2020
North American Chief Information Security Officer (CISO) Compensation Survey

Contents

A message from the authors

Welcome to our *2020 North American Chief Information Security Officer (CISO) Compensation Survey*, which examines both organizational structure and compensation for this increasingly critical role.

For this report, Heidrick & Struggles compiled compensation data from a survey fielded in April and May of this year of 372 CISOs in North America. While most carried the title of chief information security officer, the survey group also included deputy chief information security officers, as well as chief security officers and senior information security executives.

We hope you enjoy reading the survey, which is the only one of its kind. As always, suggestions are welcome, so please feel free to contact us—or your Heidrick & Struggles representative—with questions and comments.

With warmest regards,

Matt Aiello
Partner
Cybersecurity Practice

maiello@heidrick.com

Scott Thompson
Principal
Financial Services Practice

sthompson@heidrick.com

On confidentiality

The 2020 North America chief information security officer (CISO) survey has been conducted on an anonymous basis for individuals and their employers. Heidrick & Struggles has removed the data relating to identity from reported compensation figures.

Acknowledgments

The authors wish to thank **Mohd Arsalan** for his contributions to this report.

Methodology

In an online survey, we asked participants to provide information on how their role is structured, to whom they report and who reports to them, and data on 2019 compensation including base salary, bonus, and equity or long-term incentive, as well as joining bonuses. All data collected was self-reported by information security professionals and has been aggregated.

All compensation figures in tables and charts are reported in USD.

Overall respondent demographics

Overall sample (%)

All respondents	n = 405	100
Respondents with compensation data	n = 372	92

Function/role (%)

Chief information security officer	n = 276	74
Deputy chief information security officer	n = 11	3
Chief security officer	n = 46	12
Senior information security executive	n = 39	11

Experience (%)

Less than 6 months	n = 27	7
6 months to 1 year	n = 26	7
1–2 years	n = 90	24
3–4 years	n = 96	26
5 or more years	n = 133	36

Revenue (%)

Pre-revenue	n = 4	1
$100m or less	n = 15	4
$101–$500m	n = 25	7
$501m–$1bn	n = 28	8
$1.1–$5bn	n = 69	19
$5.1–$20bn	n = 101	27
$20.1–$50bn	n = 51	14
More than $50bn	n = 58	16
Don't know/prefer not to answer	n = 21	6

Industry (%)

Financial services/fintech	n = 138	37
Industrial/manufacturing/energy	n = 30	8
Technology/telecoms/SaaS/cloud	n = 92	25
Healthcare/biotech/life sciences	n = 44	12
Consumer/retail/media	n = 35	9
Business or professional services	n = 11	3
Education/not-for-profit	n = 6	2
Other	n = 16	4

Note: Numbers may not sum to 100%, because of rounding.
Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

The widening role of the chief information security officer

The chief information security officer (CISO) has become a position of critical importance to companies large and small, in technology and in nearly every other industry. As we noted in a report[1] last fall, all companies must now worry about the vulnerability of their data and other critical information assets. Companies must secure systems from attack while simultaneously managing increased regulatory scrutiny of the security and use of the data these systems contain.

These are the foundational elements of every CISO role, and while those who take it on must have a wide range of skills, there is, as yet, no single approach to structuring the position or to its place in the corporate reporting hierarchy. CISOs that once used to focus on network security, firewalls, security policies, and governance now also find themselves tasked with securing connected devices, devising identity and access management systems, implementing artificial intelligence and machine learning, as well as risk management, privacy, investigations, and physical security, among other issues. And they are doing so while managing ever larger teams.

1 Matt Aiello and Scott Thompson, "Upending tradition: Modeling tomorrow's cybersecurity organization," Heidrick & Struggles, September 18, 2019, heidrick.com.

Varied role structure, varied compensation

Our research has identified three distinct types of CISOs today. Two are specialists—the traditional Security leader and a Risk/Trust leader—while the third, which we call CISO Plus, has an ever-expanding remit that takes in varying parts of the other two areas (see the following chart) and is most often found at midsize tech companies.[2] The security group included security operations and architecture, as well as penetration testing and product/app security. The risk group included governance, risk, and compliance, as well as business continuity planning, disaster recovery, and privacy. The trust group included physical security, trust and safety, fraud, and enterprise crisis management.

Perhaps because they have a broader portfolio, people with the CISO Plus role tend to be more highly compensated than other CISOs, our data shows. It's particularly notable that among the subset of people in the CISO Plus role with the most functions reporting to them—an average of eight—median total annual compensation rises to $1,026,000. We explore compensation in detail starting on page 8.

Anecdotally, we have found very little gender or racial/ethnic diversity in the CISO role, and, as a result, diverse CISOs are, in our experience, able to command bidding wars that also raise compensation.

2 The analysis was based on which functions CISOs said most often reported to them and which were most often chosen together.

Areas of responsibility

Security	Risk	Trust
Penetration testing	Governance, risk, and compliance	Fraud
Security architecture	Business continuity planning/disaster recovery	Trust and safety
Security operations	Privacy/CPO	Physical security
Product/app security		Enterprise crisis management

Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Different industries, different CISO focuses

CISO backgrounds and required expertise vary by industry. Financial services firms, for example, often have two information security leaders, one more technical ("first line") and another more oriented towards information risk, governance, and compliance ("second line"). And those firms, along with healthcare, energy, and telecom companies, will usually require some experience working in a highly regulated environment. CISOs at companies that sell connected products must be able to concentrate on the security of those products and understand the security risks of both normal wear and tear and planned obsolescence. In large industries such as auto manufacturing, there may be multiple CISOs, to focus on security not only at the corporate level but also within business units and at the product and manufacturing levels. This is understandable because each of these areas has different needs that require different expertise to address.

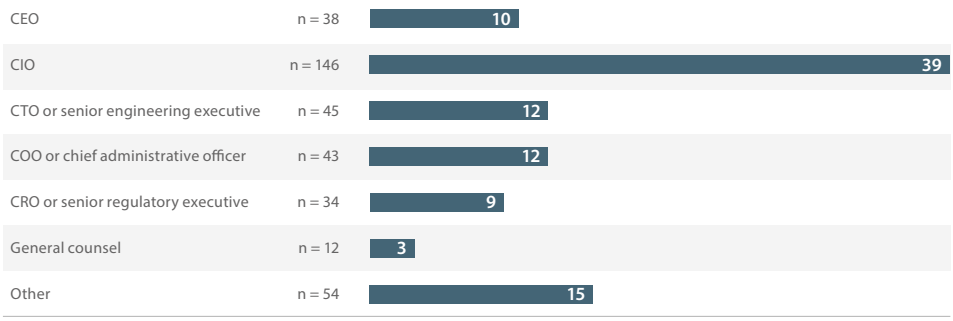
Reporting structure—not just the CIO anymore

An important theme has emerged in the past several years: the movement of the CISO role away from reporting to the CIO. Once viewed as an "IT function" alongside applications and infrastructure, security is moving more into the area of risk management and board accountability, closer to the role of internal audit. Our data reflects this—61% of all CISOs we surveyed report somewhere other than the CIO. Instead, they have a range of other reporting pathways: CEO, CTO, chief risk officer (CRO), chief operating officer (COO), or general counsel, among others. More regulated industries such as healthcare may skew the role towards risk and audit, while SaaS/cloud/tech companies orient the role around engineering leadership/CTO or COO.

Yet when the CISOs are broken out into their three distinct types, some interesting patterns appear. Sixteen percent of all those in the CISO Plus role report to the CEO, compared with 6% of Security CISOs and 3% of Risk/Trust CISOs. Among those who report to the CIO, 46% are Security, compared with 35% of CISO Plus and 26% of Risk/Trust. This latter group has the most diffuse reporting, with 16% reporting to the CRO or senior regulatory executive and 32% not reporting to any of the main positions we defined.

Overall reporting structure (%)

CISO reports to



Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Reporting structure by role type (%)

CISO reports to	Security	Risk/Trust	CISO Plus
Base size	168	31	173
CEO	6	3	16
CIO	46	26	35
CTO or senior engineering executive	15	6	10
COO or chief administrative officer	10	13	13
CRO or senior regulatory executive	8	16	9
General counsel	2	3	5
Other	13	32	13

Note: Numbers may not total 100%, because of rounding.
Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Industry distribution by role type (%)

	Security	Risk/Trust	CISO Plus
Financial services/fintech	44	52	28
Industrial/manufacturing/energy	6	13	9
Technology/telecoms/SaaS/cloud	21	13	31
Healthcare/biotech/life sciences	10	13	13
Consumer/retail/media	9	3	11
Business or professional services	3	0	3
Education/not-for-profit	2	3	1
Other	5	3	4

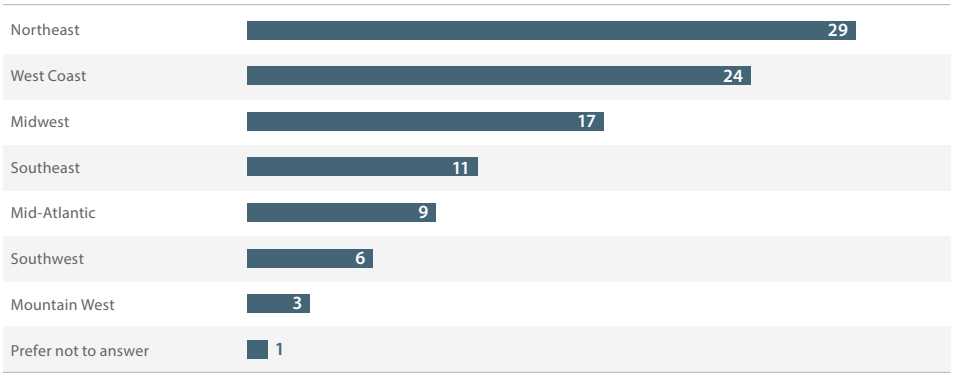
Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Other notable findings

Many information security teams are small, with 32% of all CISOs surveyed having 25 or fewer people reporting to them. Yet another 32% said they had 101 or more direct reports. And they have high visibility: 85% present directly to their company's board and/or audit committee.

Geographic distribution (%)

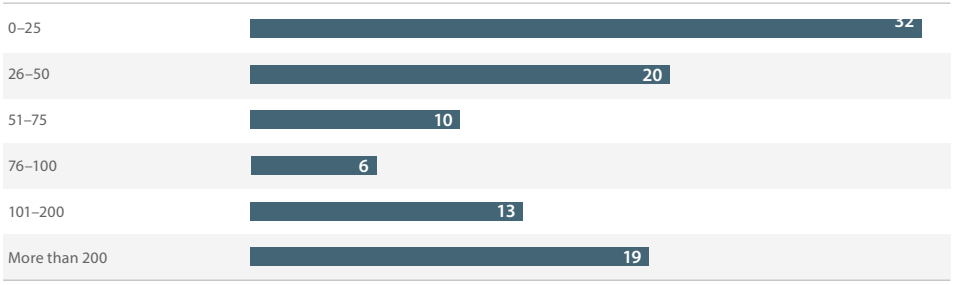
In which region of the US are you located?



Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Size of team (%)

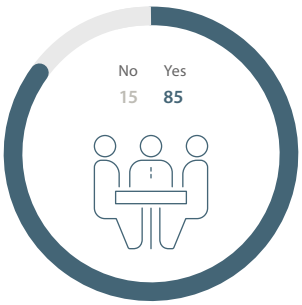
How many people are on your direct team?



Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Board/audit committee visibility (%)

Do you present directly to your company's board and/or audit committee?



Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Compensation

Annual compensation overall and by type of CISO role

As we have noted, people in the CISO Plus role tend to be more highly compensated than other CISOs, with a median cash base, cash bonus, and annual equity of $892,590, compared to $784,003 for all CISOs.[3] And the subset of the CISO Plus group with the highest number of functions reporting to them report median total annual compensation of $1,026,000.

3 To calculate total cash compensation, we totaled base and bonus for each individual and found the median. For total compensation including LTI/equity, we totaled base, bonus, and LTI/equity for each individual and then found the median. As a result, the total cash compensation and total compensation figures may not equal the sum of the individual median base, median bonus, and median LTI/equity shown in the charts.

Median base salaries fell within a narrow range of $326,000 for CISOs at companies with revenues of $5 billion or less, to $376,000 for companies with revenues above $20 billion. Median bonuses were substantially larger in this latter group: $206,690, compared with $95,753 for those in the former group. Equity and other long-term incentives were also higher for those with more direct reports.

Forty percent of CISOs surveyed reported median annual equity or long-term-incentive (LTI) compensation of less than $200,000, while 36% reported such compensation between $200,000 and $500,000, and 24% reported more. For 35%, the annual equity/LTI came in the form of restricted stock units (RSUs), while 34% reported this compensation as a mix of RSUs, performance share units (PSUs), and options.

Median compensation

	Median base ($)	Median bonus (%)	Median bonus ($)	Median total cash compensation ($)	Median equity/LTI ($)	Median total compensation including equity ($)
Overall	326,000	36	125,353	473,603	226,000	784,003
By number of reports						
100 or fewer	326,000	36	97,803	408,503	226,000	653,903
More than 100	451,000	56	294,184	765,765	376,000	1,131,546
By annual revenue						
$5bn or less	326,000	36	95,753	400,853	226,000	668,903
$5.1bn–$20bn	326,000	46	159,928	506,153	226,000	769,203
More than $20bn	376,000	46	206,690	621,390	326,000	967,715
By role type						
Security	326,000	36	125,353	471,253	226,000	731,653
Risk/Trust	276,000	36	80,053	336,928	100,000	514,628
CISO Plus	376,000	40	148,103	508,803	326,000	892,590
By quartile						
25th quartile	276,000	26	70,253	345,753	100,000	508,503
Median	326,000	36	125,353	473,603	226,000	784,003
75th quartile	451,000	56	255,340	700,528	451,000	1,160,928

Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Joining bonuses

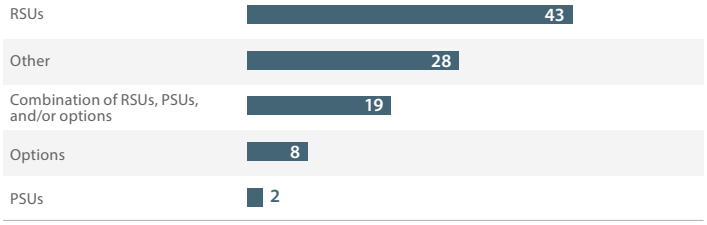
CISOs also reported receiving joining bonuses in cash and equity, which can be substantial. While the median cash bonus reported was $50,000, the average was $134,050 (a few respondents reported receiving very high joining bonuses). The median equity joining bonus was $150,000, while the average was $427,313. Sign-on equity most often came in the form of RSUs. Interestingly, newer CISOs reported higher median signing bonuses than longer-tenured ones, suggesting increasing competition for the most talented CISOs.

Those in the CISO Plus role reported receiving a median bonus of $148,103, compared to $125,353 for their Security counterparts and just $80,053 for Risk/Trust CISOs. Equity and long-term incentives were also the highest for those in the CISO Plus role.

Overall joining bonus and sign-on equity

Joining bonus ($)	In cash	In equity
Average	134,050	427,313
Median	50,000	150,000

Sign-on equity (%)

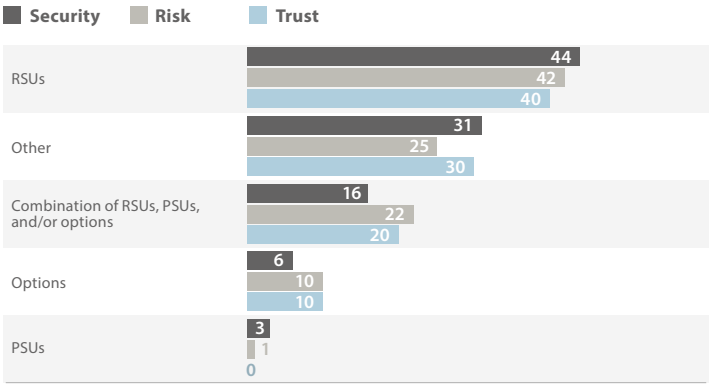


Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Joining bonus and sign-on equity by role type

Joining bonus ($)		In cash	In equity
Security	Average	113,186	334,482
	Median	50,000	100,000
Risk/Trust	Average	110,526	165,909
	Median	25,000	25,000
CISO Plus	Average	155,689	523,070
	Median	50,000	225,000

Sign-on equity (%)



Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Geographic comparisons

The largest companies in the Northeast are, on the whole, paying CISOs the most cash. The median total cash compensation was $610,428 at companies with revenues between $5.1 billion and $20 billion in the Northeast, and $700,528 at companies in the region with revenues above $20 billion. That compares with $404,678 and $508,803, respectively, at large West Coast companies, and $473,603 and $630,840, respectively, at companies elsewhere.

Median equity/LTI is higher on the West Coast, ranging from $326,000 at companies with revenues under $5 billion to $551,000 at companies above $20 billion in revenue. That compares with $226,000 and $276,000 at similarly sized companies in the Northeast.

Our survey found that median signing bonuses are also higher at smaller West Coast companies, likely because such companies there generally have a lower base and bonus and will often add joining bonuses to bridge compensation gaps. Also, in our experience, most West Coasters are joining from a company where they had unvested equity, so there is a cash flow gap that companies seek to address.

Median compensation by geographic region

Annual revenue		Median base ($)	Median bonus (%)	Median bonus ($)	Median total cash compensation ($)	Median equity/LTI ($)	Median total compensation including equity ($)
$5bn or less	West Coast	326,000	26	83,003	408,503	326,000	784,003
	Northeast	326,000	46	148,103	506,153	226,000	745,828
	Other	276,000	36	89,378	345,753	100,000	473,303
$5.1bn–$20bn	West Coast	326,000	36	90,403	404,678	163,000	610,876
	Northeast	376,000	46	208,403	610,428	276,000	880,978
	Other	326,000	46	152,903	473,603	226,000	731,653
More than $20bn	West Coast	376,000	46	133,303	508,803	551,000	1,076,028
	Northeast	376,000	56	286,440	700,528	276,000	1,119,190
	Other	413,000	46	180,653	630,840	276,000	916,378

Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

Joining bonus and sign-on equity by geographic region (%)

Annual revenue		In cash	In equity
$5bn or less	West Coast	45,000	200,000
	Northeast	22,500	95,000
	Other	25,000	82,500
$5.1bn–$20bn	West Coast	37,500	105,000
	Northeast	85,000	250,000
	Other	50,500	150,000
More than $20bn	West Coast	100,000	350,000
	Northeast	250,000	250,000
	Other	60,000	225,000

Source: Heidrick & Struggles' North America chief information security officer (CISO) survey, 2020, n = 372 information security professionals

About the authors

Matt Aiello
is the leader of Heidrick & Struggles' Global Cybersecurity Practice and a member of the Global Technology & Services and Technology Officers practices; he is based in the San Francisco office.

maiello@heidrick.com

Scott Thompson
is a principal in the New York office and a member of the Financial Services and Technology Officers practices.

sthompson@heidrick.com

Specialty Practices

Heidrick & Struggles' Specialty Practices provide expertise on emerging technologies.

These practices include:

- Artificial Intelligence, Data, and Analytics
- Blockchain/Distributed Ledger Technology
- Cybersecurity
- Digital Innovation
- Internet of Things

Leader of Heidrick & Struggles' Specialty Practices

Global

Tim Luedke
Managing Partner
tluedke@heidrick.com

Technology Officers Practice

The world is currently experiencing a revolution. With technology constantly advancing, the contemporary business landscape is now defined by rapid innovation. Advances in cloud computing, artificial intelligence, machine learning, and the Internet of Things have enabled companies to become lean, agile, and efficient competitors in the global market. Indeed, the promise of a digital future has convinced organizations across all industry segments to adopt more technology-focused business strategies.

At Heidrick & Struggles, we believe that leadership plays an essential role in this transformation. That is why our Technology Officers Practice is committed to helping our clients find the next-generation technology talent necessary to take their organizations to the next level. Our executive search consultants bring unparalleled experience, having successfully placed more than 1,000 information and technology functional officers with some of the best-known and most-admired companies around the world.

Leader of Heidrick & Struggles' Technology Officers Practice

Global

Dennis Baden
Managing Partner
dbaden@heidrick.com

WE HELP OUR CLIENTS CHANGE THE WORLD, ONE LEADERSHIP TEAM AT A TIME®