Behind the Scenes of the CIO & CSO Relationship:

Productive Partnership or Competitive Alliance?

IDG Enterprise
An IDG Communications Company

CIO COMPUTERWORLD CSO InfoWorld ITWORLD NETWORKWORLD

Security has rocketed to the top of the enterprise agenda in recent years, as Boards of Directors, C-level executives, line of business leaders, and shareholders recognize the increasingly–and seemingly inevitable–risks to the organization.

That's raising the profile of both CIOs (Chief Information Officer) and their executive-level brethren in security, whether they're called CSO (Chief Security Officer), CISO (Chief Information Security Officer), or another title altogether–for better or for worse. Each brings some unique expertise and capability to the table. Despite the high demand for experienced security leaders, those IT and security executives that can make a case for needed security investment and prove to their constituents that they are managing security effectively will surely see their stars rise. But those who fail to do so could be marginalized and shown the door.

This first CIO/CSO Partnership Survey, conducted by IDG Enterprise, reveals that CIOs and CSOs are indeed working closely together, often on a daily or weekly basis and strategizing regularly to discuss the issues at the intersection of security and technology, including existing and emerging risks compliance, and audit issues. Both groups of executives are actively educating and advising their boards and business leaders on security issues, each bringing different expertise and information to the table. But each sees the security topic through his or her own lens, sometimes disagreeing on where collaboration is most beneficial.

Organizational issues are also still evolving. While CIOs are sold on the value of the CSO or CISO role, not all of them have one. And while it's relatively split to whether IT and security functions should be separate, the majority of security executives still report in, either directly or through a dotted-line, to the CIO.

CIOs and CSOs: Working Together, But Not Always Seeing Eye to Eye

CIOs and CSOs are certainly not strangers anymore. There is a relatively high level of collaboration between top IT and security executives. More than a third (38%) of CIOs said they meet with their CSO or CISO on a daily basis and 65% reported interacting at least once a week. Likewise, 42% of CSOs/CISOs said they work with their IT counterparts weekly, while 36% reported collaborating each and every day.

Around half of CIOs (52%) have a formal strategy session with their organization's top security executive at least once a month to discuss security concerns, review technology initiatives, or go over other cybersecurity-related issues, while 23% did so at least weekly and 70% said it happens at least quarterly. Around two-thirds of top security executives (65%) said they have a formal strategy session with the CIO at least once a month, 32% strategize at least weekly, and 86% said they have such sessions with IT quarterly.

valuable to work closely with their security peers to review new regulations and compliance issues that the business may be subject to, an area which only 46% of CSOs/CISOs agreed. Conversely, 65% of top security leaders think it's a good idea to work with the CIO on enabling innovation, making it third on their list of areas ripe for collaboration, while it was a lower priority for CIOs at 52%, presumably due to the competition for resources and power these two groups share within their enterprise.

FIGURE 1: CIOs AND CSOs JOIN FORCES

What are the top issues on which CIOs and CSOs collaborate?	**CIO answer**	**CSO answer**
Audit issues and findings	**84%**	**89%**
Mitigating existing risks	**78%**	**91%**
Mitigating emerging risks	**77%**	**81%**
Compliance issues	**76%**	**83%**
Building security into new technology solutions	**73%**	**75%**

CIOs and CSOs/CISOs agree about the top issues on which they collaborate: audit issues and findings, mitigating existing and emerging risks, compliance issues and building security into new technology solutions. (See Figure 1.)

A significant number of CSOs and CISOs also reported collaborating with the CIO on third-party risks – those outside organizations with whom their business collaborates (73% of security executives versus 55% of CIOs), questions from the Board (72% versus 51%), technology vendor management (62% versus 48%), staffing (49% versus 37%), and discussions about security responsibility (49% versus 37%).

More than three-quarters of both top IT and security executives agree that it would be helpful to sit across the table from each other and address security risks in the adoption of new technologies such as cloud computing, mobile solutions, social media and big data and analytics. And just about half of each group said the two teams should collaborate on dealing with shadow IT.

Beyond that, however, was some disagreement. (See Figure 2.) More than three-quarters (78%) of CIOs said it would be

FIGURE 2: THE POWER OF TWO

In what areas would it be helpful for CIOs and CSO to collaborate?

CIOs	
Addressing security risks inherent in the adoption of new technologies	**78%**
Reviewing new regulations and compliance issues	**78%**
Understanding/managing the expectations of the Board	**68%**
Understanding/managing the expectations of senior management	**60%**
Enabling innovation	**52%**
Managing Shadow IT	**51%**
CSOs	
Addressing security risks inherent in the adoption of new technologies	**76%**
Understanding/managing the expectations of senior management	**68%**
Enabling innovation	**65%**
Understanding/managing the expectations of the Board	**55%**
Resource planning	**52%**
Managing Shadow IT	**48%**

Lines in the Sand

CIOs strongly believe that the enterprise needs CSOs or CISOs in order elevate the importance of, or focus on, security, but that is not always the case. Specifically, more than three-quarters of the IT executives believe this to be true, yet only half of them actually have a CSO, CISO, or top security executive. (See Figure 3.)

FIGURE 3: CSOs WANTED

In many organizations the CIO would prefer that the CSO, CISO or security executive be part of a separate organization outside of IT; more than half (52%) feel that the IT and security functions should be separate. In some cases, this is due to the fact that the security function's scope extends beyond IT alone. Perhaps even more importantly, many who feel the functions should be separate want to prevent conflicts of interest. As one CIO said of the security role: "You cannot be a player and the referee at the same time".

However, 83% of CIOs whose organizations have a security executive report some sort of reporting relationship between security and IT; more than half (57%) have the CSO/CISO reporting directly to them, 13% say the top security executive has a dotted line relationship with them, and another 13% say the top security executive reports to IT but not the CIO. More than half of the top security executives surveyed (53%) said they reported directly to the CIO, and 17% indicated they have a dotted line relationship to the CIO.

Addressing Security Early and Often

So what security issues keep security executives up at night when it comes to IT? More than a quarter (27%) said the biggest risk emanating to the enterprise from their IT department was that they will misconfigure existing technologies and expose the business to undue risks. Another 24% are concerned that IT could also ignore security issues when adopting or implementing new solutions, and 23% complained that IT did not spend enough money on information security.

Indeed, when asked what their CSOs might say is the single greatest security problem in IT, CIOs thought security counterparts would say it's the fact that security decisions are made after business decisions (36%) followed by the idea that IT is more concerned with speed of delivery and efficiency for new hardware, software and applications than security (27%). For their part, CIOs report that security concerns are actually most likely to be addressed in the earliest technically-oriented phases of a project (such as requirements gathering and product evaluation), with those discussions and related actions occurring less frequently in strategy phases (like determining the business need or selling the system to the business) and in latter periods of the system's lifecycle. (See Figure 4.)

FIGURE 4: TALKING SECURITY

Security Concerns are Discussed and Tested When...

Determining the business need	61%
Determining technical requirements	81%
Evaluating products or services	80%
Recommending or selecting vendors	62%
Selling internally	29%
Authorizing or approving the purchase	46%
Post implementation	54%
Upgrading or refining	54%

However, when CIOs are considering less proven solutions, security gets more attention. Seven out of ten IT leaders said the process changes when implementing emerging technology projects in the areas of cloud computing, the Internet of Things, or advanced analytics, for example.

Security at the Speed of Business

For their part, CSOs didn't agree on what IT might think is the biggest problem with the security organization: 14% said it was that security gets in the way of the business, 11% percent cited the addition of unnecessary costs to IT projects and 10% said that security is always blocking innovations. In their large pool of verbatim replies, CSOs often pointed to problems associated with resource scarcity in security organizations (from funding to talent to tools).

Both CIOs and CSOs/CISOs fret over the likelihood that line of business executives will charge ahead with their own solutions (say, a cloud computing contract or an outsourcing deal) ignoring the potential security ramifications. More than a quarter (28%) of IT leaders said the biggest risk from their line of business colleagues was ultimately shadow IT. They fear that their LOB colleagues will adopt or implement new technologies or services that create undue risks and 29% of CSOs or CISOs agree. Close behind is the concern over users who are uneducated in, or ignore, good security practices (24% of CIOs and 26% of CSOs/CISOs say that's the second biggest point of exposure created by the business). Nearly a quarter (24%) said their biggest concern is the issue of the business working with other entities (businesses or customers) that have poor security practices and thus expose their business to undue risks.

> **"If you asked CSO's two years ago about their relationship with the Board, their responses would have been something along the lines of 'I get a half a slide once a year, and the CIO presents it to the Board without me there. The CIO controls the message.' Today you see a more involved response such as, 'I have 45 minutes scheduled with the Board each quarter and the CIO is not in attendance. That 45 minutes typically turns into two hours'."**
>
> BOB BRAGDON
> VP/PUBLISHER, CSO

Security Risks Top of Mind in the Board Room and Beyond

It's little surprise that corporate boards are finally paying attention to security issues. And the majority of CIOs are keeping their Board of Directors informed on the cybersecurity state of affairs, not simply to educate them about the issues they should focus on as they oversee related initiatives but to garner support for the systems, processes, and policies necessary to protect the enterprise today. Sixty-two percent of CIOs deliver a security report to their Board of Directors at least once a quarter, 24% of them keep their directors updated on a monthly basis and nearly one in ten (9%) provide security intelligence on a weekly basis.

Once simply a necessary evil, cybersecurity has risen to the top of the agenda as breaches and compromises have hit the front page. In 2015, 38% more security incidents were detected than in 2014, according to the 2016 Global State of Information Security study. The average size of the financial hits attributed to those incidents was $2.5 million, with 8% of enterprise organizations reporting an estimated loss of more than $20 million. And those are simply the compromises that were detected and reported.

CIOs were more likely to work with line of business leaders on audit issues and findings, while CSOs and CISOs were more likely to partner with line of business executives to discuss third-party risk exposure from business partners and customers.

Line of business leaders are turning to their CIOs and CSOs or CISOs for security information and guidance as well. Both CIOs and their security counterparts say they collaborate with or advise line of business executives on mitigating existing and emerging risks, and compliance issues. (See Figure 5.)

FIGURE 5: CIOs AND CSOs SPLIT SECURITY ADVISORY DUTIES

CIOs Advise the Business On . . .	
Audit issues and findings	80%
Mitigating existing risks	79%
Compliance issues	76%
Mitigating emerging risks	72%
Building security into new technology solutions being adopted	63%
CSOs Advise the Business On . . .	
Mitigating existing risks	76%
Compliance issues	74%
Audit issues and findings	73%
Third-party risks (business partners, customers, etc.)	72%
To address questions from corporate leadership	70%

More than three-quarters (81%) of CSOs/CISOs collaborate with or advise line of business executives at least once a month and nearly half of them (48%) are meeting with them at least weekly to discuss security-related concerns.

Proactively addressing security issues with boards and business leaders is critical, because once exposure occurs it's too late. In fact, CIOs report that on the day after a breach occurs, the most common response is increased scrutiny, both of the IT organization and the security department. And what's less likely to happen is an increase in security budget. (See Figure 6.)

CIOs and CSOs are beginning to collaborate on security tactics and strategy and bring their knowledge together when partnering with business leaders and Board of Directors. But clearly, the two parties will need to outline how the responsibility for, authority over, and organization around security management and mitigation is split between their two organizations. Security breaches are now core risks to the enterprise, and they're not likely to fall off the corporate agenda anytime soon.

FIGURE 6: THE MORNING AFTER (ACCORDING TO CIOs)

What happens the day after a security breach?

More scrutiny towards the IT department	57%
More scrutiny towards the security department	50%
More meetings	48%
More training for all employees	33%
More consulting	27%
More funding	17%
Nothing at all	13%

Future of the CIO and CSO Roles

So where is the relationship between the CIO and the CSO headed? That's a great question and something that's been pondered intensely for the past 13 years. As with many questions, the answer is – it depends. Ultimately organizations are moving to a more collaborative, peer relationship as businesses come to terms with not just the benefits that technology can deliver, but also the risks that those technologies expose the business to. Organizations have watched a marked shift in separation of duties over the past decade as responsibilities of patch management, provisioning, monitoring, etc. moved into the realm of network and IT operations, while core security elements (strategy, forensics & investigations, network security, identity management, advanced detection, third party risk mitigation, etc.) remained a part of the core security team. During this same time, many senior level CSOs architected reporting structures that moved them out from under the CIO with more direct reporting to the CEO, Board of Directors or General Counsel. Some industries, like financial services, held strong to the original reporting model of CSO to CIO as it was a tried and true model that had worked for many years.

But that structure continues to fly in the face of the need for a strict separation of duties. As noted earlier in this paper, one CIO put it to us, "You cannot be a player and the referee at the same time." Just recently the FFIEC, a major regulatory body governing the financial services industry, updated their guidance that had, previously, suggested that information security officers should not report into the CIO. With its most recent update, that guidance is now a requirement. In the words of the FFIEC, "To ensure appropriate segregation of duties, the information security officers should report directly to the board or to senior management and have sufficient independence to perform their assigned tasks." As this mandate percolates throughout the financial services sector it will naturally migrate into others as well.

ABOUT OUR SURVEY

The CIO/CSO Partnership study uses quantitative research to examine the relationship between the CIO and CSO roles and gain insight into their competing and common interests, as well as involvement in emerging technologies and collaboration. Both the CIO and CSO versions of the survey were conducted online via. The CIO survey results are based off of 178 responses, and the CSO survey results are based off of 101 responses.

Examining the Marketplace

We think research is invaluable in helping to connect marketers with customers and prospects. Our research portfolio explores our audiences' perspectives and challenges around specific technologies, examines the changing roles within the IT purchase process, and arms IT marketers with the information they need to identify opportunities. **To review the presentation of full results from any of these studies, contact your IDG Enterprise sales executive or Sue Yanovitch, VP, Marketing for IDG Enterprise at syanovitch@idgenterprise.com**.

BUYING PROCESS

Each year we take a deep dive into the enterprise IT purchase process to learn more about who is involved and who influences decision-making, what sources purchasers rely on to keep up to date with technology–and throughout the purchase process–and how they feel about the vendors they're working with.

- Role & Influence of the Technology Decision-Maker
- Customer Engagement

TECHNOLOGY INSIGHTS

Each year we explore the technologies that are top of mind among our audiences to understand the business challenges, drivers, and adoption within the enterprise. Each research study is designed to help IT marketers understand what their customers are focused on and where the market is moving.

Role & Priority Studies

- CIO Tech Poll: Economic Outlook
- CIO Tech Poll: Tech Priorities
- CIO/CSO Partnership Survey
- Computerworld Forecast Study
- Enterprise Architect Persona
- Global Information Security Survey
- State of Cybercrime
- State of the CIO
- State of the Network

Technology Specific Studies

- Big Data & Analytics Survey
- Cloud Computing Survey
- Security Vendor Scorecards

ADDITIONAL WAYS TO STAY ON TOP OF INFORMATION FROM IDG ENTERPRISE:

- Sign-up for IDG Enterprise's monthly MarketingFit newsletter and receive our proprietary research, product and event information, and relevant content from across IDG Enterprise brands direct to your inbox. Go to **www.idgenterprise.com/newsletter**
- To get results from IDG Enterprise research when it happens, or any other news, follow us on Twitter: **@IDGEnterprise**
- Visit us on LinkedIn for research, services and events announcements: **linkedin.com/company/idg-enterprise**