C-SUITE PLAYERS: WHO ARE THEY?

Information security has only recently been elevated to the C-Suite, and many CISOs are new to the role with an average of almost two years experience. Understandably, many CISOs are still carving out their role in relation to the C-suite and still working to establish relationships with other business leaders.

CISOs are in a unique position. They are one of the few executives whose programs require collaboration and partnership with every other department in the organization because data protection and security initiatives impact people, process, and technology across the whole company. That means, more than any other C-level executive, CISOs must understand the motives and priorities of every other department. To establish the strongest working relationship with their peers, CISOs must understand how each leader thinks about information security.

Chief Executive Officer

2016 Priorities: Growth and digital innovation

Security Check: 44% of US CEOs are extremely concerned about cyber security in 2016 (PWC 2016 US CEO Survey)

In their words: "As technology transforms our company, the risk of intrusion and cybersecurity worries us the most. Now, we've spent serious amounts of money on this, but the reality is you're never done. As much as we used to think about protecting our physical assets, it's the same today with our non-physical assets. They're in the hands of different people, and it's sometimes harder to figure out."
- Brian Moynihan, CEO of Bank of America Corporation quoted in PWC 2016 US CEO survey

Chief Marketing Officer

2016 Priorities: Data driven marketing

Security Check: CMOs top concerns are brand loyalty and consumer confidence after a breach

In their words: "As you might imagine, data security and privacy are extremely important to this company and we've learned a couple of things along the way. There's a simple question that we ask that can guide people really easily, which is, "Are we doing something for our guest or to our guest?" And if we're doing something for our guests it implies that there's a value exchange: In return for information we are giving them something of value. Obviously it's far more complex than that. It means you must have really clear privacy policies, be transparent about opt-in/opt-out and build better preference centers. All those things are super important, but it starts with a pretty simple question."
- Jeff Jones, CMO of Target quoted in Forbes.com

Chief Financial Officer

2016 Priorities: Margin and earnings performance

Security Check: Cyber security risks are the second highest priority for CFOs

In their words: "When you talk about the finance function being involved in IT and information security, it is usually to put in place process, standards and structure related to how data is used and accessed. I don't know a CFO who wants to own the security function. CFOs interact across all departments and can play an impactful role in incorporating security throughout the organization."
- Nick Araco, President of the CFO Alliance

Chief Information Officer

2016 Priorities: Managing the digital transformation

Security Check: Security & privacy are the number two priorities for CIOs (SIM 2016 CIO survey)

In their words: "One thing I'm seeing is that in some companies, when they think about security they see it as a compliance and risk exercise, and I get that there is a place for security there. But, we are doing security wrong and doing it a disservice [when we limit it to risk and compliance] because security should actually be an enabler, customer experience enhancer, revenue enhancer. I would offer that perhaps security should report to the COO or Chief Strategy Officer."
- Theresa Payton, former CIO of the White House (excerpt from Theresa's Profiles in Confidence)

Chief Technology Officer

2016 Priorities: Secure development

Security Check: Cybersecurity risks are the second highest priority for CFOs

In their words: "Building value through technology today requires technical and business knowledge as it always has, but understanding and aligning each system with an effective security program early in the life of that system is now critical as the risks are higher than ever," said Bill Murphy, Blackstone's Chief Technology Officer. "Development and security partnering early on produces better and cheaper solutions. Bolting security on at the end never works as well and usually costs a lot more."
- Bill Murphy, CTO of Blackstone

Chief Legal Officer/General Counsel

2016 Priorities: Ethics, compliance, regulatory issues/challenges

Security Check: 59% of CLOS rated data breaches "very" or "extremely important" in 2016 (ACC CLO Survey 2016)

In their words: "Whether the CISO reports to the CCO or CLO there should be a direct report to in-house legal counsel in the event of a data breach. Short of that, the CLO should be kept apprised of changes in security systems and protocols, since those directly concern questions regarding compliance and legal liability."
- Christopher Hart, Attorney at Foley Hoag