Leadership struggles to fully understand the role of the CISO

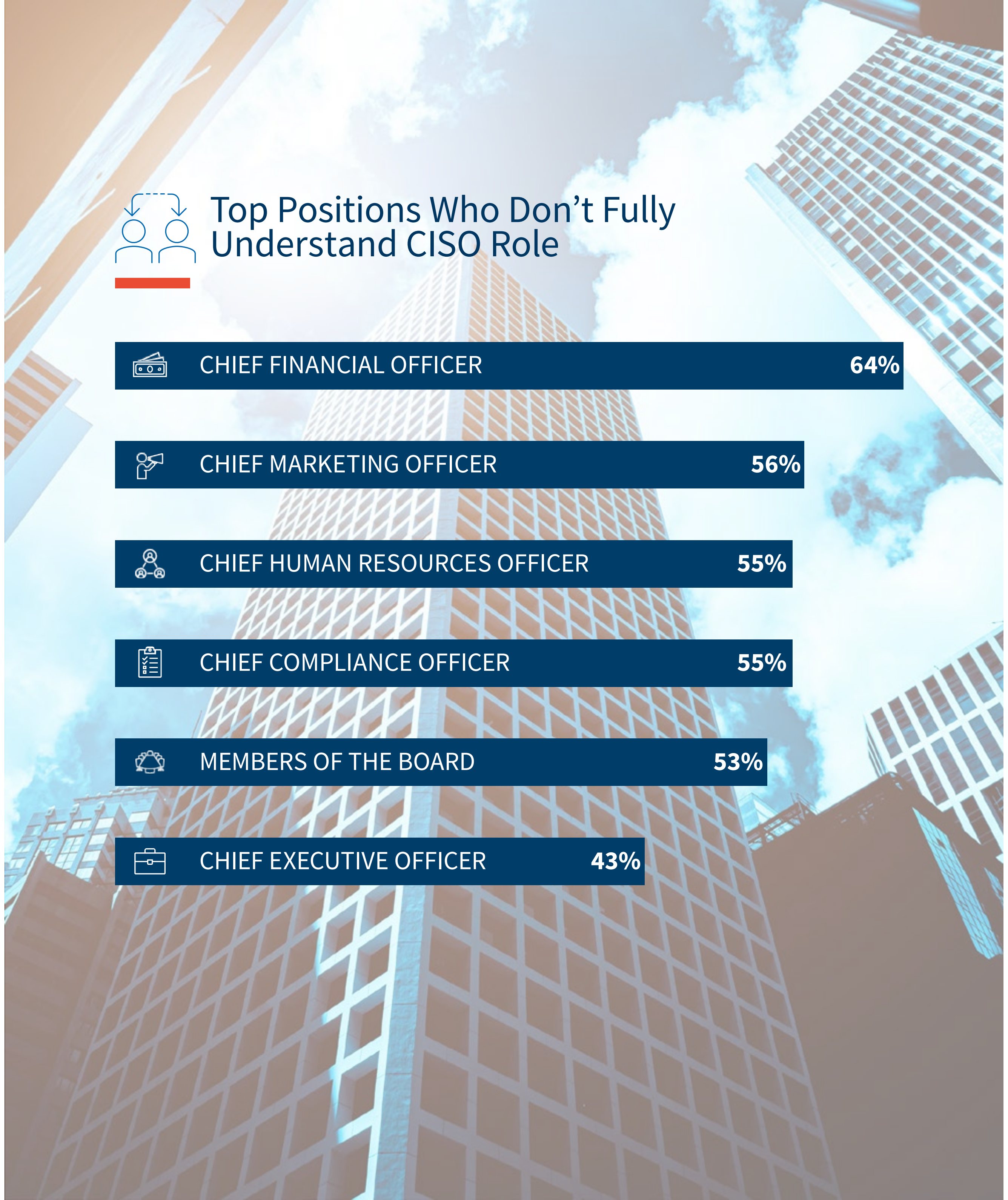
When diving deeper into this potential communications gap, the perception of those surveyed is that many in senior roles do not fully understand the CISO role.

This disconnect is seen most strongly among Chief Financial Officers (CFOs), of whom 64% of respondents believe do not fully understand their role as CISO.

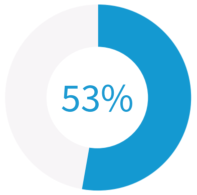
This is a particular concern considering many CFOs are directly in charge of the designation of cybersecurity budgets, and if they do not understand to what they are allocating financial resources, it could be allocated elsewhere in the business. This underscores the importance of CISOs to better communicate their role and their operational activity to this audience in particular.

The CISOs we surveyed clearly feel there was more of an endemic misunderstanding of their role across all levels of senior leadership. Perhaps surprisingly, a majority also believe those in the chief compliance officer role (55%) do no fully understand their role. Similarly, those in the chief marketing and chief human resources officer roles are perceived to struggle here. However, the Chief Executive Officer (CEO) is perceived to be the position most CISOs believe best understand their role, with 91% of respondents citing that the best way to help support them in their work is to report directly to the CEO.

That said, more needs to be done to communicate the role of the CISO effectively through company leadership structures to ensure alignment of information security and cybersecurity priorities. At the moment, over half of respondents (53%) do not believe these priorities are completely aligned with those of senior leadership.



Top Positions Who Don’t Fully Understand CISO Role



Say their information security and cybersecurity priorities are not completely aligned with those of senior leadership

> “
>
> Coordination at the executive level can take any incident response operation from good to great. In a cybersecurity incident, this need for top-level communication and organizational tactics is heightened because cyber is an extremely fast-moving and complicated environment. If CFOs and other executives do not have full clarity on the role of the CISO in managing risk, it can greatly impede a successful operational response.

JAMIE SINGER
Managing Director
Co-Head, Cybersecurity & Data Privacy Communications

With incidents on the rise, communication between CISOs and leadership is even more critical

Of those surveyed, an overwhelming majority (88%) experienced a cyber incident over the last 12 months, the most common types of attacks being malware, ransomware, and distributed denial of service (DDoS).

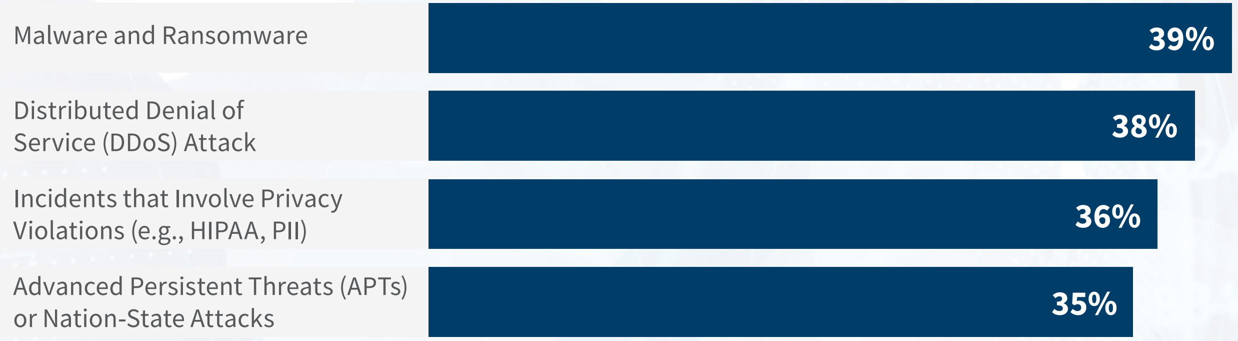
This reality has increased the pressure on CISOs to serve in a communications role.

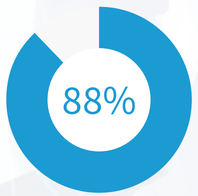
Ransomware and DDoS attacks in particular often need to be met with aggressive communications strategies, given the operational disruption commonly associated with these events.

More than any other cyber incident, ransomware most often places a communications burden on the CISO and information security (InfoSec) team. The fear that the malware may spread is extremely common – and customers, partners, suppliers, and other stakeholders may demand official assurances that there is no risk of contagion before resuming normal-course engagement with the victim organization.

With this overall rise in incidents, particularly in ones that require a fulsome communications response, it is critical for senior leadership and CISOs to coordinate closely and ensure their strategies – in terms of containment, remediation, restoration, and communications – are aligned and complementary.

Top Attacks/Incidents Experienced in the Last 12 Months





of organizations have experienced a cyber incident in the last 12 months

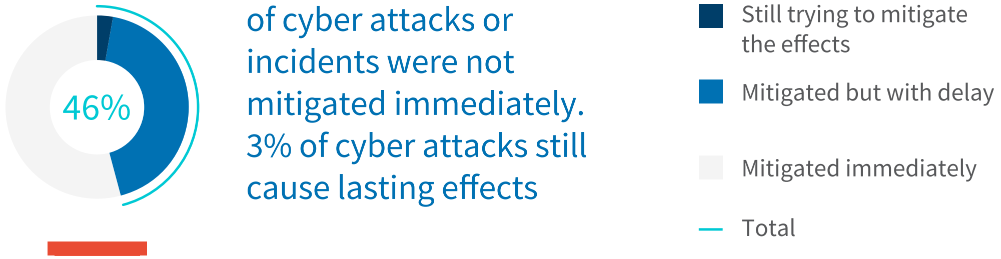
To best coordinate communications efforts in advance of an incident, organizations must have contingency plans in place to support their employees, investors, and customers and to offer accurate, timely responses to media interest. This means having the right resources and structures in place to support and inform key stakeholders. Poor communications or the lack of consistent communications during a crisis can create confusion and fear among stakeholders and lead to longer-term credibility issues. This can lead to dramatic consequences for a business, including loss in customers, loss in revenue, legal action, and lasting harm to an organization's reputation.

CISOs are challenged to manage communication with internal and external stakeholders in the face of an incident

Lack of preparedness can lead to a longer response time during an incident. For internal stakeholders, it creates fear and panic as they might feel that the company is hiding information or is not in the control of the situation. For external stakeholders, it gives them an opportunity to speculate and tell the story on behalf of the company if the company remains silent for too long. silent for too long. Instead, timely communications that reflect information the company is able to share, and in a transparent and supportive manner, can help mitigate reputational risks. This can occur simultaneous to the forensic investigation determining the cause and nature of the incident.

Almost half (46%) of the cyber attacks are not mitigated immediately in a number of situations because of roadblocks. Such challenges focused on managing communications between internal and external stakeholders account for more than half (52%) of those surveyed, responding to requests to complete security questionnaires (51%) and collaborating with multiple vendors during a crisis situation (47%).

After an incident, CISOs feel it's difficult for them to rebuild trust with key stakeholders, either internal or external. Those challenges can be mitigated with a strong communications strategy, including crisis communications preparedness and incident response communications skills for C-suite, including CISOs.



of cyber attacks or incidents were not mitigated immediately. 3% of cyber attacks still cause lasting effects

Top 3 Challenges when Responding to an Incident

1. Managing communications with internal and external stakeholders
2. Responding to requests to complete security questionnaire and/or share indicators of compromise (IOCs) with external parties
3. Collaborating with multiple vendors in a crisis situation

> "Time is money, especially when it comes to responding to cyber attacks. In the midst of the chaos, it is incredibly important to manage communications efficiently and effectively, as to maintain the confidence of key stakeholders. If that doesn't happen, trust will be lost which will be quickly followed by revenue.
>
> **MEREDITH GRIFFANTI**
> Senior Managing Director
> *Co-Head, Cybersecurity & Data Privacy Communications*