Cyber Security:

Five Leadership Issues Worthy of Board and Executive Attention

Russell Reynolds Associates

Introduction

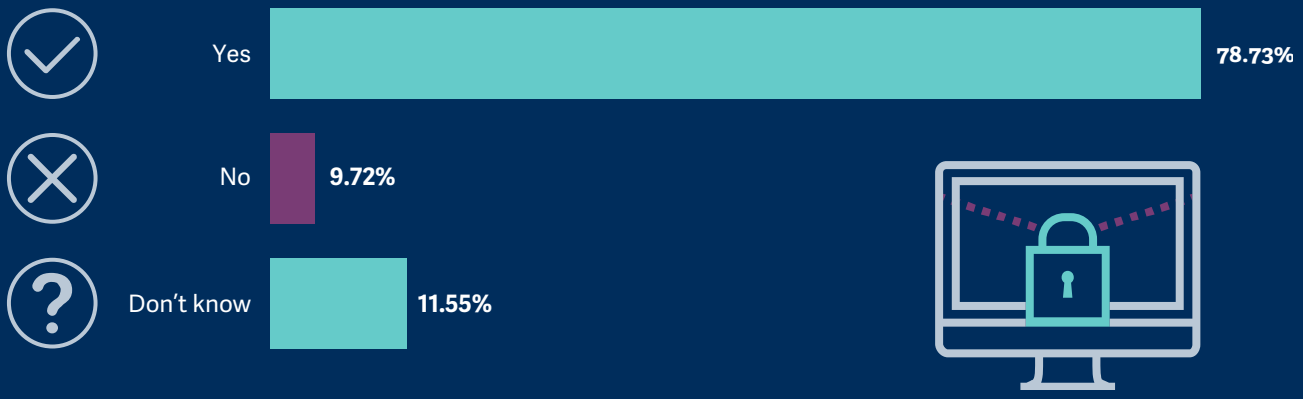
1. How effectively does your board discuss emerging risks like cyber security?
2. How effective is your chief information security officer (CISO) at clarifying the nature and urgency of cyber security risk with your board and executive team?
3. Does your CISO maintain a siloed technology view or a broader business/risk view?
4. How plugged-in is your CISO?
5. Do you have the right leadership and talent in place to protect your business?

Board Readiness

How effectively does your board address emerging risks like cyber security?

Successful security strategies require boards to play a fundamental role. While boards have focused on mitigating financial risk by way of audit committees, they must now broaden their focus to include emerging risks like cyber security. As cyber security becomes a greater concern, boards must play a more active role in navigating their firm through an increasingly complex and challenging environment.

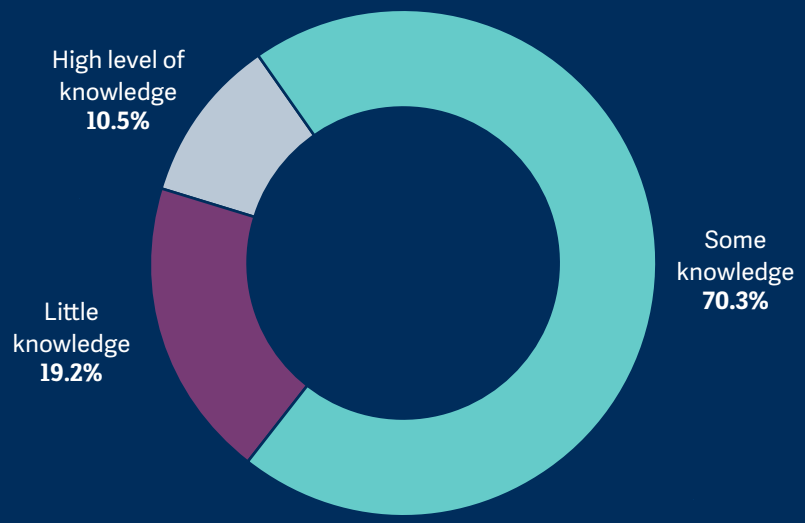
VIEW FROM CISOs: IS YOUR BOARD OF DIRECTORS CONCERNED WITH SECURITY?[1]



BOARD KNOWLEDGE OF EMERGING RISKS[2]

Despite changes in how boards view risk allocation—and additional focus on financial risk—most directors lack knowledge of emerging risks like cyber security.

Director Understanding of Cyber Security Risks



1. "No Respect: Chief Information Security Officers Misunderstood and Underappreciated by their C-level Peers," ThreatTrack Security, 2014.
2. "2014-2015 Public Company Governance Survey," National Association of Corporate Directors.

KEY POINTS

- Being proactive by embracing a broader risk management approach and prioritizing key issues like cyber security are no longer options but a necessity.
- Managing risk is increasingly a board-wide function as focus on emerging threats like cyber security continues to increase.
- While boards give more of their attention to major risks like cyber security, most directors still lack a deep understanding of cyber security risk.

Clarifying Risk and Driving Urgency

How effective is your CISO at clarifying the nature and urgency of cyber security risk with your board and executive team?

As organizations continue to focus their attention on cyber security risks, CISOs will remain fundamental to developing and implementing the organization's security strategy and vision. With boards increasingly dependent on CISOs for both information and the execution of security strategy, organizations must have the right security leadership in place and the proper reporting structure to establish key communication channels with the broader leadership team and to protect the enterprise.

WHILE CYBER SECURITY IS A GROWING CONCERN, THERE STILL REMAINS A LACK OF COMMUNICATION BETWEEN THE EXECUTIVE TEAM AND THE CISO

26%

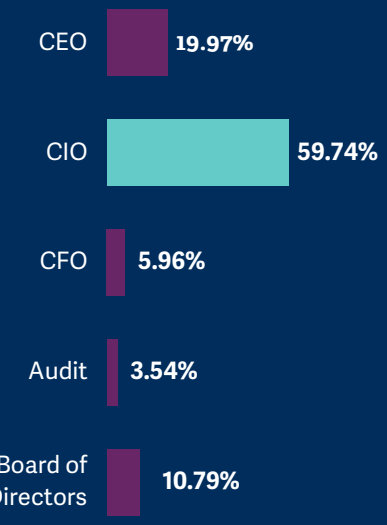
of respondents in a PricewaterhouseCoopers survey of over 500 executives and public officials said their CISO makes a security presentation to the board only once a year, while 30% of respondents said their senior security executive makes quarterly security presentations. 28% of respondents said their security leaders make no presentation at all.[2]

49%

of respondents in The Global State of Information Security Survey 2015 by PricewaterhouseCoopers said their organization had a cross-organizational team that regularly convenes to discuss, coordinate, and communicate information security issues.[3]

TO WHOM DOES SECURITY REPORT IN YOUR ORGANIZATION?[1]

Despite the prominence of cyber security threats, most CISOs continue to report to the CIO.



HAVING THE WRONG COMMUNICATION CHANNELS WITHIN AN ORGANIZATION HAS REAL FINANCIAL CONSEQUENCES[4]

14%

Organizations in which the CISO reported to the CIO experienced 14% more downtime due to cyber security incidents than those organizations in which the CISO reported directly to the CEO.

46%

Financial losses were 46% higher in organizations where the CISO reported to the CIO than when the CISO reported to the CEO. According to PwC's *The Global State of Information Security Survey 2014*, having the CISO report to almost any position in senior management other than the CIO (board of directors, CFO, etc.) reduced financial losses from cyber incidents.

1. State of Cyber security: Implications for 2015, ISACA and RSA Conference Study
2. US Cyber security: Progress Stalled – Key Findings from the 2015 US State of Cybercrime Survey, PwC, 2015
3. The Global State of Information Security Survey, PwC, 2015
4. The Global State of Information Security Survey, PwC, 2014

KEY POINTS

- Despite cyber security's growing prominence, there remains a lack of communication between security leaders and senior leadership.
- Many firms still don't have a proper reporting structure in place to establish better communication channels.
- Evidence suggests that having the CISO report to the CIO increases the likelihood and severity of security incidents.

IT Expert or Business Leader?

Does your CISO maintain a siloed technology view or a broader business/risk view?

CISOs must operate strategically, ensuring clearly visible alignment between business strategy and cyber security strategy. Top CISOs have an influential and compelling voice at board meetings and in executive committee discussions. And CISOs articulate cyber security strategy not as a simple cost of doing business but, instead, as a crucial enabler of business outcomes.

WHAT IS THE BIGGEST SKILL GAP YOU SEE IN TODAY'S SECURITY PROFESSIONALS?[1]

There is a prevailing sense that individuals in the CISO role are specialists with a narrow skill set.

While half of executives believed CISOs provide valuable guidance to leadership, nearly one-fifth view the role as primarily an advisor to the CIO on cyber security strategy.

The growing complexity of organizations requires CISOs to both protect the enterprise and support broader business objectives. Managing this balance is increasingly important, not just to the near-term health of the business but to the long-term clout of the CISO role, a role that many organizations have elevated and have included in broader strategic decision making.

62%

of CISOs developed their security strategy in conjunction with other strategies (primarily IT, risk and operations).[3]

28%

of executives said a decision by their CISO has hurt their business' bottom line.[2]

MANY CISOs STILL LACK THE CLOUT WITHIN THEIR ORGANIZATION TO UNDERSTAND THE BUSINESSES THEY PROTECT, THOUGH THIS UNDERSTANDING IS BECOMING INCREASINGLY IMPORTANT TO THEIR ROLE. [4]

61%

of executives did not believe their CISO would succeed in a non-information security leadership position within their organization.

68%

of executives did not agree that CISOs possessed broad awareness of organizational objectives and business needs outside of information security.

74%

of executives did not believe CISOs should be part of organizational leadership teams.

1. *State of Cybersecurity: Implications for 2015*, ISACA and RSA Conference Study
2. "No Respect: Chief Information. Security Officers Misunderstood and Underappreciated by their C-level Peers," ThreatTrack Security, 2014.
3. *Fortifying for the Future of Security*, IBM 2014 CISO Assessment.
4. "No Respect: Chief Information Security Officers Misunderstood and Underappreciated by their C-level Peers," ThreatTrack Security, 2014.

KEY POINTS

- The CISO role demands a strong understanding of the business, not just technical ability.
- There still remains a large number of security leaders who do not build their security strategy around the business.
- Many executives do not understand the CISO's new, expanding role, which makes it challenging for CISOs to exert influence across the company and align cyber strategy with business strategy.

Having a Strong Relationship Network

How plugged-in is your CISO?

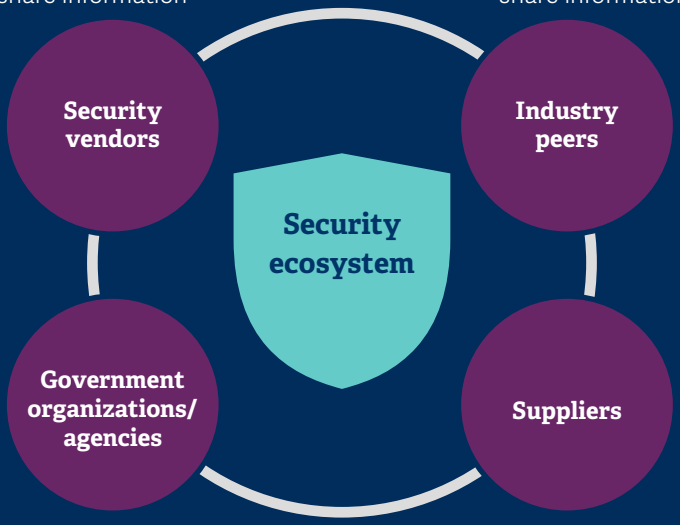
Information sharing has never been more essential. CISOs need a strong external network to better understand the extent of their vulnerabilities, to adopt best practices and to attract security talent. Being externally focused and proactive rather than internally focused is essential.

SHARING THREAT INFORMATION[1]

CISOs face an increasingly complex security ecosystem. Communication among members of the ecosystem is extremely important, but organizations still are underperforming in this area.

57%
of security vendors share information

51%
of industry peers share information



43%
of government organizations/agencies share information

22%
of suppliers share information

EXTERNAL COLLABORATION IS MORE IMPORTANT FOR MAINTAINING INDUSTRY BEST PRACTICES AND COUNTERING THREATS FROM THE SAME SOURCE[3]

62% vs. 42%

While 62% of security leaders strongly agreed that the risk level to their organization was increasing due to the number of interactions and connections with customers, suppliers and partners, only 42% of organizations were a member of a formal industry-related security forum/group.

86%

of security leaders believed industry-related security groups will become more necessary in the next three to five years.

"External collaboration gives security leaders a chance to observe industry practices and evolve with their peers to better understand where the "good stuff" is happening... The reality of today's expansive threat landscape is that we can't fully protect everything. Other firms face the same challenge so hearing the perspectives of my peers helps to improve our strategies around our most sensitive information."[2]

John Taylor, former Global Head of IT Security, British American Tobacco

1. *Fortifying for the Future of Security*, IBM 2014 CISO Assessment.
2. Ibid.
3. ibid.

KEY POINTS

- Protecting not just the firm but the ecosystem is becoming increasingly essential for organizations.
- In order to protect the ecosystem, CISOs must be externally focused and proactively build a strong network of contacts among customers, suppliers, security vendors, and government agencies.
- Regular communication among the firm's existing stakeholders in the ecosystem is and will continue to be an important part of a sound security strategy.

Talent Is the Best Defense

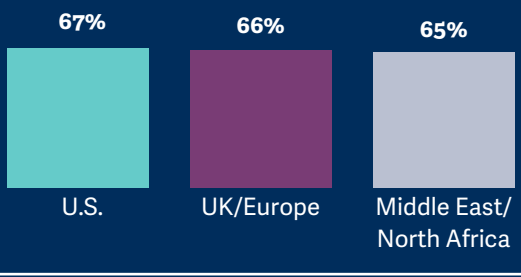
Do you have the right leadership and talent in place to protect your business?

The increasing complexity of cyber security threats requires new types of security leaders who can go beyond their traditionally narrow technical domains and understand how to protect the business in a holistic way. Cyber security leaders who can effectively do these things are scarce. With a high demand for talent and a low supply, knowing where to look for talent will become increasingly critical.

THE CYBER TALENT GAP WILL PERSIST[1]

A study by the Ponemon Institute for Raytheon in 2015 showed that the verdict across regions was the same: Organizations need more knowledgeable and experienced cyber security practitioners.

My Organization Needs More Knowledgeable and Experienced Cyber Security Practitioners



FACTORS THAT WILL HINDER IMPROVEMENT OVER THE NEXT THREE YEARS[2]

Organizations trying to prepare for the future face a number of challenges, including finding top talent. According to a major survey by the Ponemon Institute for Raytheon, the primary factor hindering improvement in cyber defense is the inability to hire and retain staff (45%), followed by a lack of actionable intelligence (44%) and the inability to curb employee-related security risks (43%).

WHERE DOES CYBER SECURITY TALENT COME FROM? CYBER SECURITY ARCHETYPES[3]:

Profile 1: Professional Services/Audit	Profile 2: General Technologists	Profile 3: Military or Law Enforcement Professionals	Profile 4: Cyber Security Threat Intelligence Specialists	Profile 5: Corporate Development/ Strategy Executives
Often holding a technical degree in engineering or computer science, these executives typically begin their career in the cyber security function of a large organization and climb their way to the top.	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 cyber security.	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 cyber security role before migrating to a senior position within the cyber security function of a corporation.	Cutting-edge cyber threat intelligence specialists who are extremely technical, often coming out of organizations like the National Security Agency or the broader intelligence community.	An emerging class of business leaders who are trained in cyber security and are positioned for broader risk management roles.

1. *2015 Global Megatrends in Cybersecurity*, Ponemon Institute for Raytheon, February 2015.
2. Ibid.
3. Russell Reynolds Associates proprietary study.

KEY POINTS

- As cyber security persists as a primary concern, the focus will shift heavily on talented leaders with both technical aptitude and business acumen.
- With a limited supply of talent, organizations must know where to find top talent in markets and sectors with which they may not be familiar, including the public sector.
- Developing bench strength below the CISO will become increasingly important as organizational challenges become more complex.

Russell Reynolds Associates is a global leader in assessment, recruitment and succession planning for boards of directors, chief executive officers and key roles within the C-suite. With more than 370 consultants in 46 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.

GLOBAL OFFICES

Americas

- Atlanta
- Boston
- Buenos Aires
- Calgary
- Chicago
- Dallas
- Houston
- Los Angeles
- Mexico City
- Minneapolis/St. Paul
- Montréal
- New York
- Palo Alto
- San Francisco
- São Paulo
- Stamford
- Toronto
- Washington, D.C.

EMEA

- Amsterdam
- Barcelona
- Brussels
- Copenhagen
- Dubai
- Frankfurt
- Hamburg
- Helsinki
- Istanbul
- London
- Madrid
- Milan
- Munich
- Oslo
- Paris
- Stockholm
- Warsaw
- Zurich

Asia/Pacific

- Beijing
- Hong Kong
- Melbourne
- Mumbai
- New Delhi
- Seoul
- Shanghai
- Singapore
- Sydney
- Tokyo

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 Fl.
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 & 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.
Mexico
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

Montréal
2000 McGill College Ave
6th Floor
Montreal Quebec H3A 3H3
Canada
Tel: +1-514-416-3300

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 11º
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
63, 3rd North Avenue,
Maker Maxity
Bandra Kurla Complex
Bandra (East), Mumbai 400 051
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

EMEA

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

Dubai
Dubai International Financial Center
Burj Daman, Office C610
Dubai
United Arab Emirates
Tel: +971-56-1748304

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

Helsinki
Unioninkatu 22
00130 Helsinki
Finland
Tel: +358-9-6226-7000

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

Oslo
Haakon VIIs Gata 1
NO-0161 Oslo
Norway
Tel: +47-2203-8010

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

RussellReynolds.com