WHITE PAPER

Bridging the Gap: How Board-CISO Collaboration Strengthens Cybersecurity and Builds Customer Trust in Financial Services

The financial sector has taken a hit in recent years, with cyber-attacks ramping up in frequency and sophistication. This not only brings financial and operational damage, but as seen in a new report, damages public trust in financial organisations' ability to protect their data.

For Financial Services Cybersecurity is Non-negotiable

Gigamon commissioned the 'Bridging the Gap' general public study in October 2024, which surveyed 2000 Brits and revealed that the UK public is most concerned about their data being held by companies that interact with and rely on financial transactions, such as online shopping platforms (**40 percent**), followed by banking/financial service providers (**18 percent**), and entertainment providers (**14 percent**). Considering previous incidents such as the 2007-2008 financial crisis and the economic implications following the COVID-19 pandemic, an erosion of public trust is inevitable. In particular, the financial services sector still has a way to go to rebuild public trust surrounding levels of data security.

The survey findings attest to a greater level of expectation from the public in financial services to maintain strong levels of security, with 3 times the level of concern in the financial sector than that of data security within health organisations. These expectations are driven by the fact that the reliance on online payments is rapidly increasing, and that UK society and business depend on them. Almost two- thirds (**63 percent**) of those interviewed believe they would be impacted by the absence of electronic payments, with **7 percent** saying it would have a devastating impact. This implies that we are advancing

Payment systems are creaking because of their dependence on legacy systems and the complexity of securing and managing hybrid cloud infrastructure. Financial services need to able to monitor systems and rebalance the load in real time to keep up with traffic peaks.

BEN HUNTER
Director of Financial Services, Gigamon

towards a cashless society, placing huge responsibilities on financial services to secure and maintain online transaction systems and its data.

Customers Demand Cybersecurity Accountability

Our 'Bridging the Gap' report reveals that **60 percent** of the UK's public is demanding cybersecurity accountability, with **93 percent** concerned about the security of their data when business leaders are not held accountable. At the same time, security leaders are facing their own challenges internally. Despite bearing the responsibility of safeguarding their organisations, many CISOs lack the support they need from executive leadership, as **46 percent** of CISOs state in the Gigamon Hybrid Cloud Survey 2024 that they don't feel strongly prepared to identify threats across their networks. This dual pressure from the UK public and corporate boards within businesses highlights a critical need for better collaboration and alignment across top leadership. With **70 percent** of Brits calling for cybersecurity to be a shared responsibility between CISOs and executive leadership teams, the message is clear – **data protection is no longer just a technical challenge, but a core leadership issue that must be embedded into every decision the organization makes**.

CISOs and Their Boards Are Not Working Together

There is a clear disconnect when it comes to collaboration between CISOs and their boards. Accountability is increasingly being placed on CISOs and other security leaders, but without the support of the board, they're being held accountable for issues they cannot directly address. With 59 percent of those surveyed in the Gigamon Hybrid Cloud Survey 2024 identifying "cyber risk being a board priority" as a factor that would most empower them to face the threat landscape today, meaningful progress in cybersecurity requires a top-down commitment.

This gap at the top has a direct impact on the entire security strategy. Breaches are going undetected, as a staggering **53 percent** of CISOs admit to being alerted to breaches only after reports of inaccessibility from end users, and 1 in 3 stating they were unable to identify the root cause. The lack of collaboration between CISOs and their boards means that security initiatives are often misaligned with organisational priorities, and investments in proactive security are overlooked. As a result, financial services organisations are left reacting to incidents instead of proactively mitigating risks, leaving critical vulnerabilities unchecked. Ultimately, accountability must be shared. While CISOs are responsible for developing and executing security strategies, the board must also take ownership, as they control the key decisions that shape the organisation's overall security posture. Without board-level engagement and accountability, CISOs lack the influence and resources needed to embed robust security measures across the organisation, leaving significant gaps that threaten long-term resilience.

The Solution Lies in Gaining Granular Visibility

CISOs cannot take full accountability for security unless they are confident in the systems and processes that protect their organisations. **50 percent** of CISOs say that achieving this level of confidence requires complete visibility into all data in motion, including encrypted and lateral traffic across the network, spanning on-premises, virtual, and cloud environments. However, the reality is very different. With **7 in 10** CISOs claiming their existing security tools are not as effective at detecting breaches as they could be, optimisation is becoming critical, but it cannot be done without the support of the board.

50 percent of CISOs say they would feel more confident in the security of their networks with complete visibility across hybrid cloud infrastructure.

Boosting CISO confidence isn't just an internal matter; it has a ripple effect. When CISOs feel supported and empowered by their boards and confident in their technology, their assurance in the organisation's security translates into greater public confidence that their data is well-protected. As a result, a confident CISO means fewer worries across the board – for customers, stakeholders, and the organisation as a whole. With this strengthened sense of security, CISOs can truly take accountability knowing they are doing everything in their power to protect the organisation. This alignment of priorities and resource allocation between boards and CISOs is essential for developing the collective confidence needed to ensure robust protection and accountability.

Maintaining data privacy, preventing fraud and data breaches, and driving digital transformation can strain security resources. IT and security leaders in financial services need to achieve deep observability across their entire hybrid cloud infrastructure to balance speed of service, security, and innovation.

BEN HUNTER
Director of Financial Services, Gigamon

Actionable Recommendations

For boards:
Boards hold the ultimate responsibility for integrating cybersecurity into the core business strategy. By directly linking security initiatives with business objectives, they can ensure that cybersecurity efforts not only protect the organisation but also drive business resilience and growth. It is imperative for boards to set the tone from the top by actively engaging with CISOs and emphasising the criticality of security as a shared organisational priority. This involves creating an environment where CISOs are empowered to communicate openly, contribute to strategic discussions, and drive initiatives that align security with broader business goals. For financial services, key business objectives that boards need to consider include:

- **Compliance with tightening regulations:** Adhering to regulations like DORA and new payment system standards is crucial. Financial services need to meet stringent speed targets for electronic payments including liquidity checks, calculated in milliseconds, with a minimum latency expectation set by the regulators. Streamlining electronic transactions should be a top priority. The upcoming ISO 20022 messaging standard, effective in 2025, offers richer data and improved interoperability but increases pressure on IT and security leaders to upgrade systems without affecting latency and payment speed. Gaining deep observability across the entire hybrid cloud infrastructure is essential to monitor data flows, reduce latency, and eliminate security blind spots, as well as meet compliance standards.
- **Staying competitive by providing excellent customer experience:** Today's consumers expect seamless, fast, and secure payment options, such as digital wallets and contactless payments. To meet these expectations, financial services must overcome challenges posed by legacy systems and complex hybrid cloud infrastructure. Gaining deep observability enables organisations to provide the availability and security needed to offer the highest levels of customer experience.

Boards must recognise that cybersecurity is not a siloed function but a critical component of business resilience. By championing collaboration, boards ensure that security challenges are addressed with clarity and resources are allocated strategically, enabling the organisation to stay ahead of emerging threats and competitive in terms of customer retention.

For CISOs:
CISOs must learn to communicate technical security challenges in a language that the board understands. This means changing the perception of security from being a cost center to a strategic business advantage. To achieve this, CISOs can take these three approaches:

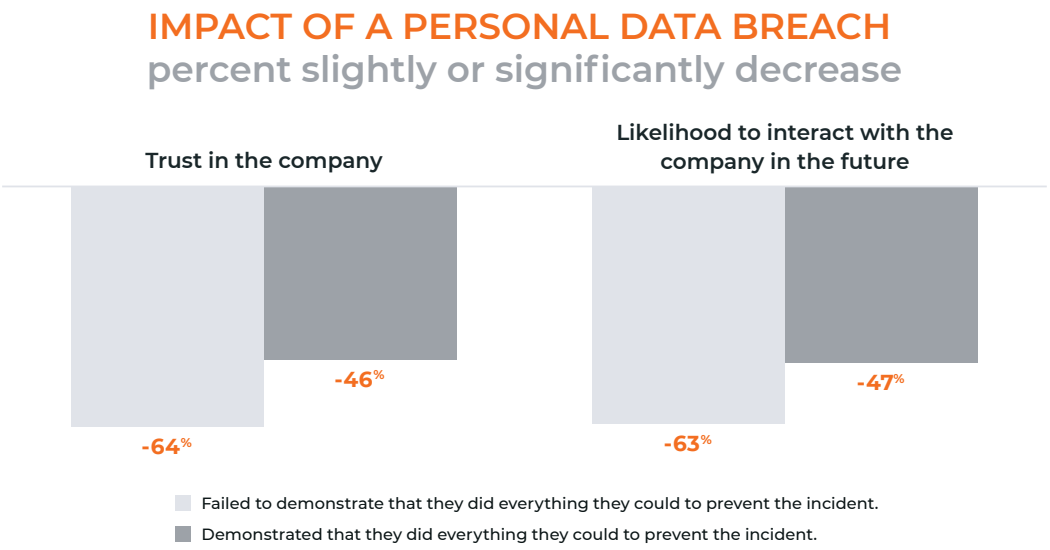
- **Aligning cybersecurity with business objectives:** Demonstrate how security initiatives support the organisation's priorities, such as customer retention, compliance, and reputation.
- **Leverage metrics:** Bring quantifiable data to the table to communicate the organisation's security posture and further needs. For example, our survey demonstrated that having deep observability across the entire infrastructure and being able to demonstrate a strong security posture offset the damage to customer trust following a data breach by almost **30 percent** and increases customer retention by **25 percent**. Presenting this kind of quantifiable statistic to the board can go a long way in security strategy discussions.
- **Educate the board:** Continuously educate the board on emerging threats, industry trends, and the organisation's current vulnerabilities to enable informed decision-making.

Methodology

The data used within this report was collated by Opinium Research following the British Polling Council's rules. The survey was conducted online, pooling 2000 UK adults aged 18 or over. Results have been weighted to be nationally representative. Fieldwork was carried out between 11-15 October, 2024.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organisations. To learn more, please visit gigamon.com.



Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com