FROST & SULLIVAN

Customer Transformation Journeys

Human Risk Management: Hoxhunt

How Hoxhunt Helped Clients Increase Phishing Reporting by up to 225% and Reduce Click Rates by Over 3X

Lead Analyst: Claudio Stahnke | Contributors: Martin Naydenov

MHCD-74 | May 2025

Contents

Summary

Hoxhunt is transforming cybersecurity awareness with its gamified, behavior-driven approach to human risk management (HRM). By utilizing automated phishing simulations, real-time micro-learning, and personalized training, Hoxhunt helps organizations enhance employee awareness and reduce security risks. This proactive method has led to a sharp drop in phishing click rates and a rise in reported threats. Clients across industries, including legal, energy, and financial services, report improved security posture and engagement. Frost & Sullivan conducted an independent analysis, which included customer interviews, to explore Hoxhunt's impact on security awareness programs. The report highlights key challenges, implemented solutions, and measurable benefits. These insights demonstrate how organizations strengthen cybersecurity and reduce human risk using Hoxhunt's innovative HRM platform.

Overview

The cybersecurity landscape continuously evolves, with phishing, social engineering attacks, and human error posing some of the greatest threats to organizations. As cybercriminals refine their tactics, businesses must adapt to protect sensitive data, financial assets, and brand reputation. However, traditional security awareness training often fails to engage employees, leading to poor retention, low participation, and a lack of real behavioral change. Organizations need a dynamic, automated, and engaging solution to build a culture of security awareness while minimizing the administrative burden on security teams.

Hoxhunt's HRM solution directly addresses these challenges with a tailored, gamified platform that personalizes phishing simulations based on employee behavior, skill level, and evolving threat landscapes. By integrating adaptive micro-learning, real-time feedback, and automated reporting, Hoxhunt ensures that cybersecurity best practices are reinforced continuously. Unlike static, one-size-fits-all training programs, this approach keeps employees actively engaged through gamification, competitive elements, and interactive simulations, making security awareness a daily habit rather than an annual requirement.

Hoxhunt

Hoxhunt is recognized as one of the leading HRM vendors globally (Frost Radar™: Human Risk Management, 2024). The company is renowned for its gamified phishing simulations that create an engaging and interactive learning experience, encouraging competition and participation. Additionally, its micro-learning modules provide continuous, behavior-driven training to ensure long-term retention and effective security practices. The platform's adaptive phishing tests dynamically adjust difficulty levels based on employee behavior, delivering personalized challenges that enhance learning outcomes. Furthermore, Hoxhunt offers a customizable reporting dashboard that provides granular insights into an organization's security posture, tracking click rates, reporting trends, and engagement levels.

Hoxhunt's commitment to client collaboration fosters continuous innovation, leading to unique features such as phishing response automation, seamless email security integrations, and multi-language support. Due to its simplicity, adaptability, and measurable security improvements, enterprises have widely adopted the platform in high-risk sectors, including finance, law, and energy. As cybersecurity threats evolve, Hoxhunt remains at the forefront of HRM, providing organizations with the tools to build a resilient security culture.

Transformation Journeys

Frost & Sullivan's research with Hoxhunt customers revealed significant benefits post-deployment.

Leading Energy Provider

A leading energy provider in the United States faced significant challenges in strengthening employee cybersecurity awareness. As a critical infrastructure company, it was a prime target for ransomware, targeted phishing campaigns, and supply chain attacks from nation-state actors and cybercriminals. Despite previous phishing awareness programs, engagement remained low, leaving employees vulnerable to attacks. Traditional training methods, such as those where employees have to sit through a slide deck for 20 minutes and then reply to a questionnaire once a year, were often ignored, leading to an alarming phishing success rate. Additionally, manually conducting phishing simulations greatly burdened the security team, limiting their ability to address threats proactively.

> *Hoxhunt's gamified approach fostered a competitive learning environment, moving away from punitive training and encouraging employees to identify phishing threats actively.*
>
> Claudio Stahnke
> Industry Analyst

The organization implemented Hoxhunt's automated, behavior-driven phishing simulations to overcome these challenges, significantly improving training efficiency and engagement. Hoxhunt's gamified approach fostered a competitive learning environment, moving away from punitive training and encouraging employees to identify phishing threats actively. The adaptive system personalized training difficulty based on user behavior, ensuring continuous improvement while integrating seamlessly with the company's incident response processes.

The company's chief information security officer (CISO) reported, "Initially, our phishing click rates were around 10%, but after implementing Hoxhunt, we've reduced them to 2% to 3%. More importantly, our phishing reporting rate jumped from 20% to 60% to 65%, greatly improving our security awareness."[1] Real-time analytics dashboards gave the security team greater visibility, enabling them to fine-tune training programs based on employee performance and emerging threats. This targeted approach reinforced a proactive security culture and enhanced the organization's resilience against evolving cyber threats.

[1] Frost & Sullivan interview, November 2024.

Global Law Firm

A global law firm with over 3,000 employees and vast amounts of sensitive client data struggled to engage senior lawyers and executives in cybersecurity training, making regulatory compliance difficult. Exempting high-ranking employees from phishing simulations created security gaps, increasing the risk of breaches, as cybercriminals often target executives with sophisticated phishing attacks. To address this, the firm selected Hoxhunt for its tailored, automated phishing simulations and engaging training model, which stood out from traditional, one-size-fits-all solutions. The firm was particularly drawn to Hoxhunt's ability to deliver personalized training based on employee behavior, seamless integration with existing security infrastructure, and its strong customer support and innovation reputation. The gamified training approach, which included interactive challenges, points, and department leaderboards, significantly boosted engagement.

Recognizing the limitations of annual training, the firm shifted to a continuous micro-learning approach, delivering regular, bite-sized training modules tailored to employee roles; this improved retention and reinforced proactive security behaviors.

Claudio Stahnke
Industry Analyst

A security leader in the law firm shared, "Getting senior lawyers and executives engaged in cybersecurity training was always challenging. We saw a complete shift with Hoxhunt's personalized approach and gamified simulations; employees now actively participate in security awareness. The ability to tailor training to our internal policies made a huge difference in making cybersecurity relevant to our workforce."[2] Recognizing the limitations of annual training, the firm shifted to a continuous micro-learning approach, delivering regular, bite-sized training modules tailored to employee roles; this improved retention and reinforced proactive security behaviors.

Additionally, the firm incorporated phishing simulations based on internal communication patterns, enabling the identification and mitigation of vulnerabilities specific to legal professionals. These enhancements led to a notable increase in participation, with employees at all levels becoming more vigilant against cyber threats. By fostering a more resilient security culture, the firm strengthened its ability to protect sensitive client data while ensuring compliance with evolving regulatory requirements.

Multinational Corporation

A multinational energy corporation with around 10,000 employees across multiple regions struggled to effectively engage employees in cybersecurity training. As a critical infrastructure provider, the company was a prime target for ransomware attacks, state-sponsored cyber espionage, and targeted phishing campaigns. Existing training programs were perceived as ineffective, with low participation rates and resistance to phishing simulations. Additionally, the manual deployment of phishing tests and the lack of multilingual support created barriers to scalability and engagement across its global workforce.

[2] Frost & Sullivan interview, November 2024.

To address these issues, the company adopted Hoxhunt, which provided automated phishing simulations, gamified learning, and extensive customization options. This allowed the company to "set it and forget it," reducing the security team's administrative workload while fostering a more engaging and proactive security culture. The CISO, admitting his initial hesitation, stated, "We were initially skeptical about the effectiveness of this approach, but it turned out to be one of the best deployments we've ever had. The platform's automation, gamification, and adaptability wholly transformed how our employees engage with cybersecurity training."[3] Employees participated in bite-sized, behavior-driven training in their preferred languages, significantly improving engagement. Phishing reports increased from 80 monthly submissions to over 2,000, and the phishing failure rate dropped below 3%, reflecting a substantial shift in security awareness.

The company collaborated with Hoxhunt to tailor training content, integrate phishing simulations with incident response workflows, and enhance real-time threat visibility. With data-driven insights and a more interactive approach, the organization strengthened its cybersecurity posture, increased phishing resistance, and ensured compliance across global operations.

Transformation Outcomes

Increased Employee Awareness and Engagement

Hoxhunt's gamified approach, featuring leaderboards, achievement tracking, and rewards, fostered a security-conscious culture where employees actively reported phishing attempts. This interactive method enhanced participation and drove a remarkable increase in engagement, with the number of emails reporting phishing surging from 80 to 90 per month to 2,000 per month after implementation. By reinforcing long-term vigilance and making security awareness an integral part of daily operations, Hoxhunt's approach transformed employees into proactive defenders against cyber threats.

Sharp Decline in Phishing Click Rates

A Hoxhunt client reduced its rate by 3 times within 3 years thanks to the company's artificial intelligence (AI)-driven, personalized training that adapts to individual risk levels. By continuously exposing employees to simulated threats based on their behavior, Hoxhunt strengthened the client's ability to recognize and avoid actual phishing attacks.

[3] Frost & Sullivan interview, November 2024.

Improved Threat Detection and Incident Response

Another Hoxhunt customer increased its email phishing reporting by 225%, giving security teams greater visibility into threats. This was the result of the better engagement brought by a gamified approach. Furthermore, seamless integration with security tools enabled automated phishing removal, reducing the risk of widespread compromise and easing the burden on information technology (IT) teams. Additionally, Hoxhunt drove measurable productivity gains by automating phishing simulations and analysis, freeing security teams from time-consuming manual tasks. The platform enhanced security and optimized resource allocation by streamlining training and response processes, making it an essential asset for modern enterprise cybersecurity strategies.

Insights for CISOs

HRM is rapidly evolving as organizations recognize that human error remains a leading cause of security breaches. A key trend shaping the HRM landscape is the convergence of cybersecurity training, behavioral analytics, and incident response tools. Organizations are shifting from one-size-fits-all security awareness programs to adaptive, data-driven solutions that dynamically adjust based on employee behavior and risk levels. Additionally, automation and AI-driven security training are becoming critical differentiators, enabling organizations to scale security awareness programs without overwhelming security teams.

To maximize the effectiveness of HRM implementations, CISOs should consider the following factors.

Integration Capabilities: Seamless integrations with existing security workflows and infrastructure that amplify returns on investment (ROI)

Multilingual & Customizable Training: Tailored content that engages a globally distributed workforce

Automation & AI: Significantly reduced manual workload on security teams; training that can scale across the entire organization

Real-time Behavioral Insights: Proactive responses to risky actions, reducing the likelihood of security breaches

Company Culture Alignment: Shared responsibility culture, promoting consistent security behaviors and support across all levels of the organization

Key Performance Indicator (KPI) Tracking: Productivity and participation improvements, enhanced completion and reporting rates, and reduced click rates, which help refine training programs over time

Frost Perspective

With cyber threats increasingly targeting employees through phishing, social engineering, and credential theft, HRM is now essential. Traditional security awareness training is insufficient, as organizations need adaptive learning solutions that evolve with modern attack techniques. Without HRM, businesses risk breaches, compliance failures, and financial losses. A strong HRM strategy reduces human-driven risks and fosters a security-aware culture.

To stay competitive, HRM providers must focus on AI-driven phishing simulations, behavioral analytics, and automated, personalized training. Future solutions will integrate with incident response tools to help security teams mitigate risks proactively. CISO-oriented dashboards will also become crucial for measuring ROI and aligning security with business objectives. Additionally, peer-driven engagement programs will strengthen the cybersecurity culture. As HRM evolves, providers that innovate and integrate with enterprise security ecosystems will lead. Hoxhunt exemplifies this shift, combining gamification, automation, and adaptive learning to help organizations reduce human risk and build long-term cybersecurity resilience.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to: permission@frost.com

Frost & Sullivan Analytics Methodology & Next Steps

Frost & Sullivan Analytics Methodology

Analytics Conceptualization	• Internal topic review by analytics team • Review with commercial team and clients • Develop scope • Develop assumptions and availability of existing data and analytics • Develop detailed outline	DATA VALIDATION (INTERNAL EXPERT & PRIMARY INTERVIEWS)

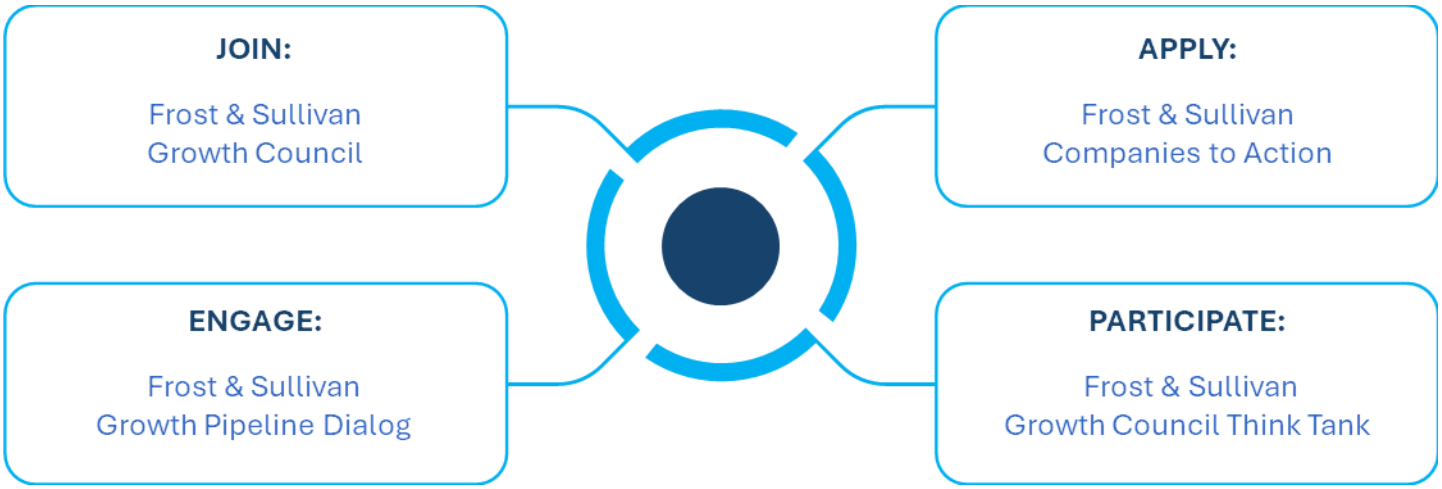
Data Procurement	• **Primary research (80%)**
	  ○ Vendors and service providers
	  ○ Customers
	  ○ Value chain partners
	  ○ Trade associations
	• **Secondary research (20%)**
	  ○ Publications
	  ○ Ecosystem websites
	  ○ Online databases
	  ○ Search engines and Generative AI tools	

Data Analysis	• Consolidate data collected from secondary sources that is validated with primary interviews • Collate data from internal and external experts • Develop and produce quantitative models and forecasts • Identify data gaps for additional primary interviews	
Analytics Intelligence	• Develop analytics structure based on initial outline • Qualitative content development • Quantitative data development • Identify data gaps for additional primary interviews	
Analytics Delivery	• Project management and peer review • Editing and quality control checks • Delivery of analytics to clients using multiple delivery mechanisms	

Source: Frost & Sullivan

Next Steps: Benefits & Impacts of Growth Opportunities

Next Steps: The Transformational Growth Partnership



Source: Frost & Sullivan