Issue 1

Shaping the Future of Security Awareness

From Outdated Training to Strategic AI-Based Empowerment: Welcome to the Future of Cyber Resilience.

Rethinking Human Security in the Age of AI

In today's evolving threat landscape, your organization faces a critical question: Are traditional security awareness programs actually keeping you safe?

The sobering truth: Despite billions invested in cybersecurity training, human error remains the primary attack vector in the majority of organizations. This is because traditional compliance-based training programs often fail to bridge the gap between knowledge and behavior. Employees might sit through training sessions or complete phishing simulations, but if they do not truly internalize what they learn, the risk remains. ***It is not just about knowing what to do; it is about actually doing it.***

Cybersecurity teams are stretched thin, juggling more threats with fewer resources. Many organizations face a shortage of skilled cybersecurity professionals, making it difficult to continuously educate, engage, and reinforce secure behaviors among employees. Traditional cybersecurity awareness and learning methods have long relied almost exclusively on phishing simulation campaigns and Learning Management Systems (LMS). While these tools provide a basic level of security training and might check some compliance boxes, they fall short of instilling a true cultural shift in cybersecurity awareness. Phishing simulations, though useful in measuring susceptibility, often fail to address the root cause of risky behavior. On the other hand, LMS-based trainings are typically generic, passive, and detached from real-world scenarios. As a result, employees complete training modules without internalizing critical security behaviors, leaving organizations vulnerable to evolving cyber threats. This outdated approach has contributed to the current gaps in cybersecurity awareness, leading to increased risks, growing vulnerabilities, and an escalating number of sophisticated attacks that specifically target the human factor as the weakest link in security defenses.

What You'll Learn in This Issue

In this special edition of ZINAD's Cybersecurity Insights, featuring research from Gartner, we will explore:

- The human factor in cyber risk— "According to the 2024 Verizon Data Breach Investigations Report, 68% of cybersecurity breaches are primarily caused by human action" [1] and what can you do about it?
- How AI is redefining cybersecurity awareness and bridging the gap between training and real-world security behaviors.
- The limitations of traditional cybersecurity training and why a new approach is needed.
- How ZiSoft provides a one-stop solution that integrates with your organization's unique culture, security needs, and business goals.

These insights, explore the revolutionary shift from outdated compliance-based training to AI-driven security awareness programs that demonstrably changes behavior and strengthens your security posture. AI-powered cybersecurity awareness solutions help bridge this gap by enabling automated, scalable, and personalized security training that adjusts to individual risk profiles and learning styles. This modernized approach not only reduces reliance on overstretched cybersecurity teams but also enhances engagement by delivering contextual security insights at the right moment. With AI at the core, organizations can foster a security-aware culture from the inside out, making cybersecurity awareness a continuous, adaptive, and behavior-driven process rather than a static compliance requirement.

Join us as we dive into expert insights, real-world success stories, and practical strategies to help your organization stay ahead of emerging threats.

Welcome to the future of cybersecurity awareness—with ZINAD.

[1] Gartner Inc., Top Trends in Cybersecurity for 2025, 12 December 2024, G00822766

Source: ZINAD

Shaping the Future of Security Awareness

From Outdated Training to Strategic AI-Based Empowerment: Welcome to the Future of Cyber Resilience.

ZiSoft: The Future of Cybersecurity Awareness for CISOs & SRMs

Cybersecurity Awareness That Drives Real Change

"There are more than 3,000 cybersecurity vendors to choose from. Consequently, SRM leaders are finding it more challenging to manage the inherent tension between trying to enhance their capabilities to address new technologies and emergent risks and concurrently reducing operational overhead and complexity"[1]. At the same time, growing regulatory pressure, evolving threats, and an industry-wide talent shortage are pushing security teams to their limits. In addition to these challenges, **winning executive buy-in for security behavior and culture programs (SBCPs)** remains a major challenge.

Figure (1): 5 reasons why your traditional awareness training falls short | ZINAD

- **No Measurable ROI** → According to a survey, **over two-thirds (68%)** of surveyed leaders have found it more difficult to obtain executive buy-in for their organization's SBCP in comparison to their existing security awareness and training program, although just a few say it's been significantly more difficult (4%).
    - **ZiSoft** provides measurable, dashboard-driven data analytics that translate security awareness into **actionable KPI metrics**, making it easier to justify investment in broader security initiatives.
- **Limited C-suite Engagement** → Without **targeted insights and industry updates**, leadership remains disconnected from security priorities.
    - **ZiSoft** goes beyond standard training and includes **C-suite-specific content**, offering key statistics, industry trends, and regulatory updates that help decision-makers stay ahead of emerging threats. A well-informed leadership team makes faster, more strategic security investments, strengthening the organization's overall resilience.
- **Compliance ≠ Security** → Organizations mistakenly equate compliance with security, leaving them vulnerable to cyber threats as employees are not adequately trained to recognize and respond to risks beyond regulatory mandates.
    - **ZiSoft** AI-powered security awareness programs bridge this gap by providing tailored training that enhances **both technical and non-technical** employees' understanding of cybersecurity risks, ensuring they are prepared to detect and mitigate threats effectively, rather than merely fulfilling compliance requirements.
- **The Knowledge-Action Disconnect** → CEOs must invest in solutions that go beyond check-the-box training.
    - ZiSoft, empowered by AI and recent behavioral research, moves beyond surface-level metrics into changing feelings and behaviors to instill real habit change. **It is not just about knowing what to do; it is about actually doing it.**
- **Vendor Sprawl** → Managing multiple awareness solutions across different departments creates inefficiency in awareness data and objectives. In addition, managing different licenses increases **costs, complexity, and operational overhead**

  .
    - **ZiSoft** is your one-stop-shop with one license, 6 different modules to eliminate complexity, reduce overhead, and ensure a streamlined, effective approach to security awareness.

Customer Success in Action

Case Study (1): Strengthening Security at Global Enterprises

A global financial services firm, facing a rise in targeted phishing attacks, implemented ZiSoft to enhance its cybersecurity posture. The AI-driven **Phishing Assessment** module helped tailor simulations to the specific threats the company faced, resulting in a 50% decrease in successful phishing attempts within the first quarter of deployment.

Moreover, the organization reported higher overall participation in security training, rising from 40% to 85%, driven by the platform's incentivized Motivational Framework. The customized learning paths and interactive workshops contributed to a noticeable shift in employees' engagement levels and attitudes towards security, significantly reducing their vulnerability to cyber threats.

Case Study (2): Scalable Cloud Solutions for Governmental Sectors

A National Cybersecurity Authority identified a gap in accessible resources and coordinated efforts to strengthen citizens' cybersecurity practices and culture.

Cyber Emissaries module blueprint incentivized citizens to actively engage in tasks like training and sharing awareness content, reaching a peak in the prestigious Cybersecurity Champion Shield. This approach enhanced cybersecurity awareness across schools, universities, and organizations, empowering citizens to actively contribute to national cybersecurity efforts and fostering a well-informed, engaged, and security-conscious community.

With ZiSoft's modern architecture, a large-scale awareness campaign was deployed, supporting over 9 million users within the governmental sector without compromising agility or ease of use. The cloud-based infrastructure enabled rapid scalability, providing comprehensive coverage across global operations. This scalability was key to ensuring that all participants, regardless of location, received consistent, high-quality training.

[1] Gartner Inc., Top Trends in Cybersecurity for 2025, 12 December 2024, G00822766

Source: ZINAD

Shaping the Future of Security Awareness

From Outdated Training to Strategic AI-Based Empowerment: Welcome to the Future of Cyber Resilience.

Research from Gartner

The Impact of Generative AI on Security Behavior and Culture Programs

GenAI and LLM have captured the interest of organizations aiming to enhance their security training programs. SRM leaders should understand how this technology can be used to improve security training programs, and more importantly, the organization's overall security culture.

Evidence

[1] **Phishing**, Mitre Altas.

[2] **Zscaler Research Finds 60% Increase in AI-Driven Phishing Attacks**, Zscaler.

[3] **NSA, FBI, and CISA Release Cybersecurity Information Sheet on Deepfake Threats**, CISA.

[4] **2022 Gartner Cybersecurity Awareness Survey.** This survey was conducted via invitation to Gartner clients across industries and geographies between February and April 2022 and provided 154 responses. The objective of the survey was to understand headcount and resources that organizations allocate (and are planning to allocate) to security awareness programs and common approaches taken to implement security awareness programs.

Overview

Impacts

- Threat actors exploit generative AI (GenAI), enabling them to rapidly and continuously adapt their attack tactics.
- GenAI also makes it far easier for employees across the organization to undertake technology work. This is a double-edged sword — it can enhance operational outcomes but also introduce new vectors for realizing operational cybersecurity risks.
- Traditional (or legacy) cybersecurity skills training falls short in addressing modern GenAI risks.

Recommendations

SRM leaders exploring GenAI to improve cybersecurity training and overall corporate security culture should:

- Focus on protecting the organization against evolving attack methods by incorporating AI capabilities.
- Expand their focus beyond static computer-based training and phishing campaigns by embracing GenAI to enable behavioral changes.
- Augment their existing security behavior and culture program with GenAI tools to improve the scale and understandability of security guidance and expectations.

Strategic Planning Assumption

By 2026, enterprises combining GenAI with an integrated platforms-based architecture in security behavior and culture programs will experience 40% fewer employee-driven cybersecurity incidents.

Introduction

The integration of AI into security behavior and culture program capabilities is not a recent cybersecurity trend. For the past decade, SRM leaders and vendors have incorporated AI elements, such as threat and anomaly detection, into their programs and platforms, which eventually feed into personalized learning. What is new, however, is the rapid and pervasive emergence of GenAI.

> *Gartner defines GenAI as technologies that "can generate new, derived versions of content, strategies, designs and methods by learning from large repositories of original source content."*

GenAI and its capabilities have enhanced existing tactics and processes that aim to promote secure behavior in employees. Examples of potential enhancements include AI assist chatbots, interactive simulations and adaptive, hyperpersonalized social engineering threat simulation capabilities. The current maturity of these enhancements vary from nascent to established. Ultimately, these advancements address the need for more adaptive and dynamic security engagement with counterparts in IT and the business.

Moreover, GenAI empowers SRM leaders to take greater ownership of their security training programs, reducing reliance on vendors to build campaigns and training. Vendors will still have an important role to play. Organizations developing internal GenAI tools do so to improve productivity, which is crucial in the cybersecurity function where resources are often limited. Those responsible for security training programs should expect a significant increase in impact and scale. This increase comes with potential challenges and ethical concerns, such as data privacy.

Many leaders are still in the experimentation phase, exploring the best ways to leverage GenAI within their security training programs. This research aims to delve into the impact of GenAI on these capabilities, specifically addressing tools and content.

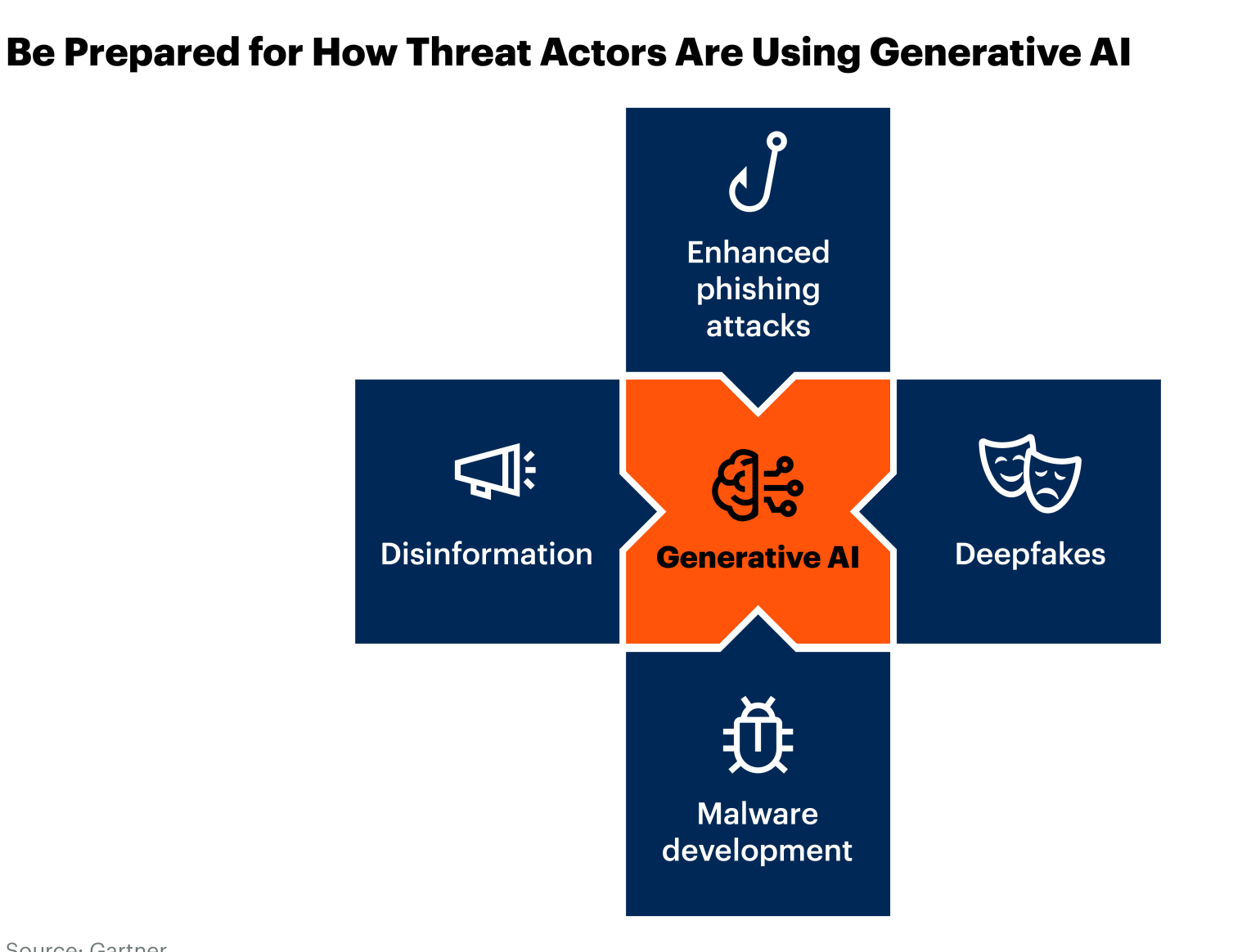
Impacts and Recommendations

Threat Actors Exploit GenAI, Enabling Them to Rapidly and Continuously Adapt Their Attack Tactics

The rapid evolution of GenAI has provided threat actors with sophisticated tools to enhance and diversify their attack methodologies. This paradigm shift in cyberthreat landscapes necessitates a comprehensive understanding of the capabilities and implications of GenAI in cybersecurity.

Additionally, it is important to note that threat actors are using GenAI for other malicious actions. While not an exhaustive list, Figure 1 depicts these other actions.

Figure 1. Be Prepared for How Threat Actors Are Using Generative AI



Source: Gartner
Note: The list mentioned is not exhaustive.
816736_C

Gartner

We explore two main examples of social engineering.

Enhanced Phishing Attacks

One of the primary areas where GenAI has made a significant impact is phishing. Traditional phishing attacks often relied on rudimentary techniques that could be easily detected by vigilant users and advanced email filters. However, with the advent of GenAI, threat actors can now craft highly convincing and personalized phishing emails. GenAI, including LLMs that generate synthetic text, visual deepfakes of faces, and audio deepfakes of speech, enables adversaries to scale targeted phishing campaigns. LLMs can interact with users via text conversations and be programmed with a meta prompt to phish for sensitive information.[1] According to a report, global phishing attacks increased 60% in 2023, with a notable rise in the sophistication of these attacks attributed to AI-generated content.[2]

Deepfake Technology

The proliferation of deepfake technology, powered by GenAI, poses a significant threat to cybersecurity. Deepfakes can be used to create realistic but fraudulent images, videos and audio recordings. This technology has been employed in social engineering attacks to impersonate executives and other high-profile individuals, thereby facilitating enhanced victim targeting and other forms of fraud. The FBI, Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA) in the U.S. have issued warnings about the increasing use of deepfakes in cybercrime, emphasizing the need for advanced detection mechanisms.[3]

Technological Advancements From GenAI Improve the Existing Capabilities of Traditional Training Programs

GenAI is not something that is only used by attackers. It can be used to improve the security knowledge of employees in your organization. Traditional security awareness programs are often ad hoc (e.g., part-time effort, informal reporting and few, if any, metrics), with lean staffing and moderate spending.[4] The prevalence of ad hoc training programs reflects the low staffing and funding levels training programs receive. While severely lean staffing will persist for the foreseeable future, SRM leaders can expect to see GenAI improve the following existing capabilities in security training programs:

Advanced Social Engineering Campaigns

Organizations can create targeted training programs for each employee, based on their individual weaknesses and areas of improvement identified through data analysis. Data to consider includes:

- **Social engineering campaign results:** Analyzing employee performance during simulated phishing attacks can highlight specific vulnerabilities and areas needing improvement.
- **User behavior analytics:** Monitoring how employees interact with emails and links can reveal patterns that indicate susceptibility to campaign attempts.
- **Incident reports:** Reviewing past incidents of successful attacks within the organization can help identify common traits among affected employees.
- **Surveys and feedback:** Collecting feedback from employees about their experiences and knowledge can provide insights into their security behavior and culture aptitude.
- **Campaign history:** Evaluating previous training sessions and their effectiveness can guide the development of more targeted content.
- **Demographic data:** Understanding the roles and responsibilities of employees can help tailor campaigns to specific job functions that may be more vulnerable.

This approach ensures that employees receive the most relevant and effective training to enhance their resistance against phishing attacks.

Advanced social engineering campaigns utilize GenAI algorithms to automatically deliver microtrainings to employees in real-time, exactly when they are most susceptible to falling for a phishing attempt. These microtrainings are designed to engage employees and promote safe behaviors, such as recognizing phishing emails, avoiding suspicious links and reporting potential threats.

The use of GenAI in advanced social engineering campaigns not only improves the effectiveness of training programs but also saves time and resources for organizations. Instead of conducting generic and repetitive training sessions, GenAI-driven campaigns deliver personalized and dynamic content that adapts to the evolving threat landscape.

Furthermore, GenAI can continuously monitor and evaluate employee performance, providing ongoing feedback and recommendations for improvement. This feedback loop ensures that employees remain vigilant and proactive in their defense against phishing attacks.

Recommendation:

- Use GenAI to guide each employee on a unique path to improve their security behaviors. Advanced social engineering campaigns automatically deliver in-the-moment microtrainings to drive engagement and safe behaviors.

Hyperpersonalized Learning

Engagement levels are a key determinant of SBCP effectiveness. The more employees are motivated to engage with SBCP initiatives (training, communications etc.), the more likely they will be prepared to alter their behaviors and work practices — thereby helping to reduce employee-driven cybersecurity incidents. GenAI will enable SRM leaders to create hyperpersonalized learning material that speaks to each employee's unique requirements. By analyzing individual learner's strengths, weaknesses and learning styles, GenAI can create personalized training programs that cater to each employee's unique needs. This ensures that learners receive the most relevant and effective training materials, increasing their engagement and retention of security training behaviors.

One innovative approach GenAI employs to achieve personalized learning is through the enhancement of **role-based training**, leveraging user behavior analytics data sourced from existing security tools such as security information and event management (SIEM) systems and web application firewalls (WAF). By integrating this data with a commercial or internally developed LLM, GenAI can generate hyperpersonalized training material tailored to address an individual's specific deficiencies. This methodology ensures that employees receive cybersecurity knowledge and skills that are directly pertinent to their job functions.

By analyzing the specific challenges and risks associated with different roles within the organization, GenAI tools can craft training content that speaks directly to the recipient's unique context. This targeted approach not only increases engagement but also enhances the likelihood of behavioral adaptation, as employees perceive the training to be more relevant and applicable to their daily responsibilities.

For instance, consider a scenario in which a financial analyst within an organization frequently accesses sensitive financial data. User behavior analytics might reveal that this individual has a pattern of neglecting multifactor authentication (MFA) protocols. By integrating this behavioral data with an LLM, GenAI can generate training modules that emphasize the importance of MFA, provide real-world examples of breaches resulting from MFA lapses, and offer step-by-step guidance on implementing MFA effectively. This personalized training material would be far more impactful than generic cybersecurity training, as it directly addresses the analyst's specific vulnerabilities and the critical nature of their role.

Additionally, GenAI incorporates **segmented training** to account for the varying levels of cybersecurity knowledge and expertise among employees. GenAI can assess the proficiency of individuals and provide training materials appropriate for their skill level. This ensures that employees receive training that is neither too basic nor too advanced, optimizing their learning experience.

Whether it is for the entire organization or individuals who have previously undergone training, GenAI's hyperfocused personalized learning approach ensures has two main benefits:

- Employees receive training that is tailored to their specific needs and maximizes their learning potential.
- Allows the user to interact with an unbiased curriculum, reducing the risk of employee backlash to training, HR friction, and less resource intensive material planning.

Recommendation:

- Continuously assess and update the training materials based on individual learner's progress and feedback. By regularly evaluating the effectiveness of the training programs and incorporating learner feedback, GenAI can ensure that the personalized training remains relevant and impactful.

Metrics Collection and Reporting

Historically, training programs struggle to measure success. Measurable employee behavior change is the primary objective of the vast majority (84%) of training programs; yet, less than half (43%) of programs consistently measure employee behavior.4 GenAI can improve security training metrics and reporting in several ways:

Enhanced data analysis: GenAI can analyze vast amounts of security-related data, such as logs, incident reports and user behavior patterns to identify trends, anomalies, and potential risks. By processing this data more efficiently than traditional methods, GenAI can provide deeper insights into security incidents and help identify areas that require attention.

Natural language processing: GenAI can leverage natural language processing to analyze and understand security-related conversations, emails, or other textual data. This capability enables it to identify potential security risks, detect phishing attempts and provide real-time guidance to users, thereby improving overall security training and reducing the likelihood of security incidents.

GenAI's impact of specific cybersecurity training and cultures metrics to track include:

- Enhancing phishing detection to reduce susceptibility.
- Prioritizing and categorizing security service edge (SSE) and security information and event management (SIEM) alerts for more accurate insights.
- Analyzing web browsing behavior to decrease unsafe activity.
- Identifying patterns of deliberate security control avoidance.
- Monitoring and detecting unauthorized external storage device usage.
- Analyzing policies and configurations to reduce violations and misconfigurations.
- Assisting developers in identifying and remediating nonsecure code.
- Proactively identifying critical vulnerabilities in in-house applications.
- Providing recommendations to reduce security misconfigurations and rollback incidents.

Recommendation:

- Use cybersecurity outcome driven metrics to help inform and guide future engagements with targeted employees. Additionally, consult with the privacy office, legal and HR to conduct the necessary assessments to identify risks to employee privacy and implement appropriate mitigating measures.

GenAI Introduces New Possibilities for Generating Security Training Content

The integration of GenAI into traditional training programs introduces a range of new capabilities. These include processing large amounts of data quickly and efficiently, adapting and learning from new information, generating realistic content, and enhancing interactivity and engagement. As a result, GenAI significantly boosts the effectiveness and efficiency of traditional training programs, enabling them to better understand and respond to complex situations in real time. SRM leaders can expect to see GenAI create the following new capabilities:

GenAI Assist Chatbot for Cybersecurity

The primary use case for the GenAI Assist Chatbot is to enable cybersecurity teams to provide scalable guidance to application developers, business technologists and other internal or external stakeholders. This empowers them to make informed decisions regarding cybersecurity.

To effectively use the GenAI Assist Chatbot, it is important to have a well-defined security control environment and clear behavior expectations. This ensures that the guidance provided by the chatbot aligns with the organization's security policies and requirements.

One of the key benefits of using AI in cybersecurity is the speed and scalability it offers. The GenAI Assist Chatbot can help lower the barrier to entry for cybersecurity training and implementation, making it more accessible to a wider audience within the organization.

Overall, the GenAI Assist Chatbot has the potential to improve the adoption and implementation of cybersecurity training. By targeting the internal cybersecurity team and providing scalable guidance, it can empower employees to make more informed decisions regarding cybersecurity.

Recommendation:

- GenAI Assist Chatbot should be directed toward the internal cybersecurity team, specifically Business Information Security Officers (BISOs), analysts, and governance, risk, and compliance (GRC) leads. These individuals are experts in the field and can effectively interpret documents within the security ecosystem.

Interactive Attack Simulations

GenAI opens up opportunities to create more immersive attack simulation platform capabilities for security operation teams, executive management teams and other senior leaders. These GenAI-enhanced platforms enable organizations to improve cyber readiness, test incident response processes and playbooks, measure and track capabilities, and cultivate a skilled, aligned and confident security team. By leveraging realistic simulations of various security threats and attacks, GenAI-enabled attack simulation capabilities empower learners to actively participate and experience the real-time consequences of their actions, fostering a hands-on learning approach that reinforces the importance of security behaviors.

One of the key requirements for optimizing the use of this capability is having well-defined incident response and crisis management playbooks based on foreseeable risk scenarios. This ensures that organizations have a structured framework in place to effectively respond to security incidents and align their simulation exercises accordingly.

> *GenAI-enabled immersive attack simulation capabilities should test incident response playbooks, allowing security leaders to continuously validate and refine their incident response strategies through realistic scenarios.*

Recommendation:

- Leverage realistic simulations of various security threats and attacks. GenAI empowers learners to actively participate and experience the consequences of their actions, fostering a hands-on learning approach that reinforces the importance of security behaviors.

Figure 2 summarizes the key impacts of GenAI and the top recommendations for security and risk management leaders.

Figure 2. Impacts and Recommendations for SRM Leaders

Impact and Top Recommendations for SRM Leaders

Impacts	Top Recommendations
Threat actors exploit GenAI, enabling them to rapidly and continuously adapt their attack tactics.	Maintain focus to protect against evolving attack methods using AI capabilities.
GenAI is a double-edged sword — it improves operational outcomes but can also introduce new cybersecurity risks.	Expand the focus beyond static computer-based training and phishing campaigns by embracing GenAI to enable behavioral changes.
Traditional (or legacy) cybersecurity skills training falls short in addressing modern GenAI risks.	Augment the existing security behavior and culture program with GenAI tools to enhance the scalability and understandability of security guidance and expectations

Source: Gartner
816736_C

Gartner

Source: Gartner Research Note G00816736, Alex Michaels, Will Candrick, Richard Addiscott, Andrew Walls, Victoria Cason, 11 November 2024