5 Common Cybersecurity Mistakes Financial Institutions Overlook — and How to Fix Them

SBS CyberSecurity

sbscyber.com

Table of Contents

Cybersecurity risk management isn't just an IT issue —

it's a business necessity with real impact.

Introduction

When overlooked or mismanaged, cyber risks can lead to serious consequences such as regulatory fines, operational downtime, and loss of market share, affecting every part of your organization. Yet too often, even well-intentioned teams fall into traps that weaken their defenses and create blind spots in their risk management efforts.

This guide breaks down five of the most common cybersecurity challenges financial institutions face and how to address them with practical, expert-backed strategies. Whether you oversee cybersecurity, manage compliance, or guide strategy, these insights will help you address persistent risks before they become costly problems.

MISTAKE #1

Combining IT and Information Security Roles Under One Person

In many institutions, a single individual may be responsible for administering the network, developing cybersecurity strategy, performing risk assessments, responding to incidents, and writing policies. While this structure may seem efficient, it limits institutional growth and introduces serious operational challenges, especially around segregation of duties. If the same person is both implementing and auditing controls, who is left to provide a credible challenge?

Why It Matters

When one person is responsible for both implementing IT changes and ensuring their security, it creates a conflict of interest.

Strategic functions like risk assessments and board reporting often take a back seat to operational demands.

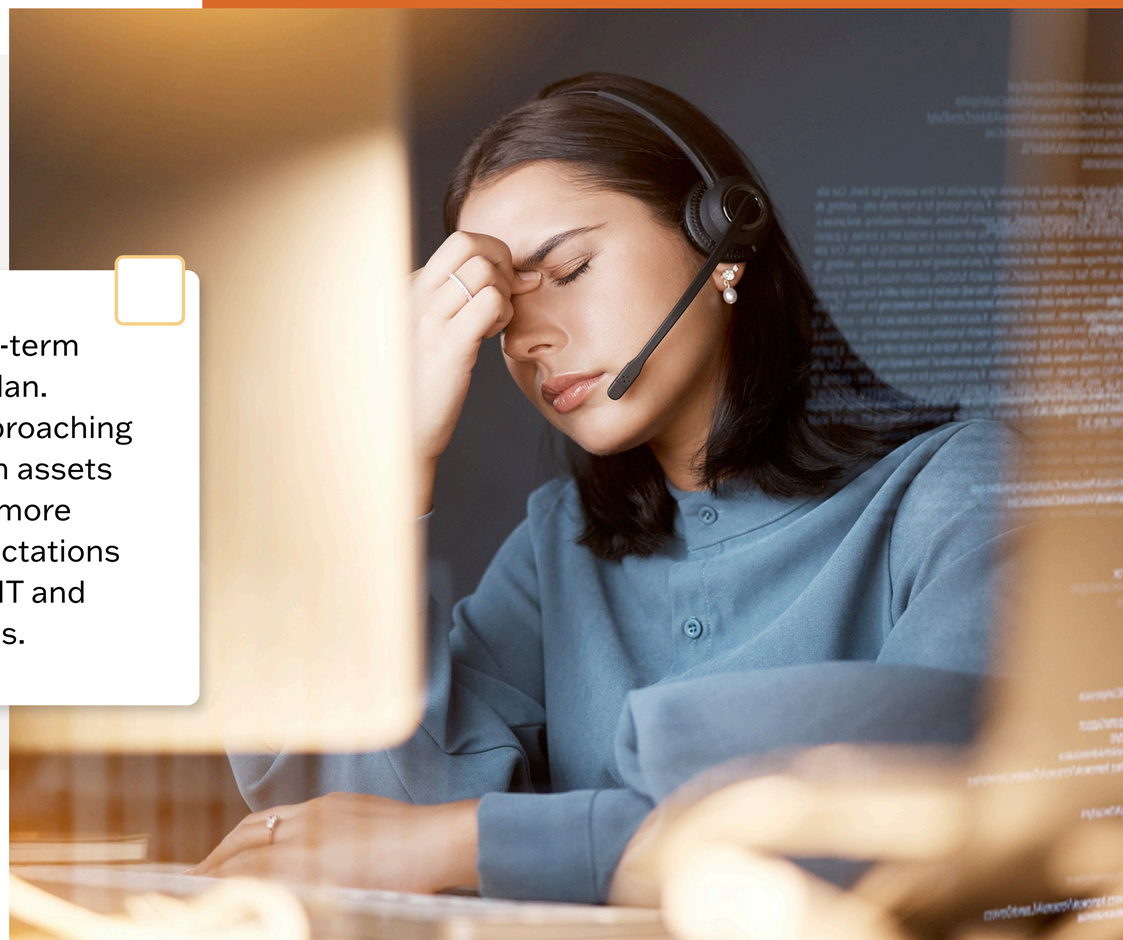
More than 750,000 cybersecurity roles remain unfilled in the U.S. in 2025, leading to widespread understaffing (ACSMI, 2025).

How to Fix It

Clarify who owns IT operations and who is responsible for information security — they should be distinct roles. After all, you wouldn't expect a loan officer to also calculate the loan loss reserve.

Fill leadership gaps through internal reassignment or by engaging a virtual chief information security officer (vCISO) to provide guidance on security strategy, governance, and oversight.

Build a long-term staffing plan. Institutions approaching $500 million in assets are seeing more examiner expectations to separate IT and ISO roles.



MISTAKE #2

Building a Disconnected Security Program

When audit findings arise, it's tempting to plug the gap with a new tool — one for vendor reviews, another for IT risk, and yet another for business continuity. Over time, your security program becomes a patchwork, and leadership loses visibility.

Why It Matters

- Inconsistent scoring across disconnected tools undermines board and auditor trust.
- Employees waste time reconciling siloed data instead of managing real risk.
- Core tasks like patch management slip through the cracks in fragmented systems.

How to Fix It

- Consolidate risk activities into a unified governance, risk, and compliance (GRC) platform.
- Standardize vendor management, business impact analysis, and IT risk processes.
- Choose solutions that automate scoring and offer executive-level reporting.

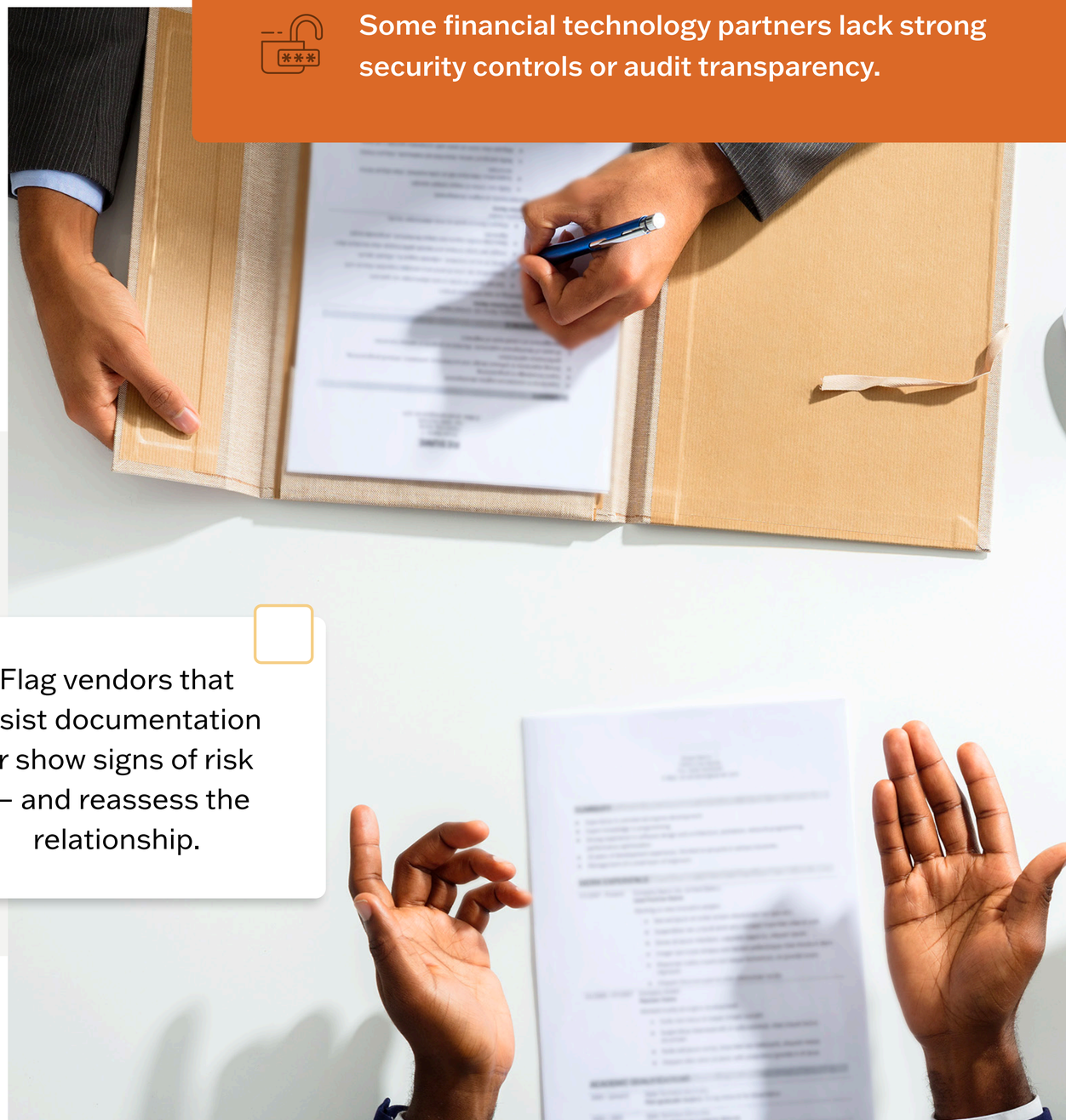
MISTAKE #3

Underestimating Third-Party Vendor Risk

You've likely outsourced everything from digital banking to cloud infrastructure. But are those vendors truly secure? Too often, vendor management is treated as a one-time compliance task.

Why It Matters

- Nearly a third of data breaches involve third-party vendors (Verizon, 2025).
- Missed renewal windows can lock in risky or underperforming providers.
- Some financial technology partners lack strong security controls or audit transparency.



How to Fix It

- Conduct risk-based vendor due diligence during vendor selection, not as a post-onboarding checkbox.
- Use tools to track contract terms, service-level agreements, and vendor financial health.
- Flag vendors that resist documentation or show signs of risk — and reassess the relationship.

MISTAKE #4

Treating Cybersecurity as a Technical Problem Instead of a Business Risk

Cybersecurity doesn't just affect your network. It impacts customer trust, compliance posture, and long-term growth. When it's viewed as only an IT issue, it's often underfunded and disconnected from business priorities.

Why It Matters

- Boards may lack context to evaluate cyber risk alongside financial priorities.
- Without executive support, security becomes reactive instead of proactive.
- Cyber investments often miss the mark when they're disconnected from business goals.

How to Fix It

- Involve ISOs and CISOs in strategic planning and board-level conversations.
- Use risk quantification to tie security threats to business impact.
- Help board members understand their cybersecurity oversight responsibilities and the risk of inaction.

MISTAKE #5

Failing to Build a Cybersecurity-Aware Culture

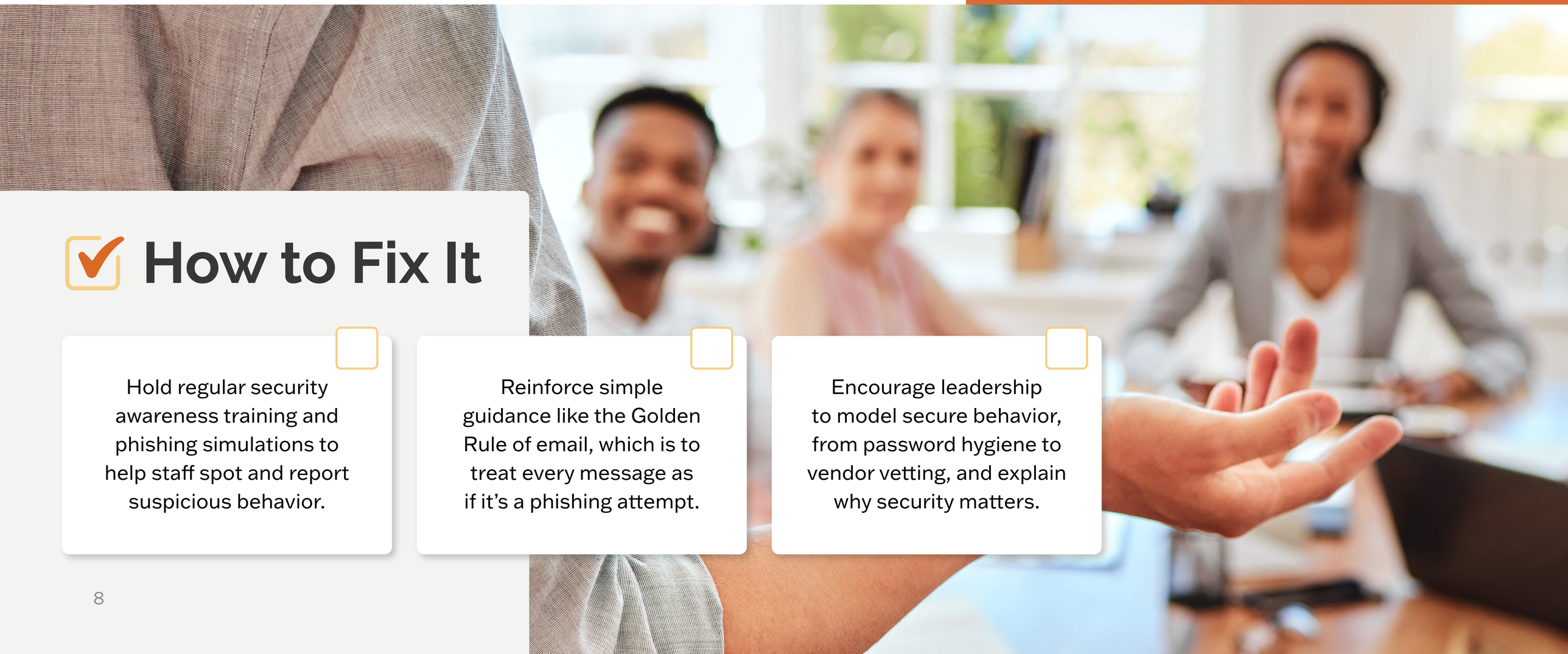
You can have the best tech stack in the industry and still suffer a breach because someone clicked a link. A strong security culture starts with leadership and carries through every employee interaction.

Why It Matters

Human error drives 60% of breaches, with phishing as a major factor (Verizon, 2025).

In Q1 2025, more than 30% of global attacks targeted banks and payment platforms (APWG, 2025).

Without leadership modeling secure behavior, culture initiatives lose traction.



How to Fix It

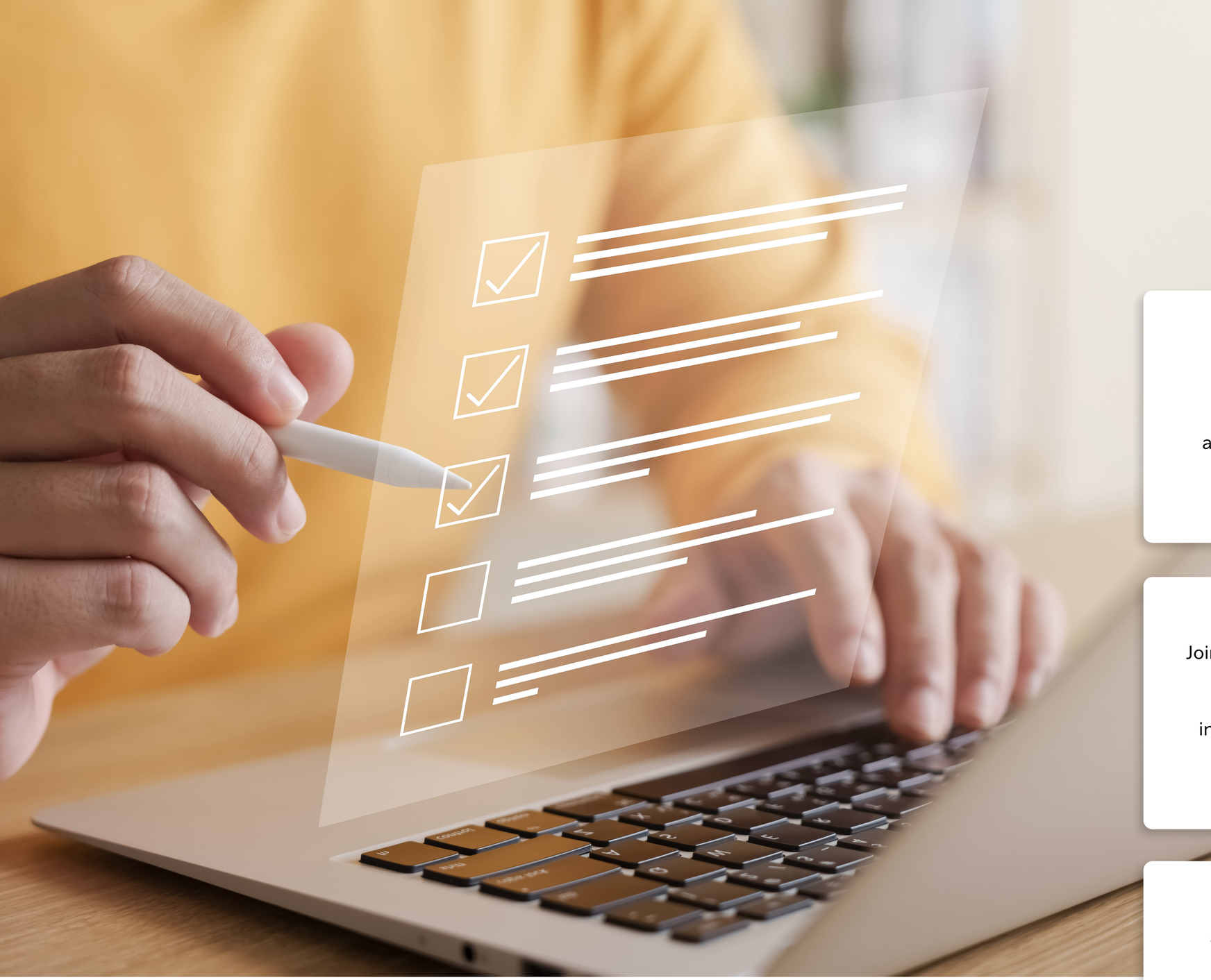
- Hold regular security awareness training and phishing simulations to help staff spot and report suspicious behavior.
- Reinforce simple guidance like the Golden Rule of email, which is to treat every message as if it's a phishing attempt.
- Encourage leadership to model secure behavior, from password hygiene to vendor vetting, and explain why security matters.

Strengthen Your Institution's Cyber Risk Posture

Avoiding these common cybersecurity mistakes isn't about spending more — it's about structuring smarter, leading proactively, and aligning your resources with real business risk.

Want to know where your institution may be exposed? Contact our cybersecurity experts to start building a stronger, more resilient program.

link.sbscyber.com/contact



Additional Resources

Hacker Hour

This interactive webinar series explores timely cybersecurity topics, emerging threats, and best practices. Each free session invites participants to ask questions, share ideas, and join the conversation around real-world cyber risks.

link.sbscyber.com/hackerhour

Cyber Showcase

Join this free monthly webinar that breaks down complex cybersecurity concepts into practical, actionable insights. Each edition highlights SBS services, introduces new tools, and gives attendees the chance to ask questions and connect with our experts.

link.sbscyber.com/cybershowcase

SBS Institute

Strengthen your institution's cybersecurity posture with on-demand training and certifications tailored for executives, managers, and technical teams. Prepare your team to manage threats, meet regulatory expectations, and speak confidently with examiners.

link.sbscyber.com/certs

SBS CyberSecurity

sbscyber.com