

INFOSEC HRM™

POWERED BY RIGHT-HAND CYBERSECURITY

How enterprises are at the forefront of human risk management

— and how you can be too



The human element in cybersecurity

Security breaches don't just happen — they often start with a single click, a moment of trust or an honest mistake. According to [Verizon's 2025 Data Breach Investigations Report](#), 60% of breaches stem from the human element, whether through social engineering or unintentional errors.

Yet many security leaders face a common challenge: their security awareness training programs have plateaued. Despite regular training and phishing simulations, organizations struggle to drive further improvements in security behaviors. Program managers need to demonstrate value and ROI while keeping employees engaged and reducing security incidents.

For enterprises managing thousands of employees across multiple locations, successfully addressing human risk requires moving beyond traditional security awareness training. Leading organizations now place individual employees at the center of their security strategy, using real-time data and personalized approaches to reduce risky behaviors and prevent incidents before they occur.

The organizations featured in this guide have overcome challenges by evolving their approach. They've built programs that adapt to each employee's needs and risks through automation, personalization and data-driven insights. Their experiences offer a roadmap for maturing your program, whether you're looking to scale globally, unify training across divisions or break through that plateau.

INFOSEC HRM

POWERED BY RIGHT-HAND CYBERSECURITY

Infosec and Right-Hand Cybersecurity have united their security awareness and human risk management expertise. This partnership combines proven training content with real-time risk insights, delivering alert-based training nudges that respond to actual security events. By increasing visibility into security risks and providing personalized education, organizations can build stronger security cultures while reducing incidents.

[Learn More](#)

Enhancing training with notifications

Western Alliance Bancorporation, ranked #1 among the 50 largest public U.S. Banks by S&P Global Market Intelligence, manages \$50 billion in assets across 54 banking offices.



CHALLENGE

With a shift to remote and hybrid work, employee households became extensions of the corporate network. They needed a security awareness solution that could adapt to individual learning curves and styles while ensuring engagement and knowledge retention outside the office.



APPROACH

They selected a platform offering mobile app, web browser and email push notifications for training flexibility. The solution uses artificial intelligence to deliver personalized learning nudges based on each user's training needs and risk profile, enabling "in-the-moment" coaching.



OUTCOME

The program transformed employees' engagement with security training through one-minute games reflecting real-world scenarios. Employees access training through their preferred methods, either mobile, web or email, making participating convenient regardless of location.

The gamified approach with leaderboards and rewards maintains engagement while reinforcing security concepts. Rather than traditional compliance-based training that "checks the box," the platform creates unique curriculums for each user. Integration capabilities with tools like Microsoft Teams and Slack ensure training reaches employees where they already work, strengthening the organization's security culture.



ORGANIZATION

Western Alliance Bancorporation

INDUSTRY

Financial Services

CUSTOMER

Victor Vinogradov, CISO



Most solutions deliver brushstroke training campaigns for all users, but this created unique curriculums for each user based on what they needed to know. Offering the flexibility of multiple access points allows users to consume content in their preferred method of how they work."

— Victor Vinogradov

Reducing employee-generated security alerts

A prominent debt servicing and loan management company manages complex portfolios, including mortgages, auto loans and credit card debt for financial institutions and government agencies.



CHALLENGE

The organization faced frequent phishing attacks and business email compromise (BEC) attempts. Additionally, employees handling sensitive financial data created a high volume of security alerts, straining the security operations center (SOC) team while creating compliance and security risks.



APPROACH

They implemented a human risk management platform that combined phishing simulations and security awareness training with their existing security tools. The solution delivered real-time user nudges when employees generated security alerts, integrating with their email security and SIEM solutions through MS Teams.



OUTCOME

Within 60 days, sensitive data exposure incidents decreased by 17%, showing rapid behavior change. Training completion rates reach 96% across campaigns, a significant improvement from previous programs. The organization saw a 19% increase in reported phishing emails and reduced click rates to below 4%.

Integrating existing security tools proved particularly valuable, enabling the SOC team to efficiently manage alerts while providing targeted interventions. The behavior-based training assignments, tailored to real incidents within the organization, maintained high engagement levels and demonstrated clear ROI through reduced security events.



ORGANIZATION

Leading Financial Services
Organization

INDUSTRY

Financial Services (Debt Servicing and
Loan Management)

CUSTOMER

Security Program Manager



The automated delivery of targeted employee training has been a great alternative to traditional e-learning. When we can see alerts decrease by 17% in just 60 days, that's real behavior change. The platform provides insightful data on employee behavior, enabling targeted interventions and more informed decision-making."

— Security Program Manager

Scaling training globally

Amway is a global health and beauty company with 15,000+ employees across 100+ countries, generating \$8.8 billion in revenue and holding 780 patents.



CHALLENGE

Despite having in-person training and a learning management system, Amway needed a scalable solution to reach its global workforce effectively. Its existing program couldn't adequately protect the company's intellectual property or provide consistent training across regions and divisions.



APPROACH

After evaluating multiple vendors, the team selected a platform based on automation capabilities and regional customization features. They launched their first automated global campaign to 18,000 learners, focusing on delivering targeted training that could adapt to each region's needs.



OUTCOME

The program achieved a 90% training completion rate with positive feedback on content relevance. By combining computer-based training with offline resources like posters, they reinforced key security measures effectively. The team now tracks success through employee surveys, focus groups and platform analytics.

Most significantly, they've created a proactive security culture where employees ask about upcoming training and demonstrate increased security awareness in their daily work. The automation features simplified campaign management, from scheduling to tracking progress and reporting metrics to stakeholders.



ORGANIZATION

Amway

INDUSTRY

Health and Beauty

CUSTOMER

Dan Teitsma, Information Security Specialist



We've significantly increased awareness overall and are starting to see a shift in culture. Employees understand the importance of information security and are playing a much more active role in keeping our data secure. If you're going to increase awareness and motivate behavior change, you need to deliver content in different ways."

— Dan Teitsma

Unifying awareness across agencies

The **State of Kansas** manages critical government functions across multiple agencies, providing essential services for state residents, from healthcare to infrastructure.



CHALLENGE

State agencies often lag behind the private sector and technological advancement while facing sophisticated phishing campaigns and internal vulnerabilities. With inconsistent training across agencies weakening overall security, they needed a unified approach to protect sensitive information.



APPROACH

The Kansas Information Security Office (KISO) evaluated dozens of security awareness vendors before selecting a platform to deliver consistent methods and messaging across all executive branch agencies. They focused on compliance requirements while ensuring the solution was cost-effective with public funds.



OUTCOME

The program dramatically improved security metrics, with one agency reducing phishing susceptibility from over 8% to just 2%. The platform's timely content updates, including real-world training examples around events like the [CrowdStrike incident](#), kept training relevant and engaging. As they saw results, more agencies voluntarily joined the phishing campaigns.

The unified approach ensured that employees at smaller agencies receive the same high-quality training as larger departments, creating consistent protection across state government. Employees now complete more than their mandatory training, engaging with suggested modules that help them protect both work and personal data.



ORGANIZATION

State of Kansas

INDUSTRY

State and Local Government

CUSTOMER

Gary Scott, Security Analyst



Government security is only as strong as its most vulnerable agency. We needed uniform training across all state government agencies to ensure employees at small agencies get the same training as those at larger, more prominent agencies. When people understand how cybersecurity impacts their daily lives, they're more likely to pay attention."

— Gary Scott

Increasing employee engagement and behavior change

A global marketing technology company that serves thousands of direct-to-consumer (D2C) clients, supporting over 1,000 employees worldwide with data-driven solutions for customer engagement.



CHALLENGE

With a hybrid workforce spread across the globe, they needed a unified human risk management program that could scale. Traditional training wasn't resonating with users, and they required granular reporting for specific follow-ups based on user risks and gaps.



APPROACH

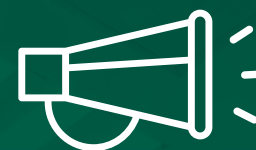
After evaluating over a dozen vendors, they selected a platform offering automated delivery of targeted training. The solution integrated with SSO for easy onboarding and provided custom configurations to map training to corporate policies and culture, meeting learners where they work.



OUTCOME

The automated, gamified approach transformed their security culture. After completing assigned modules, employees began requesting additional learning about phishing red flags. The micro-learning format and interactive user experience improved knowledge retention while overcoming the traditional "forgetting curve."

The security team gained visibility across departments to identify which groups were most and least cyber-ready, enabling targeted follow-ups. The platform's automation simplified program management, while custom content aligned with company policies maintained cultural relevance.



ORGANIZATION

Leading Marketing Technology
SaaS Company

INDUSTRY

D2C Marketing Technology

CUSTOMER

Security Program Manager



Other solutions were too 'check-the-box' or 'one-size-fits-all.' Once configured, the system runs automatically across all users. Being able to fine-tune and customize content to map to our policies and corporate culture makes training stick. The gamified, micro-module approach helps make knowledge last."

— Security Program Manager

Reducing employee phishing susceptibility

Penn Entertainment is the largest domestic casino and hotel operator in the United States, employing over 16,000 people across multiple states and gaming jurisdictions.



CHALLENGE

Email-based threats, particularly phishing and business email compromise, posed significant risks to the organization. With an initial 20% employee phishing rate, they needed a solution to effectively teach employees how to detect and avoid email-based threats.



APPROACH

After evaluating nearly 20 training programs, they implemented a role-based security awareness program. Starting with bi-monthly phishing simulations to identify weak points, they analyzed trends by department, office location and simulation types to build targeted education campaigns.



OUTCOME

The program achieved remarkable results, dropping phishing rates from 20% to just 2%. They observed a significant increase in employees reporting suspicious emails to the security department. Monthly phishing simulations — combined with in-person new hire training, security newsletters and monthly manager meetings — kept security in focus.

The team continually adapts phishing templates to mirror actual threats facing the organization, making training scenarios realistic and relevant. This comprehensive approach helps validate lesson retention and overall awareness, while regular communication through manager meetings ensures security stays a priority across all departments.



ORGANIZATION

Penn Entertainment

INDUSTRY

Entertainment and Hospitality

CUSTOMER

Marc Puhala, Security Analyst



Since starting these campaigns, we've noticed a huge increase in suspicious emails reported to the security department. People are definitely more aware. Employee training needs to be relevant to their role, or it won't work. We tailor training to specific individuals in cases where extra support is needed."

— Marc Puhala

KEY TAKEAWAYS

How can you lead in human risk management?

Throughout these case studies, successful enterprise security leaders revealed several key strategies for evolving security awareness into effective human risk management:



Automate to scale

- » Deploy automated campaigns that deliver training at the right time
- » Use integration capabilities to streamline program management
- » Let automation handle scheduling, tracking and reporting



Personalize the experience

- » Provide training through learners' preferred channels
- » Deliver content relevant to each employee's role and risk level
- » Create targeted interventions based on actual security events



Measure what matters

- » Track both quantitative metrics and qualitative feedback
- » Monitor security incidents, alert volumes and behavior changes
- » Use data to demonstrate program ROI to stakeholders



Make training relevant

- » Customize content to align with company policies and culture
- » Use real-world examples and timely threat updates
- » Keep lessons brief and focused on practical application



Start simple. Prioritize what training topics are most important to your business and select a tool that allows you to effectively deliver that training to the most people possible. Make it easy for employees to participate and find ways to make content relevant to their daily work.”

— Dan Teitsma,
Information Security Specialist

Ready to transform your security awareness program?

Book a meeting to learn more about [Infosec HRM](#) and discover how you can implement these enterprise best practices in your organization.

Additional resources



[See Infosec HRM in action](#)



[Learn about infosec HRM](#)



[Browse award-winning training content](#)



[Learn about human risk management](#)

INFOSEC HRM

POWERED BY RIGHT-HAND CYBERSECURITY

Infosec HRM increases visibility into security risk and provides alert-based training nudges to improve employee behaviors and decrease security events.

Infosec HRM will help you to:

- » Detect and measure risky employee behaviors
- » Provide in-the-moment training when a security event is detected
- » Deliver personalized alert-based training nudges through your existing tech stack
- » Cultivate a positive security culture within the organization

Key benefits:

- » Stronger collaboration between the security training and security operations sides of your organization
- » A reduction in security events and SOC alert fatigue
- » Behavior and data-driven insights to clearly communicate ROI and the impact of the program
- » More value from existing security investments

[Book Meeting](#)

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. More than 70% of the Fortune 500 have relied on Infosec to develop their security talent, and more than 5 million learners worldwide are more cyber-resilient from Infosec IQ's security awareness training.

Learn more at infosecinstitute.com.