KARYSBURG

SECURITY MISBEHAVIOR

THE HIDDEN THREAT TO DIGITAL TRANSFORMATION

TABLE OF CONTENTS

THE HUMAN FACTOR IN CYBERSECURITY

Digital transformation has revolutionized business operations, but it has also amplified an often-overlooked vulnerability: security misbehavior. This occurs when employees—whether through negligence, lack of awareness, or manipulation—engage in actions that compromise security, such as:

- Clicking phishing links
- Misconfiguring cloud services
- Reusing weak passwords
- Bypassing security protocols

Key Stat: About 60% of breaches involve human error, according to Verizon's 2025 Data Breach Investigations Report. Even with advanced cybersecurity defenses, a single employee mistake can lead to catastrophic breaches. For example, in 2024, the Change Healthcare ransomware attack—the largest medical data breach in U.S. history—stemmed from compromised credentials, exposing data for 190 million people.

Technology alone cannot mitigate human risk. Organizations must adopt human-centric security strategies that account for behavioral vulnerabilities.

DIGITAL TRANSFORMATION’S DILEMMA

While digital tools enhance productivity, they introduce new attack vectors. Digital transformation expands the attack surface, requiring continuous monitoring and adaptive security policies. Take a look at the table below:

Risk Factor	Impact	Example
Remote Work	67% of breaches target remote workers due to weaker endpoint security and unsecured networks.	HiatusRAT malware (2024) exploited vulnerable web cameras and DVRs, primarily affecting remote workers.
Cloud Misconfigurations	23% of cloud security incidents originate from misconfigured cloud storage, APIs, or SaaS settings.	Blue Yonder (2024) suffered a ransomware attack due to supply chain vulnerabilities, disrupting payroll systems for US Starbucks and UK supermarkets.
Supply Chain Attacks	Third-party breaches can cascade across multiple organizations.	MoveIt vulnerability (2023) impacted thousands of businesses via a single compromised file-transfer tool.

TOP CAUSES OF BREACHES

(2025 Data)

- Ransomware (35%) – Ransomware attacks surged 84% year-over-year, heavily targeting SMBs (70% of cases). North America saw a 15% increase, even as EMEA experienced a drop.
- Phishing (40% of email threats) – Phishing skyrocketed by over 1,200%, fueled by generative AI. Half of business email compromise (BEC) incidents used spear phishing links.
- Cloud Attacks (75% rise in intrusions) – Misconfigurations caused 23% of cloud breaches, with over half involving stolen credentials via phishing.
- Device Exploits – Attackers now leverage edge and IoT devices as stealth entry points. Alarmingly, only 4% of organizations rate these assets as secure.
- DDoS Attacks (31% increase) – DDoS campaigns averaged 44,000 attacks per day in 2023. Despite law enforcement takedowns of attack services, the volume remains relentless.

CASE STUDIES

Company	Attack Vector	Impact
Twitter (2020)	Social engineering via fake login pages	$118K in Bitcoin scams
Robinhood (2021)	Employee tricked into granting access	$20M settlement
Twilio (2022)	Smishing (SMS phishing)	Employee credentials stolen
Change Healthcare (2024)	Ransomware via stolen credentials	190M records exposed

Security misbehavior is not just about ignorance. It's about exploiting human psychology.

WHY SOCIAL ENGINEERING WORKS

Psychological Triggers Hackers Exploit

- **Fear** ("Your account will be locked!")
- **Urgency** ("Wire transfer needed NOW!")
- **Curiosity** ("Click to see your bonus!")

Why Traditional Training Fails

- **Information overload** – Annual compliance training is forgotten quickly.
- **Mistrust** – Simulated phishing tests feel like traps.
- **Evolving tactics** – Attackers now use AI-generated deepfake voice calls (vishing).

A Better Approach

- **Hyper-personalized simulations** (e.g., finance teams receive BEC scam tests).
- **Two-way reporting** (employees flagging and reporting suspicious activities).
- **Behavioral AI** detects anomalies in real-time.

format string:
format string:
Press any key to continue . . .
is used for the IFormatProvider:
with digit group size = 2 and
1,18,76.54
1,187654E+004

BEYOND EMAIL PROTECTION

While email security is critical, attackers exploit alternative channels. This includes:

- **Smishing (SMS phishing)** – Fake texts impersonating banks or IT support.
- **Vishing (voice phishing)** – AI-generated deepfake calls mimicking executives.
- **Social media scams** – Fake job offers or malware-linked ads.

For example, in 2024, attackers used fake Google ads to distribute DeerStealer malware via a fraudulent Google Authenticator app.

A better solution would be to deploy an integrated threat detection tool that extends protection beyond emails to collaboration tools.

A MULTILAYERED SOLUTION

Layer	Strategy	Example Tools
People	Role-based training, phishing simulations	Brightside AI (personalized risk scoring)
Processes	Approval workflows, change management	ServiceNow (automated security workflows)
Technology	Behavioral AI, UEBA, Zero Trust	CrowdStrike Falcon (endpoint detection)

It is important to assume that humans will make errors so that safeguards can be built to catch mistakes before they escalate.

SECURING THE FUTURE OF WORK

To mitigate security misbehavior:

Train smarter

Use AI-driven microlearning to enhance cybersecurity awareness and ensure continuous staff training.

Automate checks

Deploy AI-powered SIEM (Security Information and Event Management) tools to detect anomalies.

Monitor behavior

Implement UEBA (User and Entity Behavior Analytics) tools to flag unusual activities.

It is important to know that a single breach can undo years of digital progress. Proactive, human-centric security is no longer optional. It’s now a business imperative.

CHECKLIST

For Employees:

✓ Report suspicious emails/texts immediately.
✓ Use password managers and authentication apps.
✓ Verify unusual requests (e.g., wire transfers) via a secondary channel.

For IT Teams:

✓ Conduct monthly phishing simulations.
✓ Enforce DMARC/DKIM for email authentication.
✓ Deploy behavioral AI (e.g., Vectra Cognito).

For Leadership:

✓ Fund role-specific security training.
✓ Implement 3-person approval for high-risk transactions.
✓ Review incident response plans annually.

CONCLUSION

Security misbehavior is the Achilles' heel of digital transformation. While technology can block attacks, human behavior determines resilience. By adopting AI-driven training, behavioral monitoring, and Zero Trust policies, organizations can reduce risk without stifling innovation.

Next Steps:

- Assess your human risk exposure (e.g., digital footprint analysis).
- Upgrade from compliance-based to behavior-based training.
- Integrate AI-powered threat detection across all channels.

The future of cybersecurity isn't just about firewalls. It's about fostering a culture of vigilance. And this is part of what we do at **Karysburg**.

ABOUT KARYSBURG

Karysburg is a cybersecurity partner built for today’s threat landscape. In a world where breaches are inevitable and supply chain risks keep growing, we help businesses stay one step ahead.

Our approach goes beyond defense and empowers growth through proactive, intelligent security. With deep expertise and a relentless focus on protection, Karysburg gives you the clarity, resilience, and confidence to thrive in an age of uncertainty.

We do more than secure systems; we strengthen the foundation of your business. When you partner with Karysburg, you gain more than protection , you gain peace of mind.

☎ (704) 740-1641
🌐 WWW.KARYSBURG.COM
✉ CONTACT@KARYSBURG.COM
📍 HUNTERSVILLE, NC, US