: +46-8-545-074-40

Warsaw
Belvedere Plaza
ul. Belwederska 23
00-761 Warsaw
Poland
Tel: +48-22-851-68-38

Zürich
Löwenstrasse 28
CH-8001 Zurich
Switzerland
Tel: +41-44-447-30-30