The Human Factor in Cybersecurity: Turning Weaknesses into Strengths

eBook

WeActis
by Mondata

Empowering Employees to Strengthen Enterprise Security

The cybersecurity space has evolved, but one fundamental weakness persists: human behavior.

Traditional security awareness training often emphasizes compliance over **creating genuine, lasting change in employee actions.**

This ebook examines why conventional methods are inadequate and presents a strategic approach to transforming security awareness into a behavior-driven, risk-reducing practice.

What You will Learn

→ **Why Traditional Training Fails**

The limitations of compliance-based programs and their inability to drive long-term behavioral change.

→ **Understanding Human Error in Cybersecurity**

Cognitive overload, forgetfulness, and the necessity for behavioral monitoring.

→ **The Key to Effective Security Culture**

Strategies to personalize security education, provide real-time nudges, and align training with real-world scenarios.

→ **Actionable Frameworks for CISOs and CTOs**

Metrics that matter, gamification techniques, and engagement strategies to build a proactive security-aware workforce.

By adopting these recommendations, security leaders can move from mere checkbox compliance to a sustainable security culture in which employees are empowered to actively participate in risk reduction.

The Shift in Cybersecurity: from Compliance to Behavioral Change

The cybersecurity landscape has experienced a significant transformation in recent years. As organizations of all sizes confront high-volume and fast-paced cyber threats, the need for robust, proactive cybersecurity measures has become increasingly clear. Simultaneously, the shortage of skilled cybersecurity professionals has prompted businesses to reevaluate their approach to risk management and concentrate more on **empowering their workforce to act as a line of defense.**

Despite the mounting threats, one critical gap remains: employee behavior.

69%

A 2024 Gartner survey found that **69% of employees ignored or bypassed their organization's cybersecurity protocols in the past year**, and 74% would willingly bypass them if it served a business purpose.

This statistic reveals a critical flaw in conventional training methods emphasizing knowledge acquisition without sufficiently changing behaviors.

The problem isn't simply a lack of knowledge.

This is a deeper, systemic issue: the failure to instill long-term behavioral changes in how employees engage with IT and its cybersecurity counterpart. Organizations must move away from traditional compliance-based programs toward **strategies that cultivate genuine, sustainable cybersecurity habits.**

Chapter 1

The Current State of Security Awareness Programs

The Rise of Compliance-Driven Training

For years, security awareness programs have been designed to meet compliance requirements imposed by regulations and frameworks such as GDPR, HIPAA, ISO 27001, and SOC 2. While these requirements have played a crucial role in standardizing and accelerating cybersecurity practices, they have inadvertently pushed organizations to emphasize audit readiness over creating meaningful change.

A culture of compliance is not synonymous with a culture of security.

Compliance-based training typically adheres to a rigid, one-size-fits-all model, requiring employees to complete designated modules or pass a series of tests to meet compliance standards. Unfortunately, these initiatives often disconnect from the real-world challenges employees face daily. These programs seldom integrate contextual relevance or motivate employees to apply their knowledge to actual threats, leaving them unprepared when confronted with genuine cyber risks.

While these programs can assist organizations in meeting regulatory requirements, they have not effectively promoted a resilient cybersecurity culture. Compliance-focused programs often lack personalization, which leads to **employee disengagement.**

Traditional Training Methods
What's Missing?

While traditional awareness training methods are widespread, they have proven inadequate in addressing the root causes of security incidents.

Common practices include:

Digital Learning Modules

These flexible, asynchronous training modules enable employees to complete them remotely, providing convenience. However, they often place too much emphasis on abstract concepts and tend to overlook the connections between theoretical knowledge and practical real-world scenarios.

Phishing Simulations

While phishing simulations are a common approach to evaluating susceptibility to email-based attacks, they frequently emphasize testing employees' skill in recognizing scams without considering the underlying behavioral tendencies that contribute to risky actions initially.

Awareness Campaigns

These campaigns aim to highlight specific security themes, such as password policies or phishing threats, but they tend to be sporadic and lack ongoing reinforcement, which diminishes their long-term impact.

Environmental Cues

Visual reminders like posters or digital signage aim to reinforce security practices. However, they tend to be passive, and employees often overlook them after becoming accustomed to the environment.

Despite widespread use, these methods often fail to produce long-lasting behavioral change. Employees may pass a course or even complete a phishing simulation, but without context or ongoing reinforcement, they are unlikely to implement what they've learned in real-world scenarios.

The Limitations of Traditional Approaches

Persistent Human Error

Human error continues to be one of the biggest contributors to **cybersecurity breaches**. Even with thorough training programs established, employees still make mistakes that jeopardize their organization's security posture. This is partly due to the shortcomings of traditional training methods, which do not consider the complexities of human behavior.

A National Institute of Standards and Technology (NIST) study found that 84% of organizations measure success based on course completion rates and phishing test outcomes.

While these metrics are useful for tracking training participation, they are **unreliable indicators of actual behavioral change.** Success should be assessed by how employees respond when confronted with a potential threat—not simply by whether they click on a phishing link during a test.

84%

of organizations measure success based on course completion rates and phishing test outcomes.[1]

[1] National Institute of Standards and Technology (NIST) study titled "Measuring the Effectiveness of U.S. Government Security Awareness Programs."

Cognitive Overload and Forgetfulness

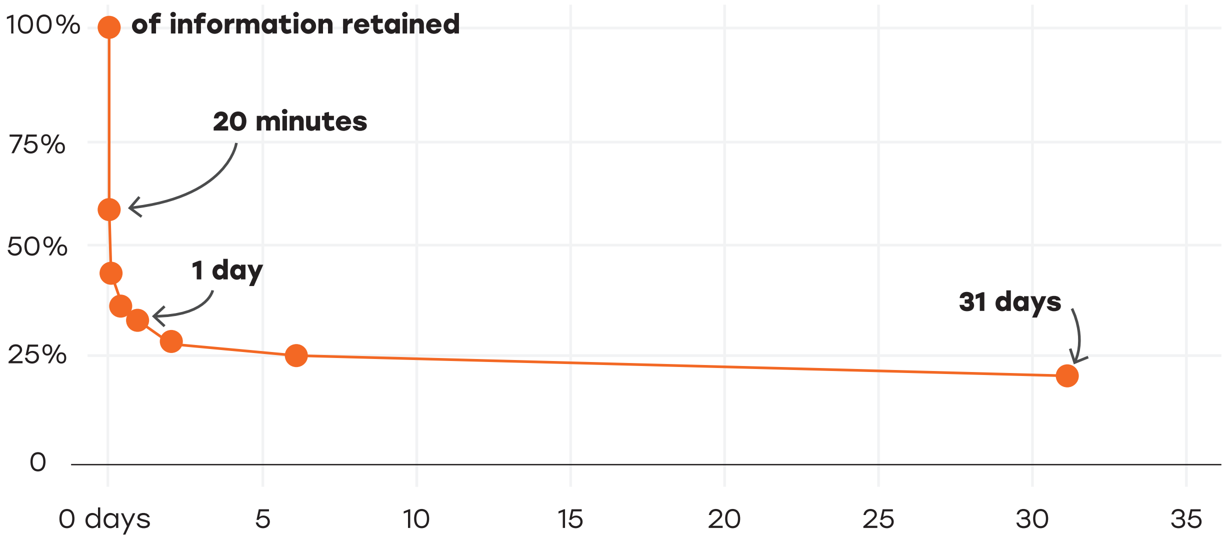
The Ebbinghaus forgetting curve[2] is an established concept in cognitive science that **illustrates how quickly information can be forgotten over time, particularly without reinforcement.**

Traditional training methods usually offer one-time sessions, resulting in employees retaining and applying much information without additional reinforcement. This can cause information overload, leaving employees overwhelmed by a flood of information without sufficient time or space to absorb and retain essential concepts.

Furthermore, without regular updates or reminders, employees quickly forget the security protocols they learned, rendering the initial training session nearly irrelevant after a short time.

Research suggests that **80% of learned information can be forgotten within a month** without regular reminders.

Hermann Ebbinghaus' forgetting curve



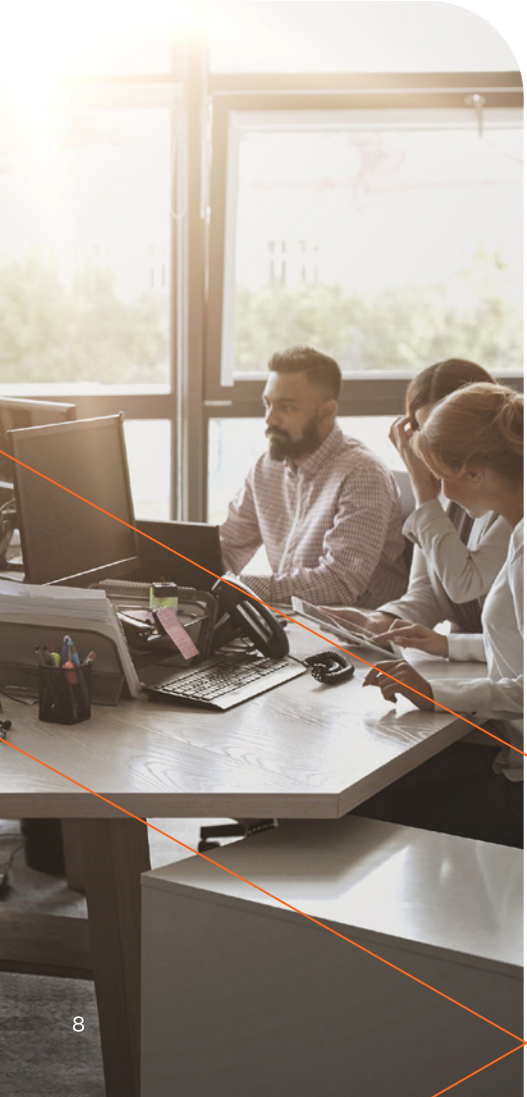
[2] Ebbinghaus Forgetting Curve (Definition + Examples) - Practical Psychology

Lack of Behavioral Monitoring

Another significant shortcoming of traditional security awareness programs is **the absence of post-training monitoring.** After finishing a course or phishing test, employees are frequently not evaluated continuously regarding how they implement their knowledge in practice.

For instance, if an employee completes a security training course yet continues to use weak passwords or disregards multi-factor authentication recommendations, the lack of post-training behavioral assessments means that organizations do not have insight into these practices.

Behavioral monitoring can provide **valuable insights** into whether employees genuinely follow secure practices and help pinpoint areas that need further training.



Disconnect from Real-World Scenarios

Traditional training methods often fall short because **they lack real-world context.** Abstract, theoretical lessons or static materials, such as slideshows and posters, do not resonate with employees. Security awareness is more effective when practical training is rooted in real-world scenarios.

For example, employees are more likely to remember security protocols when they learn through scenario-based exercises that reflect the challenges they encounter in their daily roles. This approach engages them more thoroughly and provides them the opportunity to **practice making the right decisions in a low-risk environment** before implementing those decisions in high-risk situations.

Strategic Recommendations for Security Leaders

Security leaders need to go beyond traditional security awareness programs and adopt a behavior-driven, data-informed strategy for risk reduction. Achieving lasting change involves improving how security success is assessed, tailoring security education, and providing practical, engaging solutions that promote long-term employee participation.

1

Refined Metrics

Shift from Compliance to Behavioral and Meaningful Indicators

Traditional security awareness programs frequently gauge success by tracking completion rates, phishing click rates, or the quantity of reported incidents. Although these metrics offer a basic perspective on engagement, they fail to evaluate changes in behavior or monitor the ongoing enhancement of security practices. **Security leaders should focus on:**

→ **Behavioral Security Metrics**

Rather than just monitoring completion rates, gauge how frequently employees implement security principles in practical scenarios, including:

- The rate of secure file sharing on cloud services.
- Growth in the number of employees utilizing robust authentication measures (MFA, password managers, or other available tools).
- Decrease in policy violations over time (e.g., fewer data misconfigurations in M365).

→ **Adaptive Risk Scoring**

Establish a risk scoring model that adapts based on employee behavior over time. For instance, employees who consistently report phishing emails and follow security protocols should be categorized as low-risk. At the same time, someone who often circumvents policies may require targeted training and could represent a greater risk.

→ **Contextualized Risk Management**

Utilize behavioral analytics to produce department-specific insights, enabling security teams to pinpoint high-risk areas and customize security interventions.

2

Contextualized Security Education

Make Cybersecurity Relevant and Actionable

Employees are more likely to embrace security when it feels **directly relevant to their daily work.** Rather than generic training, security leaders should implement:

→ **Role-Based Security Guidance**

Security training should be tailored to specific job roles and practical scenarios.

- **Finance teams:** Recognizing social engineering in invoice fraud.
- **HR teams:** Identifying insider threats and safeguarding PII (Personally Identifiable Information).
- **IT/Admins:** Reducing misconfigurations in cloud environments.

→ **Just-in-Time Security Nudges**

Instead of relying on annual training, provide real-time security guidance within workflows.

- **Example 1:** If an employee is about to share a sensitive document externally, trigger an in-app security alert with best practices.
- **Example 2:** When an employee forgets to enable MFA, prompt a quick walkthrough explaining why and how to fix it.

→ **Simulated Incident Response Exercises**

Go beyond static phishing simulations and implement interactive tabletop exercises where employees can practice decision-making under pressure in real-world cyber threat scenarios.

3

Actionable Engagement

Encourage Employees to Participate in Security

To cultivate a security-conscious culture, organizations must **empower employees** by providing opportunities to engage in security actively, beyond just passive training.

→ **Security Champions Program**

Identify and train internal security advocates across various departments who can promote security best practices among their peers.

→ **Gamification & Incentives**

Implement engaging challenges, leaderboards, and rewards for employees who exhibit proactive security behaviors (e.g., highest phishing detection rate, most security recommendations implemented). Some organizations have begun gradually incorporating these new metrics into employee scorecards and reviews.

→ **Employee-Driven Threat Intelligence**

Motivate employees to report security incidents and provide feedback loops that show how their contributions help reduce risks efforts.

By refining metrics, contextualizing security education, and providing engaging, actionable solutions, security leaders can **create a sustainable culture of security** where employees are active participants in risk reduction rather than passive training recipients.

Key Takeaways

Traditional training is ineffective → Compliance-focused programs raise awareness but fail to change behavior.

Behavioral change is essential → Employees require reinforcement, real-world context, and ongoing engagement.

Measuring security success demands new metrics → Shifting from completion rates to behavioral indicators demonstrating tangible security improvements.

Personalization boosts effectiveness → Role-based training, real-time nudges, and adaptive learning enhance engagement.

Engagement fosters cultural change → Security must be integrated into daily workflows through gamification, incentives, and peer-driven programs.

Concrete Actions to Start With

1 **Reassess Your Security Training Approach**

Audit your current program to identify gaps in behavioral reinforcement.

2 **Implement Behavioral Metrics**

Track security habits, not just training completion rates.

3 **Introduce Real-Time Security Nudges**

Provide in-app prompts when employees engage in risky behaviors.

4 **Launch a Security Champions Program**

Empower employees to advocate for departmental security.

5 **Gamify Security Engagement**

Utilize leaderboards, challenges, and incentives to promote proactive security behavior.
Make it fun!

About WeActis

WeActis revolutionizes cybersecurity by turning employees into active defenders and making security a shared responsibility rather than an IT burden.

Integrated into Microsoft Teams, it seamlessly embeds security into daily workflows, guiding employees to mitigate risks in under five minutes per week.

By improving data hygiene in Microsoft 365, strengthening governance, and streamlining risk reduction, **WeActis** helps organizations build a Cybersecurity Resilience Culture–enhancing compliance, reducing data exposure, and driving measurable, lasting security improvements.

info@weactis.com
1-833-666-3282
WeActis.com

WeActis
by Mondata