HLB Ireland's Strategic Integration of Cybersecurity Services in Partnership with FutureRange

by Mark Butler

The digital revolution requires adaptation and foresight in the evolution of advisory services. Mark Butler, Managing Partner at HLB Ireland, emphasised this necessity during a recent discussion about enhancing the firm's advisory services to meet client needs as they evolve. He detailed his firm's strategic enhancements to its service portfolio, with a notable focus on cybersecurity, expressing enthusiasm about the progress and impact of these initiatives.

Evolving Advisory Services to Meet Dynamic Business Needs

Advisory services have undergone significant transformation over the years to keep pace with the dynamic needs of businesses. Mark reflected on the journey: "The sector has been traditionally focused on financial guidance." However, the rapid digitalisation of industries now compels advisory firms like HLB Ireland to broaden their services. The firm has invested heavily in technology to enhance service delivery—making processes faster, more accurate, and more efficient—thereby freeing up team members to engage more directly with clients.

This technological empowerment has led to a greater appreciation of the value of tech for clients and an understanding of the cyber risks they face. "The threat to advisory firms is real given the information we hold. So we as a firm strategically take cybersecurity very seriously," Mark emphasised, acknowledging the potential for a firm experiencing a cyberattack to act as a bridge to compromising client data.

In June, HLB Ireland was shortlisted for and received high commendation for the "AI Innovation Initiative of the Year" at the International Accounting Awards for using artificial intelligence to improve its analysis and advisory services. "By automating routine processes, we can engage actively and closely with our ambitious clients, maximising the value of our advisory services through one-on-one interactions," said Mark.

HLB Ireland and FutureRange Collaboration

HLB Ireland has forged a strategic partnership with FutureRange to address these growing cybersecurity challenges effectively. "This collaboration allows us to provide top-tier cybersecurity services under the HLB brand, leveraging FutureRange's specialised expertise in a seamless, integrated manner," explained Mark. This partnership embodies a proactive approach to cybersecurity, enabling HLB Ireland to extend comprehensive cyber protection services to its clients while maintaining focus on their core advisory services.

The Challenge of Acquiring Cybersecurity Expertise

Securing top cybersecurity expertise is a significant challenge today due to the swift evolution of cyber threats and the growing demand for skilled professionals. As technologies such as artificial intelligence advance, cyber threats become more complex. This makes it difficult for organisations to rely solely on their internal capabilities. Hiring external cybersecurity experts is crucial. These experts bring specialised skills and keep organisations updated, helping them stay ahead of potential vulnerabilities and maintain strong defences in a rapidly changing digital world.

Benefits of the White-Label Cybersecurity Solution

HLB Ireland's white-label solution offers several strategic benefits:

1. **Revenue Growth:**
   By incorporating FutureRange's cybersecurity solutions into its offerings, HLB Ireland opens new revenue streams. This integration allows the firm to tap into the growing demand for cybersecurity across various sectors, enhancing its overall market presence.

2. **Client Retention and Protection:**
   Robust cybersecurity services ensure secure data and operations, protecting clients' operational integrity and enhancing client loyalty. This protection is crucial, as it helps maintain HLB Ireland's reputation as a guardian of client interests.

3. **Brand Building:**
   Offering advanced cybersecurity solutions under the HLB brand enhances its standing in the market. It positions HLB Ireland as a forward-thinking firm, capable of addressing contemporary business challenges, thus attracting new clients and entering new market segments.

"This white-label solution means we can offer you expert cybersecurity services without the overheads of creating a separate department. It allows us to focus on what we do best—advisory—while ensuring top-level security for our clients' operations," Mark added,

highlighting the efficiency and strategic focus of the firm.

Board of Directors Responsibility in Cybersecurity

HLB Ireland is committed to supporting ambitious owner-managers and board directors, with cybersecurity forming a critical part of this support. The role of the board of directors in overseeing cybersecurity has become increasingly vital. Boards are tasked with ensuring that their organisations have robust cybersecurity measures to safeguard company assets, customer data, and operational capabilities. As part of our advisory role, we actively assist boards of directors in overseeing governance responsibilities encompassing various risk management measures.

This responsibility extends beyond simple oversight; it is a core component of broader corporate governance duties encompassing risk management and compliance with legal and regulatory standards. Consequently, directors must be well-informed about their companies' potential cyber risks and ensure that appropriate policies and procedures are established to mitigate these risks effectively.

Cybersecurity challenges today are marked by a level of sophistication that often surpasses the traditional capabilities found within many organisations.

The advent of AI and machine learning has equipped cybercriminals with tools that enable relentless attacks, necessitating equally relentless defences. As such, cybersecurity can no longer be seen as solely an IT director's responsibility. Instead, it requires a distinct skill set that blends technology, strategic risk management, and regulatory compliance.

External expertise is often necessary to keep pace with these demands. Cybersecurity experts like those at FutureRange provide the specialised knowledge and skills required to develop effective cyber defences. Their involvement ensures that cybersecurity strategies are comprehensive and adhere to the latest standards and practices, thus safeguarding sensitive information and corporate assets more effectively.

This level of expertise and vigilance must be mirrored at the board level, where strategic decisions about cybersecurity investments and policies can significantly impact the organisation's resilience against cyber threats. Boards that understand and prioritise cybersecurity protect their organisations from potential financial and reputational damage and position them as leaders in corporate responsibility and governance.

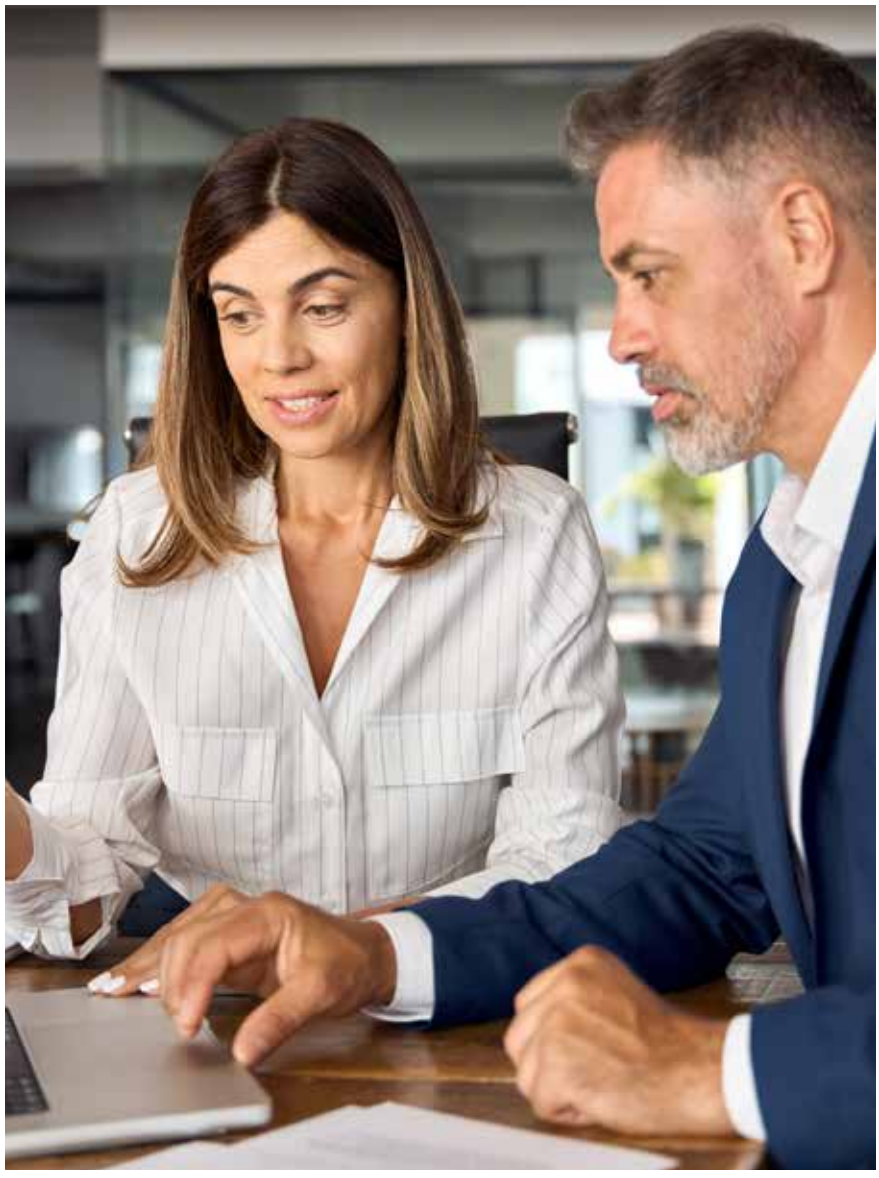
Real-World Cyber Attack Examples

Cyber-attacks can devastate, underscoring the critical need for proactive cybersecurity measures. The reality of these threats highlights how essential it is for businesses to strengthen their defences and prepare for potential incidents.

Recovering from a cyber-attack involves addressing the immediate damages and fortifying systems against future vulnerabilities. This ongoing vigilance is crucial for safeguarding against the increasingly sophisticated nature of cyber threats.

Here are two examples of attacks that clients have experienced: a ransomware attack, which locks an organisation out of its systems, demanding a ransom to restore access and potentially leading to significant operational disruptions and financial losses, and a phishing attack, where sensitive information is stolen, leading to data breaches and compromising both customer trust and corporate integrity.

1. **Law Firm Cyber Attack:**
   A law firm experienced a severe cyber-attack where hackers locked them out of their case management and document storage systems, demanding a ransom to restore access. In addition, sensitive client data was stolen. This attack led to substantial operational disruptions, including significant delays in legal proceedings, loss of billable hours, and a severely tarnished reputation. The theft of client data added



layers of risk, leading to potential breaches of confidentiality and legal consequences.

2. **Logistics Business Phishing Attack:** In another instance, a mid-sized Dublin-based logistics company fell victim to a sophisticated phishing attack. The finance team was deceived into transferring funds to purchase five new vans to a fraudulent account, believing they were dealing with their regular vehicle supplier. This incident caused significant financial losses, impacting the company's operational budget and necessitating an urgent review and enhancement of its cybersecurity measures.

These examples illustrate the complex nature of cyber threats and the extensive consequences they can have on businesses.

Cybersecurity as a Business Imperative

"Cybersecurity is not just an IT issue but a business imperative... to all businesses," Mark stated, underlining the integration of cybersecurity into HLB Ireland's service offerings. In today's landscape, cybersecurity transcends traditional IT concerns, becoming a critical component of national security and affecting businesses of all sizes. The increasing sophistication of cyber threats, propelled by advancements in artificial intelligence, demands robust defensive measures.

Conclusion

Integrating robust cybersecurity measures into business operations has become essential for the entire professional services industry as digital threats evolve. Advisory Firms' strategic response, including the adoption of partnerships with companies like FutureRange and an emphasis on board involvement, highlights the sector's adaptation to the changing landscape of advisory services.

This proactive approach is crucial for maintaining relevance and competitiveness, ensuring that firms stay at the forefront of client service and business resilience in an increasingly digital world.

Through technological advancements, strategic partnerships, and a commitment to cybersecurity at the highest levels of governance, the profession is demonstrating a modern approach to advisory services.

This comprehensive strategy safeguards clients' interests and underscores the importance of evolving with clients' needs. As the industry moves forward, firms must continue considering their clients' changing demands, positioning themselves as forward-thinking leaders in the professional services industry.

www.hlb.ie

Mark Butler

Managing Partner

Mark Butler, managing partner of HLB Ireland has led the firm through a number of mergers in recent years, most recently with John McCarrick & Associates, an accountancy firm founded in 1990 by former Irish international runner John McCarrick. The deal is the fifth transaction HLB Ireland has been involved in so many years as it continues to scale the firm.