Survey

The State of the "C" in CISO

Pete Lindstrom
Michael Versace

Christina Richmond

IDC OPINION

The position of chief information security officer (CISO) is a new one, when compared with other "chief titled" positions across industries. Though Steve Katz claimed the title (or at least the representative position) 20 years ago after a Russian hacker stole $10 million from Citibank in 1994, the level of authority, reporting hierarchies, and set of responsibilities vary significantly across industries and enterprises. To understand the current state of the CISO role in business today, IDC conducted a survey of 269 information security executives in conjunction with Tech Exec Networks, Inc. (T.E.N.) about the position of CISOs in their organizations. Key findings include:

- More than 65% of CISOs report directly to the CEO (15%) or are one-level removed from a direct reporting relationship (50%).
- Higher education and government/nonprofit companies lead the way with 33% and 32%, respectively, of CISOs reporting directly to the CEO.
- Manufacturing companies lag significantly behind others with 55% of CISOs reporting at three or four levels below the CEO. This is a level too low to provide any true level of authority.
- CISOs report that the attention given to the security problem has increased (average 3.98 on a scale of 1-5) and has had a positive effect on the organization (average 4.06 on a scale of 1-5). What's more, 65% of respondents scored either a 4 or a 5 in both categories.
- Regulatory compliance reigns supreme as the primary driver for senior management security investments and objectives, beating out both reactive incident-related and proactive risk-related drivers. The Snowden affair with its social consequences was largely an insignificant anomaly for business.
- Four in five CISOs have had to notify their senior management of a significant breach in their careers; 45% of CISOs have disagreed with their senior management's final determination on whether to disclose the details.
- 12% of CISOs believe they would be fired in case of a breach, though less than 1% actually have been fired and almost 5% have been promoted. 5% of CISOs would feel compelled to resign.

IN THIS STUDY

Methodology

This study discusses the nature of the chief information security officer's relationship and position at the executive level in his/her organizations.

In conjunction with T.E.N., a security executive networking firm, IDC surveyed 269 chief information security officers and other senior-level information security executives responsible for overseeing security efforts for major national and global corporations headquartered in the United States. Many responses were provided by executives attending T.E.N.'s ISE Program Series, which bring together security executives, industry visionaries, and solutions providers to discuss current information security and technology risk management issues and trends and are held in major cities across the United States and Canada (more information is available at **www.ten-inc.com**).

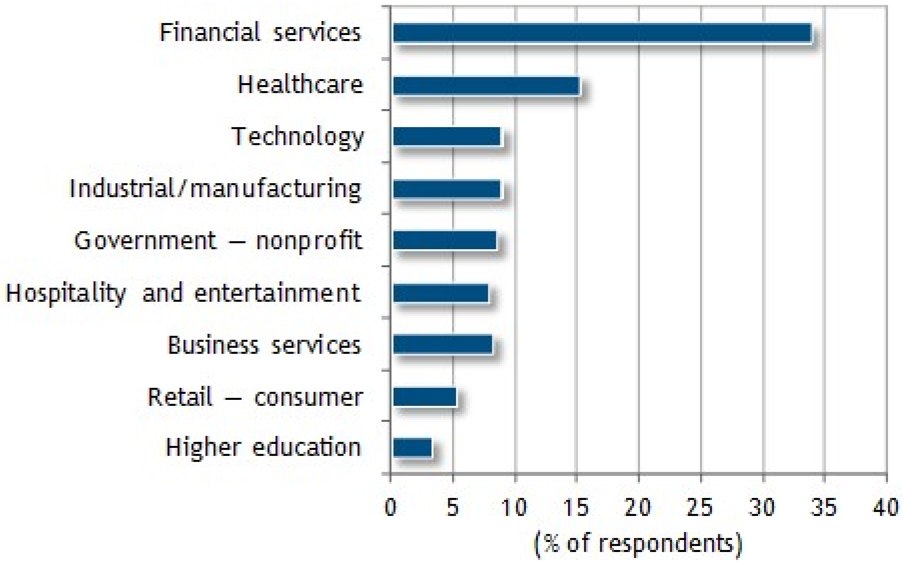
Note: All numbers in this document may not be exact due to rounding.

Respondent Profile

Figures 1-3 break out the survey respondents by industry, total revenue, and number of employees.

FIGURE 1

Respondents by Industry

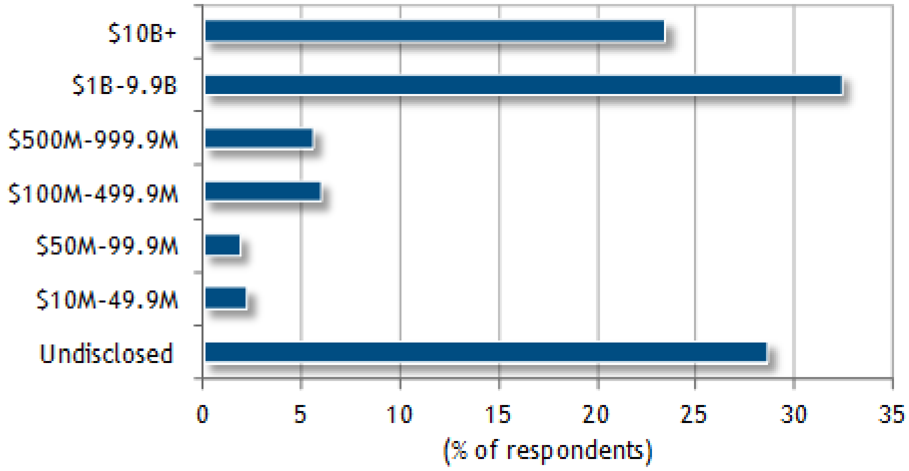


n = 269

Source: IDC's *State of the "C" in CISO Survey,* 2015

FIGURE 2

Respondents by Total Revenue

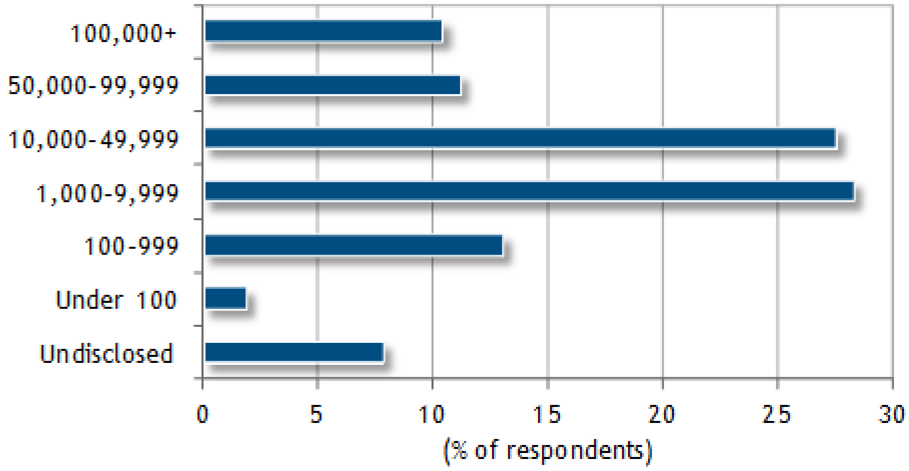


n = 269

Source: IDC's *State of the "C" in CISO Survey*, 2015

FIGURE 3

Respondents by Number of Employees



n = 269

Source: IDC's *State of the "C" in CISO Survey*, 2015

SITUATION OVERVIEW

The past few years has significantly increased the profile of the information security function with the senior executives and board members of companies.

What Is the CISO's Level of Authority?

Security professionals are quick to pay tribute to senior security executives by giving them the "CISO" title. But CISOs fit into organizations at various levels. Given corporate culture, a CISO who is at a higher level will likely have more clout than one at a lower level. We asked respondents to identify how many levels there are between their organization's CISO and the CEO (e.g., if the CISO directly reports to the CEO, he/she is at level 1).

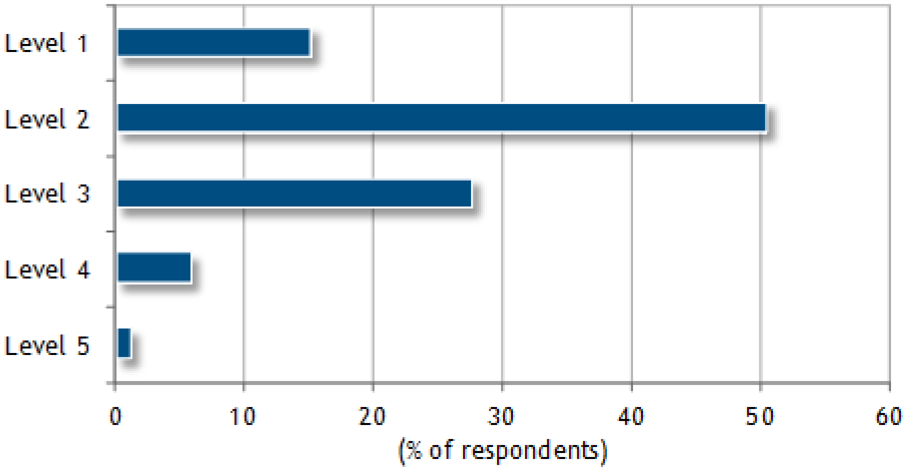
Figure 4 shows the distribution of CISO reporting levels within his/her organization. As illustrated, slightly more than 15% of senior security executives surveyed indicate that their organization's CISO reports directly to the CEO of the company. While not a significant number, anecdotal evidence from seasoned security professionals suggests it is growing, and IDC predicts this number will be 75% by 2018 (see *IDC FutureScape: Worldwide IT Security Products and Security Services 2015 Predictions — Moving Toward Security Integration,* IDC #253026, December 2014). When we include the further 50% of respondents who are only one-level deeper — something not completely uncommon for executives with a "C" in their title — it shows an increasing realization that the CISO position is an important one.

One confounding factor is that further analysis (not shown in Figure 4) shows that larger companies are much less likely to have a CISO with a direct reporting relationship to the CEO. Our belief is that this reflects a different kind of organizational hierarchy where CISOs are aligned with lines of business, and a broader operational risk perspective is more common.

While the movement to increased authority is promising, the fact that over one-third of respondents remain at three or more levels deep in the organization continues to highlight the disparity in what constitutes a "chief" and how much attention is being given to technology risk management.

FIGURE 4

Distribution of CISO Reporting Levels



n = 269

Note: Level 1 indicates reporting directly to CEO.

Source: IDC's *State of the "C" in CISO Survey*, 2015

Table 1 shows the reporting level breakdown by industry. Notably, government and higher education appear to be the most progressive in CISO authority levels. We believe this is for different reasons – regulatory attention in the former case and flatter reporting structures with frequent incidents in the latter.

TABLE 1

CISO Reporting Levels by Industry (% of Respondents)

	Reporting Level					
Industry	1	2	3	4	5	Total
Business services	14.3	47.6	28.6	4.8	4.8	100.0
Financial services	16.3	52.3	26.7	4.7	–	100.0
Government — nonprofit	31.8	45.5	18.2	4.5	–	100.0
Healthcare	5.4	62.2	24.3	8.1	–	100.0
Higher education	33.3	55.6	11.1	–	–	100.0
Hospitality and entertainment	14.3	42.9	33.3	4.8	4.8	100.0

TABLE 1

CISO Reporting Levels by Industry (% of Respondents)

	Reporting Level					
Industry	1	2	3	4	5	Total
Industrial/manufacturing	16.7	29.2	41.7	12.5	–	100.0
Retail — consumer	–	71.4	21.4	7.1	–	100.0
Technology	12.5	45.8	33.3	4.2	4.2	100.0
Total	15.1	50.4	27.5	5.8	1.2	100.0

n = 269

Source: IDC's *State of the "C" in CISO Survey,* 2015

Have CISO's Been Invited to the Table?

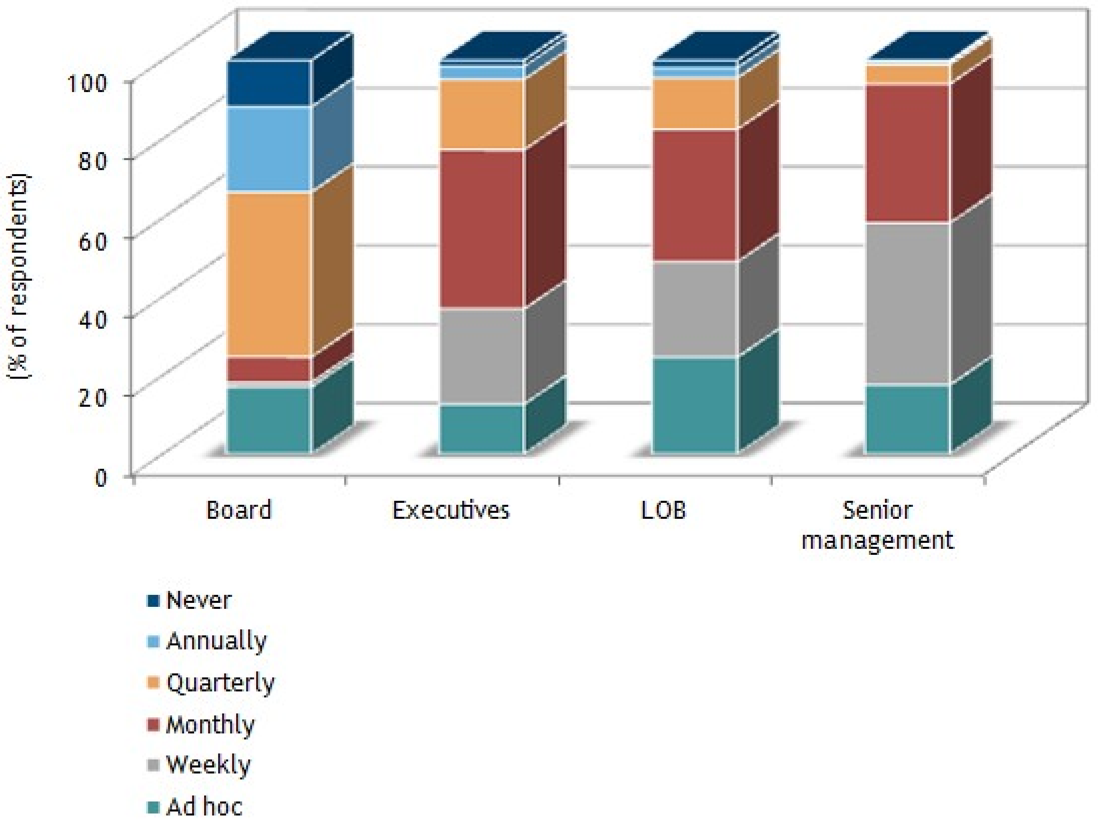
Though public relations professionals assert that all attention is positive attention, this may not be the case with information security. It is certainly possible that any interaction with the CISO is treated like a visit to the dentist – you go there because you have to but you'd rather be somewhere else. This forced negative interaction along with the fact that no legitimate CISO can answer the questions "what direct value or ROI comes from my information security investments" and "are we secure" affirmatively can easily create a challenging environment in which to operate.

IDC asked the group of CISOs and senior security executives about the frequency and nature of their interactions with their respective boards of directors, executive and senior management teams, and line-of-business leaders to understand just how up to date these groups are kept on information security matters. Further, we asked whether the increased attention over the past few years has had a positive or negative effect for information security within their organizations.

We found that a full 42% of CISOs were, in fact, reporting to their company's board of directors on a quarterly basis. This level of interaction provides the open lines of communication necessary to ensure that an organization understands its security capabilities and value delivered at the highest level. On the other hand, there are still 12% of organizations in which the CISO has never addressed its board. While the message could be carried forward by others, the nuances associated with information security management would surely be lost (see Figure 5).

FIGURE 5

Distribution of Reporting Frequency for Management Levels



n = 269

Source: IDC's *State of the "C" in CISO Survey*, 2015

In addition to identifying the reporting frequency, we were particularly interested in whether it has changed recently. We asked respondents to assess how the frequency level has changed and whether that impact has been positive or negative.

It is heartening to see that about 62% of senior security executives surveyed believe that the frequency of communications has increased (4 or 5) and the impact has been positive (4 or 5). Another 11% of CISOs responded that the impact was positive though the frequency did not change (or in a couple of cases was reduced). Overall, this is a positive finding, under the assumption that it leads to understanding and action (see Table 2).

TABLE 2

Comparison of Frequency and Effect Scores (% of Respondents)

	Less/More Frequency				
Negative/Positive Change	1	2	3	4	5
1	1.2	–	–	–	–
2	–	1.6	0.4	0.8	0.4
3	–	0.8	11.3	5.1	3.9
4	–	1.2	8.6	24.2	11.3
5	–	–	2.0	4.3	23.0

n = 269

Source: IDC's *State of the "C" in CISO Survey,* 2015

How Strategic Is the Executive Team in Information Security Management?

Attention to breaches and security tends to come in waves, but attacks, breaches, and compromises have been around as long as computers have been communicating. The mature organizations will see through the media hype and maintain a strategic, proactive approach to information security management. For some organizations, a reactive, incident-driven approach is the norm.

To determine whether organizations are more proactive and strategic versus reactive and opportunistic, IDC asked CISOs to assess the level of attention given to strategic drivers (proactive and strategic) compared with a recent set of security events (reactive and tactical).

Table 3 tells the story – compliance reigns supreme in the minds of senior management. While this is not unexpected, the focus on compliance as the sole, strategic goal of information security management clouds judgment when attempting to reduce information security risk and incidents in the enterprise – as reflected by the fact that the other more strategic objectives – key risk indicators and line-of-business security postures were a lower priority. Business growth, improved customer convenience, and product/service margin improvement were not even mentioned as strategic objectives of information security management. The focus on compliance also illustrates concerns over a different kind of loss – the potential for regulatory fines and legal action that comes from many high-profile breaches. This focus seems disproportionate with the direct losses that can accrue from the breaches themselves.

While it is clear that the Snowden affair was an anomaly that received much attention in sociopolitical world, it had very little impact on companies. Aside from compliance, media attention does appear to drive the focus of executive attention. Tactical responses to breaches and vulnerabilities are still given high priority in enterprises, demonstrating a reactive approach to security. This needs to change.

TABLE 3

Key Security Drivers

	Average Score
Regulatory compliance	4.15
Heartbleed vulnerability/exploit	3.99
Shellshock vulnerability/exploit	3.84
Target breach	3.70
Strategic KRIs	3.66
LOB security postures	3.35
Snowden affair	2.42
n =	269

Source: IDC's *State of the "C" in CISO Survey*, 2015

How Often Do CISOs Face a Breach Disclosure Decision? Who Makes It?

Breaches seem to be a fact of life for any organization and, by extension, the CISO. Some may see it as a rite of passage. But there is more fairy tale than fact in the newer meme that "there are two kinds of companies – those that have been breached and those that don't know it yet." While including a garden variety malware infection may lend credibility to this statement, in practice most organizations think of breaches in terms of only those incidents that require disclosure. So in our mind that begged the question – How many CISOs have actually had to notify management of a serious breach, requiring disclosure or not?

Table 4 shows the results to the question, "In your career, have you ever had to notify senior management of a breach/incident?" It turns out that just about four out of five CISOs have had the displeasure. While the results vary a bit by industry, one shouldn't read too much into the results since the question on the survey related to the CISO's career while the industry was identified based on his/her current job.

TABLE 4

Breach Notification Frequency by Industry (% of Respondents)

Q. Have you ever had to notify senior management of a breach?

	No	Yes

TABLE 4

Breach Notification Frequency by Industry (% of Respondents)

Q. Have you ever had to notify senior management of a breach?

	No	Yes
Business services	18.2	81.8
Financial services	23.3	76.7
Government — nonprofit	17.4	82.6
Healthcare	17.5	82.5
Higher education	22.2	77.8
Hospitality and entertainment	28.6	71.4
Industrial/manufacturing	25.0	75.0
Retail — consumer	28.6	71.4
Technology	20.8	79.2
Total	22.1	77.9

n = 269

Source: IDC's *State of the "C" in CISO Survey,* 2015

Given the reluctance of organizations to disclose breaches (and yes, we do assume that as a given) and the complexity of the issues involved, disagreement in the need to disclose is a reasonable expectation. These disagreements are sometimes used to illustrate some sort of "smoking gun" that a breached organization (the victim) is willfully breaking the rules and that aforementioned complexity is a much more likely reason.

As a follow-on question, we asked, "In your career, have you disagreed with superiors about disclosure requirement?" The responses were split, as illustrated in Table 5.

The intention here was to illustrate a difference in belief, and perhaps risk tolerance, between a CISO and his/her senior management. With 45% of CISOs reporting a disagreement, the misalignment seems obvious, though manufacturing and higher education have a much stronger alignment with only one in three reporting disagreement.

We believe this split highlights a significant problem in our field – that either CISOs don't have a similar level of risk tolerance or their advice is not valued much higher than a flip of the coin.

TABLE 5

Breach Disclosure Disagreement by Industry (% of Respondents)

Q. Have you ever disagreed with senior management about the need to disclose a breach?

	No	Yes
Business services	59.1	40.9
Financial services	61.5	38.5
Government — nonprofit	39.1	60.9
Healthcare	41.5	58.5
Higher education	66.7	33.3
Hospitality and entertainment	61.9	38.1
Industrial/manufacturing	66.7	33.3
Retail — consumer	50.0	50.0
Technology	50.0	50.0
Total	55.4	44.6

n = 269

Source: IDC's *State of the "C" in CISO Survey,* 2015

Should CISOs Lose Sleep at Night?

On an individual career level, it seems CISOs are on the firing line for any breach even though it is common knowledge that complete protection is impossible, especially with the human element so heavily involved in breaches. IDC aimed to dig a bit deeper into the reality of this scenario. We asked two questions – first, whether they had ever experienced any of the outcomes listed in Table 6 due to a breach; and second, what their anticipated outcome is should their current organization experience a breach.

As shown in Table 6, the actual past outcomes associated with the group differ significantly from anticipated future outcomes. A significantly higher number of CISOs believe they will be fired due to a breach that has actually happened in the past. In fact, only a single respondent reported having been fired due to a breach. Meanwhile, over 12% believe they would be fired from their current position. This dissonance becomes even more interesting when factoring in the earlier suggestion that attention being given by the board is of the positive variety.

TABLE 6

CISO Career Outcomes: Actual Versus Anticipated (% of Respondents)

Q. What happened after a (prior) breach? What would happen after a (future) breach?

	After Breach	Anticipated Future
Fired	0.4	12.2
Demoted	1.5	1.5
Promoted	4.9	0.8
Resigned	0.4	4.9
No change	61.9	70.7
NA	31.0	9.9

n = 269

Source: IDC's *State of the "C" in CISO Survey,* 2015

If we add the almost 5% of respondents that would "fall on their swords" and resign in the face of a breach, that's 17% of respondents who expect to be out of a job because of a breach — an unhealthy situation.

Finally, it is interesting to see that 5% of respondents actually benefited from a breach and earned a promotion. It is unclear whether this means there are others waiting in the wings to capitalize on breaches or public pressure for companies to have a higher-level CISO is having an effect.

FUTURE OUTLOOK

By and large, organizations are getting the message that information security is an important part of their ability to operate in the future. The onset of 3rd Platform technologies (cloud, mobile, social, and Big Data) creates significant opportunities for businesses but are not without a downside that is increasing as well. Organizations that factor information security into their strategic plans and demonstrate leadership in this arena are more likely to weather disruptions associated with breaches.

ESSENTIAL GUIDANCE

For enterprise security professionals:

- **Focus on business value.** Boards and executive management speak in terms of business value. CISOs need to understand this language and provide insight and recommendations in these terms. Expect to discuss impact on employee productivity, manufacturing timelines, supply chain management, financial reporting, and go-to-market plans, for example.

- **Operate in terms of security; advise in terms of risk.** CISOs must recognize and address the technical reality of attacks and compromises on a day-to-day basis, but they must learn to think and act strategically in terms of probability and impact.
- **Represent the security profession internally.** Businesses need to understand consistent, strategic viewpoint on managing information risk. Often, security professionals get frustrated about how executives act when the reality is that we need to understand and embrace their viewpoint.
- **Execute on the vision.** The focus of this survey is how CISOs are gaining attention within organizations. To continue moving the dial and building on the positive indicators is by building a security program with efficiency and effectiveness.

LEARN MORE

Related Research

- *Sony Breach Postmortem* (IDC #254190, February 2015)
- Shift to Predictive: Results of 2014 Cyber-Analytics Survey (IDC #FI252653, December 2014)
- Addressing Technology Risk in the Face of Compliance Needs (IDC #249635, June 2014)

Synopsis

This IDC study discusses the nature of the chief information security officer's relationship and position at the executive level in his/her organizations.

By business standards, the position of chief information security officer (CISO) is a new one. Though Steve Katz claimed the title (or at least the representative position) 20 years ago after a Russian hacker stole $10 million from Citibank in 1994, the level of authority and set of responsibilities can vary significantly across enterprises. IDC conducted a survey of 269 information security executives in conjunction with Tech Exec Networks about their position in their organizations.

The results of the survey were mostly promising. CISOs claim a certain amount of growing authority and level of increased interest in their organizations. The changes happening to organizations have been mostly positive. There are a few outlier situations that must be addressed.

"Whether the 'C' in CISO is truly appropriate or just hand waving at a problem depends on the level of authority the CISO has in an organization and his/her interaction with executives," said Pete Lindstrom, research director, Security Products. "Because breaches often come full of 'stick' with very little 'carrot,' there can also be a backlash against security professionals. Luckily, this hasn't happened, and it appears that organizations are finally giving security and the attention they deserve."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice