SBS CyberSecurity

You Are a **Technology Company**

Jon Waldman
President, Partner, and Co-Founder
SBS CyberSecurity, LLC

That's Right! **Yes, You.**

The original version of this eBook was drafted in 2018, but its message and ideas ring even more true today than at the time of its first publication. Since then, the world has endured a major pandemic (COVID-19), entered a remote-work revolution, migrated most networking workloads to cloud computing, watched autonomous vehicles move closer to daily reality, continued to invest in cryptocurrency and blockchain, and jumped aboard the next technological revolution — AI. On the horizon sits quantum computing, which promises to upend how we use technology altogether. So much has changed, yet so much remains the same.

As the world marches full steam ahead into the next wave of technological advances, and as your organization reviews its strategic plans for the coming years, pause for a moment to evaluate how you use technology as a core component of your business. Let's be honest — most organizations have moved beyond simply using technology to support the services we provide to customers. Today, we are technology companies first, with our specific services built upon that foundation.

Think of it this way: If most of your day-to-day operations involve technology, especially customer interactions — whether it's your website, a customer relationship management system (CRM), online banking, mobile payments, apps, email, or smartphones — then **you are a technology company.**

Another way to reality-check yourself is to ask this big question: "If all of the technology at our organization suddenly stopped working for an extended period of time, could we still do business effectively and serve our customers?" For most, the answer is a resounding "no." The reality of today's business world is that nearly all organizations, regardless of scale, rely heavily on technology, and without it, we would essentially be unable to conduct business long-term.

"If all of the technology at our organization suddenly stopped working for an extended period of time, could we still do business effectively and serve our customers?"

Focus on the Customer

We often hear that technology — especially information security — is regarded solely as an expense to a business's bottom line, but it's time to change that perspective. Gone are the days when getting a customer to enter your physical location and agree to a handshake deal was the best way to do business. That's not to say forming relationships with your customers isn't important. In fact, it's as important as ever, if not more so. However, many businesses romanticize this notion to the point that they let the "old way" of doing business interfere with what customers really want in today's market: simple, convenient, and time-saving ways to do business with you.

Time is the top currency organizations trade on today — not because customers are lazy but because everyone is extremely busy. Look at some of the largest companies in the world today (by market cap). Of the top 10, most are technology-focused, including Microsoft, Apple, NVIDIA, Amazon, Meta, and Google.

Amazon has won and will continue to win, even though not everything you buy on Amazon is the lowest possible price. Amazon succeeds because the service allows you to purchase nearly anything you want, anytime you want it, on any device you want, and it's delivered directly to you with free two-day shipping (well, mostly). It's simple, convenient, and saves time. Amazon also started a side project to rent out its additional computing power back in 2003. That project became Amazon Web Services (AWS), which now generates more than $100 billion in revenue with profits much greater than Amazon's e-commerce platform. (By the way, Amazon considers itself a technology company, not an online retailer.)

Microsoft has always been a technology company, which isn't surprising since what Microsoft produces (software) is purely technology-based. However, Microsoft has doubled its annual revenue since 2018 with the massive adoption of its Microsoft 365 (M365) platform. M365 now serves more than two million companies globally that have converted their day-to-day operations to Microsoft's cloud-based platform. Microsoft (and Amazon) are among the driving forces behind the shift to the cloud, where today's newest technologies live — along with today's biggest threats and next-generation security controls. Organizations are no longer developing new technologies to live on traditional, on-premises networks. Even Microsoft is slowing development for traditional platforms. (Can you even buy an on-premises version of Microsoft Office anymore?)

Then there are all of today's new "tech" companies: fintech, biotech, agtech, traveltech, edtech, and so on. Remember when you had to go to Best Buy, buy a box of software on floppy disks or CDs, and manually install it on every device? No one wants that today. We want to access what we need from our smartphones or laptops, typically while on the go. We want fast, next-gen technologies that allow us to do what we need faster from anywhere. These technologies live in the cloud.

The most important reason we highlight the tech companies that continue to win and "disrupt" the industry is that today's marketplace focuses primarily on the customer and their experience. Ask yourself the same burning questions that today's technology companies ask:

- How can we improve our customer experience?
- How can we save our customers time and simplify their experience?
- Are we providing our customers with fast, convenient options for completing their tasks?

Playing the Long Game

Today's banking market, like the tech industry, is customer-focused and customer-driven. If your institution doesn't provide the products and services customers want and need, they will find another institution that does. According to Consumer Affairs, the average U.S. consumer had accounts at more than five financial institutions in 2024. Consumers also used about 14 financial apps on average to invest, manage multiple banking accounts, budget their finances, and more. (Source: Consumer Affairs)

For a financial institution to remain viable, revenues must be sustainable and continue to grow. There are primarily three ways to grow revenues:

1. Acquire new customers.

2. Acquire another financial institution (to gain customers).

3. Get more revenue from existing customers.

With the widespread adoption of online banking, a consumer can open an account with virtually any financial institution via the web or a mobile app in just a few minutes. If your customers take their money elsewhere because your institution isn't meeting their needs, you're in trouble.

So, what should your institution do?

Focus on the customer!

Institutions that provide simple, convenient, and time-saving digital banking solutions will win in the long run. Fortunately, there are many ways to accomplish this objective today. Mobile banking platforms have become increasingly robust. If your mobile platform isn't keeping up with your institution's or your customers' needs, it might be time to consider alternatives.

Additionally, there's no shortage of fintech partners available to integrate into your ecosystem. Many financial institutions have adopted a fintech-centric approach to meeting customer needs by partnering with a variety of apps and integrating them into their mobile banking platforms. However, fintech partners require strong vendor management and due diligence to ensure both the security of the data being shared (it's your responsibility to protect customer information no matter who stores, transmits, or processes it) and the long-term viability of the product (many fintechs are acquired or fail, so make sure you're confident in the sustainability of any app you offer customers).

Another way to evaluate your institution's sustainability is to understand your ability to retain your youngest customers. While customers ages 25–44 are prime acquisition targets — because that's when customer spending takes off — it's not as simple as targeting this age group. By the time a customer reaches 25, they've typically already chosen their primary financial institution — the one where they hold most of their money, receive paycheck direct deposits, and handle their spending. Switching primary institutions today isn't impossible, but it's inconvenient, especially with automatic bill payments. The most common reason customers switch is another institution offering more simplicity, convenience, and time savings for everyday banking needs. Better rates help, but fees — and especially the absence of them — are now one of the strongest factors driving customers to switch institutions, according to The Financial Brand. Focusing on younger generations now allows you to provide the simple, convenient, and time-saving experiences they want. (Source: The Financial Brand)

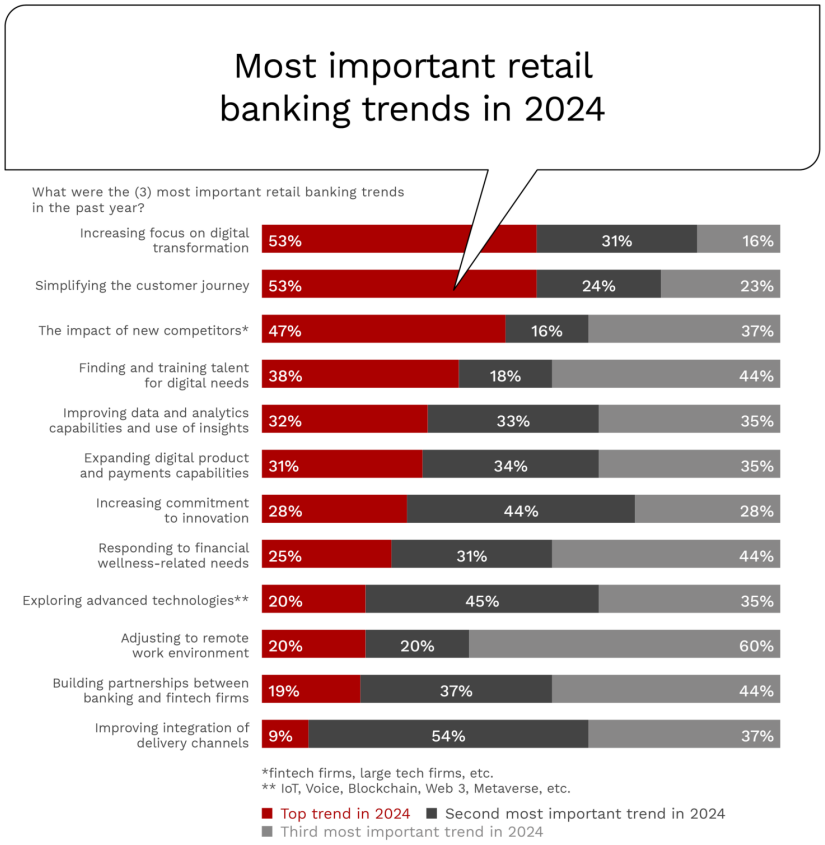
Nearly everyone under 30 is technology- and mobile-savvy, and they expect services to be technology-based. Offering products and services that appeal to younger customers will make it far easier (and more cost-effective) to retain them during their prime-spending years than trying to acquire them after they've established relationships with other institutions.

While your efforts to acquire younger customers should be a strategic priority, don't ignore your long-term customers. Here's the secret: 99% of consumers over 50 own a tablet, laptop, or desktop device, and they're the fastest-growing segment of digital product users. In fact, according to the American Bankers Association, more than 75% of all banking customers access their accounts via online banking or mobile apps. Don't let long-term customers become an excuse not to embrace digital products and services. They want simplicity, convenience, and time savings as much as anyone.

Source: American Bankers Association

Banking Trends for 2025 and Beyond

According to The Financial Brand, the top trends in retail banking for 2024 centered on digital transformation, simplifying the customer journey, and the impact of new competitors.



Source: The Financial Brand

Those priorities have evolved but remain heavily focused on digital banking.

The top three trends for 2025 are:

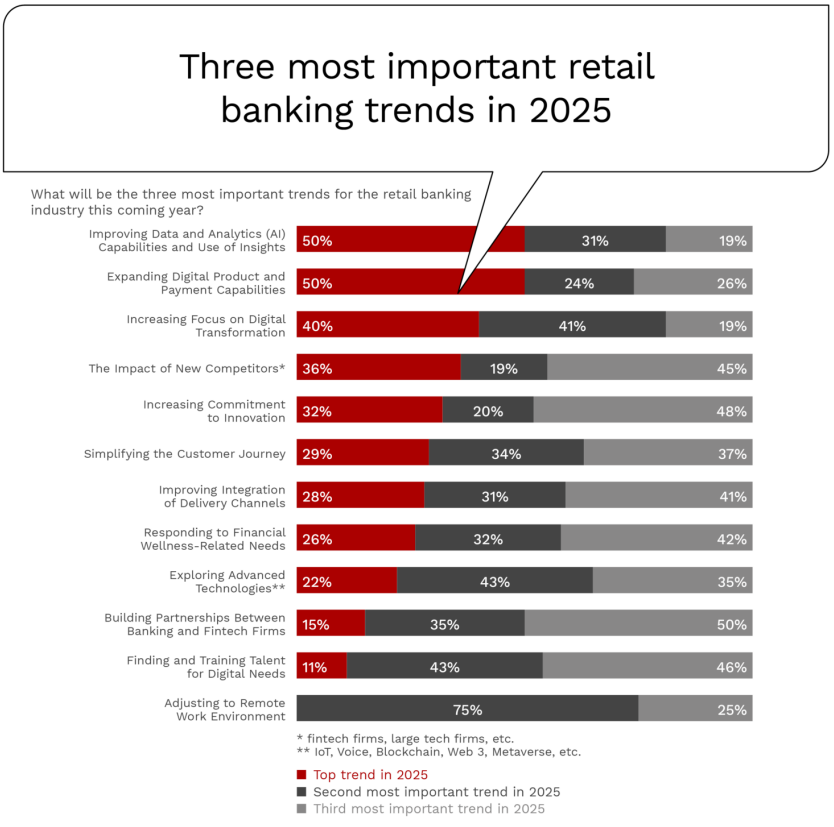
1. Improving data and analytics capabilities

2. Expanding digital product and payment capabilities

3. Increasing focus on digital transformation

These priorities underscore a consistent theme: retail banking continues to move toward being more digital, customer-centric, and data-driven. The question for financial institutions is how to make it easier for customers to accomplish what they want from a variety of different devices, how to make them feel valued at every touchpoint, and how to keep them satisfied with digital offerings. One thing is clear: The answer does not lie in more manual processes.

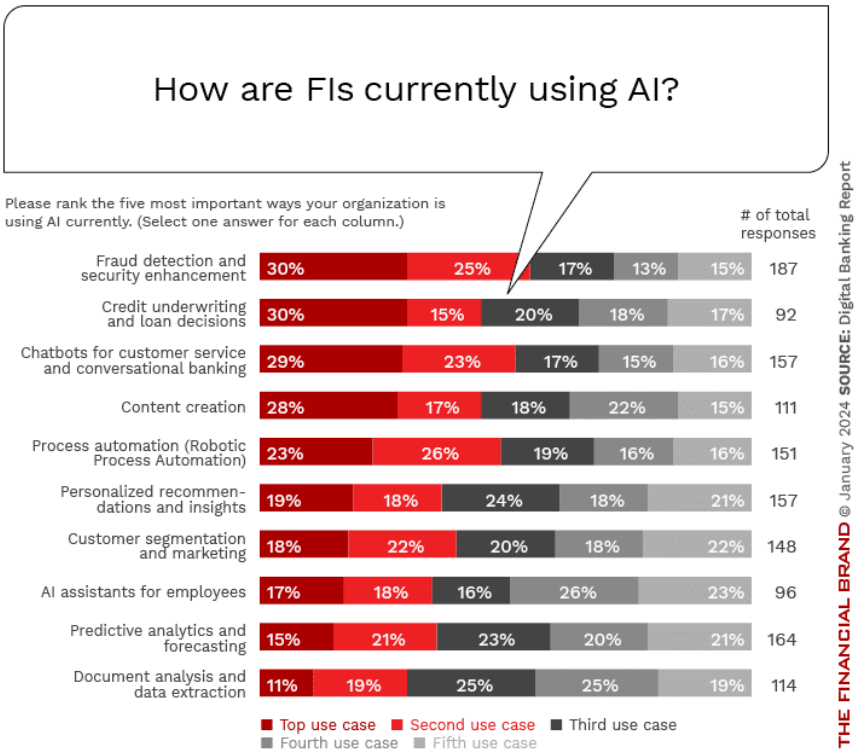
Three most important retail banking trends in 2025



THE FINANCIAL BRAND © May 2025 **SOURCE:** Digital Banking Report Research

Source: The Financial Brand

Speaking of automating manual processes, AI continues to be a major opportunity for financial institutions across multiple fronts. The widespread adoption of generative AI (like ChatGPT or Microsoft Copilot) has opened new possibilities for digital transformation, customer satisfaction, and risk management in cybersecurity and fraud detection. If your institution isn't actively exploring use cases for how AI can create efficiencies and improve productivity, you are already behind the curve!

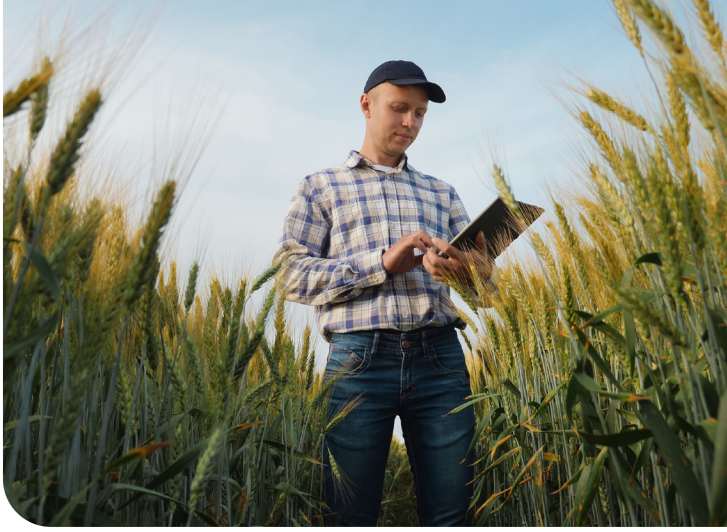


Source: The Financial Brand

Investment in digital transformation also continues to grow. Many financial institutions have already transformed or are planning to transform their digital account opening and customer onboarding processes in the near term. Most are also implementing or planning projects around small business mobile banking apps, chatbots, virtual agent chat, end-to-end digital consumer lending and mortgage applications, predictive advisory alerts, small business lending, and even AI-based communications.

At the same time, smaller institutions are discovering that investing in technology that simplifies the customer experience, builds convenience into processes, and saves time allows them to compete for valuable clients far beyond their traditional geographic footprint. Technology-based products and services have truly leveled the playing field for financial institutions. Still, many smaller institutions have been slow to invest and find themselves further behind the curve. If a financial institution can't acquire new clients in today's market, it's in trouble. The technology gap is also one reason we're seeing mergers and acquisitions pick up again.

Not Just Financial Institutions



While technology is transforming financial institutions, it's not only banks and credit unions that depend on it. Nearly every business today relies on technology and automation to stay competitive. Healthcare organizations, municipalities, utility companies (especially telecoms), government agencies, manufacturers, and agricultural operations are all increasingly dependent on technology to run day-to-day operations and drive efficiencies.

Unfortunately, you don't have to look far to find headlines about these sectors for the wrong reasons — hospitals hit with ransomware, government agencies suffering data leaks, and small businesses compromised due to weak security.

The point is simple: If your organization relies on technology and the internet to operate and serve customers, you're effectively a technology company. And if losing that technology or internet access would significantly harm your customers, you're definitely a technology company.

Why does this matter? Because technology companies tend to prioritize securing their networks and customer data. Organizations that cling to the "old ways" and view cybersecurity only as an expense are far more likely to be caught off guard.

Technology Companies Pay Attention to Cybersecurity

Once you shift your mindset and buy into the idea that your organization is a technology company, you'll think differently about how to protect it. Technology and cybersecurity can no longer be seen as a "necessary evil" or a line-item expense — they're critical to doing business. There's a return on investment for technology and cybersecurity, and while it varies for every organization, "staying in business" is a pretty solid ROI for anyone.

Here are three ways technology companies think differently about security:

1. They Understand the Risk

Mitigating risk starts with truly understanding it. A meaningful risk assessment doesn't just label risk as "low" or "medium." It helps you identify what systems and assets you have, how important they are, how exposed they may be, and where to focus your next security dollar. Don't run a risk assessment just to check the box. Instead, use it to make informed decisions and strengthen your defenses.

2. They Test People, Processes, and Technology

There are three ways to protect your information: **people, processes,** and **technology.** Your organization must put risk-mitigating controls in place, and just as importantly, you must test those controls to be sure they work.

People:

Social engineering assessments, such as phishing emails, phone or physical impersonation, or dumpster diving, measure how prepared your staff is.

Processes:

External IT audits or cybersecurity gap assessments confirm your policies and procedures are effective.

Technology:

Vulnerability assessments, penetration testing, red team testing, and Microsoft 365 assessments help ensure your security is strong, both inside and outside your network.

Of the three, **people** are your greatest attack vector. Here's the big secret: Cybersecurity is fundamentally human. **People** design the technology, market it, buy it, and use it — which means the human element can never be eliminated. That's why your security strategy has to focus on **people** just as much as **processes** and **technology**.

Because **people** are your biggest attack vector, you must actively include them in your cybersecurity efforts. Educate, motivate, and activate your staff to be your strongest line of defense against cyber threats. Don't just roll out one 60-minute training video and expect employees to practice good security for the other 364 days. Have ongoing conversations about real threats, run phishing simulations, and make security part of the culture. And remember, this area should be tested most frequently, not least.

For most organizations, that means regular security awareness training followed by phishing email assessments to make sure the lessons stick. Frequent testing dramatically reduces the number of employees clicking malicious emails, which in turn lowers your risk of data breaches, ransomware, and other attacks. With the right training and testing, you can turn your biggest attack vector into your first line of defense.

3. Cybersecurity Starts at the Top

To truly embrace the idea that you're a technology company, the message must start at the top and be backed up by action. If your board, CEO, or senior management talk about cybersecurity but ask to be removed from phishing tests or skip training, employees will see the real meaning behind the message — it's important enough to say but not to do. Leadership must model the behavior they expect and invest not only in technology but also in the people, training, and processes that make it effective.

Building a cybersecurity culture also means extending education beyond your employees to your customers. It shows everyone you're serious about protecting their information and about doing what's best for them. Testing your people regularly ensures they're prepared to defend confidential data from cyberattacks and social engineering tactics.

Finally, accountability matters. If employees repeatedly fail phishing tests with no consequences, you're telling the whole organization that cybersecurity doesn't really matter. The same goes for testing employees but not executives or board members. Everyone should be on an even playing field when it comes to testing your people. Attackers don't discriminate between staff and leadership, and neither should your security program.

Act Like a Technology Company

By thinking of your organization as a technology company and acting accordingly, you set yourself up for success on multiple fronts. Customers expect services that are simple, convenient, and efficient. If your organization can't deliver these three basic needs, customers will find someone who can. It's that straightforward.

Seeing your organization as a technology company also changes how you protect your networks and customer information. When you realize that your organization's very existence depends on the technology you deploy online to serve customers, your mindset shifts from "cybersecurity is a necessary evil and an expense" to "we must protect our networks and customer information because our very existence depends on it." Making that shift and investing in cybersecurity dramatically reduces the risk of an attack that could shut down your business. Even implementing a basic level of security puts you ahead of most small to medium-sized businesses that treat cybersecurity as an expense.

Technology continues to evolve rapidly. According to UBS, ChatGPT reached 100 million users in just two months — compare that to the internet itself, which took seven years to reach the same milestone. Leveraging today's (and tomorrow's) technology is critical to simplifying the customer experience, making business convenient, and saving time for everyone. This approach remains the key to winning in business, today and beyond. Once you start thinking and acting like a technology company, barriers fall away and opportunities multiply. Change your mindset today.

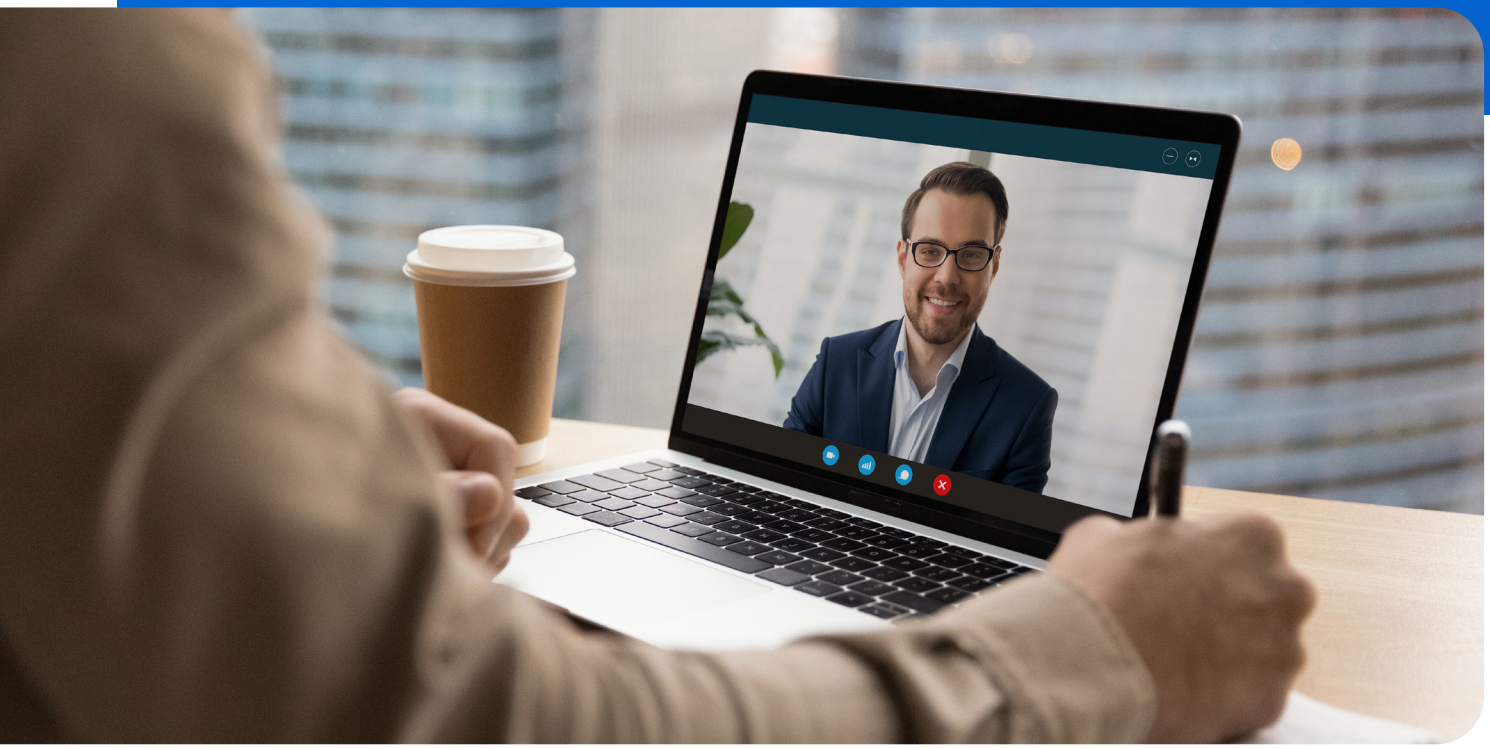
Source: UBS

How SBS Can Help

If you're ready to start thinking and operating like a technology company but aren't sure where to begin, SBS CyberSecurity has you covered. Our virtual chief information security officer (vCISO) service helps organizations like yours build a strong information security program (ISP), empowering you to make smarter decisions about information and cybersecurity — including where to invest your next security dollar.

vCISO clients are paired with an information security consultant who brings training, education, tools, frameworks, and templates to your organization. Together, we build an ISP that works for you, not just one that checks the boxes for compliance or framework alignment. We'll partner with you to mature your security posture while keeping you current on the regulatory and threat landscapes.

To learn more about the vCISO offering, visit link.sbscyber.com/vciso.



SBS's training division, the SBS Institute, also offers the Certified Banking Security Manager (CBSM) program for financial institutions and the Certified Business Security Manager (also CBSM) for nonfinancial institutions. The CBSM is designed to help ISOs and IT professionals learn how to build a comprehensive, valuable, and repeatable ISP that empowers you to make better decisions, including how to implement this risk management process at your organization.

To learn more about the CBSM, visit link.sbscyber.com/certs.

SBS CyberSecurity

Free Resources

Resource Library
Share our cybersecurity training tools with both your employees and your customers.

link.sbscyber.com/resources

Hacker Hour
Join our monthly interactive webinar series focused on cybersecurity issues and trends.

link.sbscyber.com/hackerhour

TRAC Action Tracking
Stay on top of remediation by creating, assigning, and monitoring security plans tied to your risk assessment.

link.sbscyber.com/actiontracking

Weekly Newsletter
Sign up for our In the Wild newsletter for a snapshot of key cybersecurity headlines and threat intelligence.

link.sbscyber.com/inthewild

Your Cybersecurity Ally

SBS CyberSecurity, LLC (SBS) is a top-rated consulting and audit firm. With over 20 years in the cybersecurity industry, SBS has provided solutions to thousands of regulated organizations across the United States and abroad. We offer dynamic solutions to help you build a proactive risk management program capable of withstanding the daily threats your organization faces. Our services are designed to assist you in making informed cybersecurity decisions to better protect your business.

sbscyber.com | 605-923-8722