You are a TECHNOLOGY COMPANY

Written by: Jon Waldman, President, Partner, Co-Founder
SBS CyberSecurity, LLC

That's Right.
Yes, YOU!

The original version of this exposition was drafted back in 2018, but the message and ideas in this paper ring even more true today than during the original publication. Since 2018, the world has endured a major pandemic (COVID-19), jumped right into a remote working revolution, migrated the majority of networking workloads to Cloud Computing, watched the evolution of autonomous vehicles becoming closer to daily reality, continued to invest in cryptocurrency and the blockchain, and jumped aboard the next technological revolution that is Artificial Intelligence (AI). Not to mention Quantum Computing, which is just around the corner and will turn our use of technology on its head. So much has changed, yet so much remains the same.

As the world marches full steam ahead into the next series of technological advances, and as your organization is reviewing its strategic plans for next year and beyond, please stop and take a moment to evaluate the use of technology as a core component of your business. If most of you are being honest with yourselves, you will realize that your organization has shifted from performing a service for a customer and using technology to make that service more convenient to truly operating as a technology company that offers your customer a specific service.

Look at it this way: if the majority of your day-to-day operations, especially customer interaction, involve some component of technology, whether it's through your website, a customer relationship management system (CRM), online banking, mobile payments, other mobile applications, email, smartphones, or your smartphone app, then **you are a technology company**.

Another way to reality-check yourself is by asking this big question, "If my organization threw all our technology out the door today, could we still do business effectively and really serve our customers?" For most of you, the answer is surely a resounding "NO." The reality of today's business world is that nearly all organizations of any scale rely heavily on technology, and without our tech, we'd essentially be unable to do business long-term.

> "If my organization threw all our technology out the door today, could we still do business effectively and really serve our customers?"

Focus on the Customer

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

Time is the #1 currency organizations trade on today; not because our customers are lazy, but because everyone is extremely busy. Take a look at some of the largest companies in the world today (by market cap). Of the Top 10, seven companies 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 wins because the service allows you to purchase nearly anything you want, any time you want it, on any device you want, and it will be delivered directly to you with free 2-day shipping (well, mostly). Simple, convenient, and time-saving. Amazon also started a little side project to rent out its additional computing power back in 2003, which led to Amazon Web Services (AWS), which now boasts over $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 is not surprising since what Microsoft produces (software) is solely technology-based. However, Microsoft has doubled its annual revenue since 2018 with the massive adoption of its Microsoft 365 (M365) platform. M365 now boasts over 1 million companies globally that have converted their organizational day-to-day operations into Microsoft's cloud-based platform.

We talk about Microsoft (and Amazon) as one of the driving forces behind the push to the cloud, where all of today's newest technologies live – along with today's big threats and next-generation security controls. Organizations are no longer developing new technologies to live on traditional networks. Even Microsoft is slowing down development for traditional platforms. Can you even buy an on-prem version of Microsoft Office anymore?

Then there are all of today's new "tech" companies: FinTechs, BioTechs, AgTech, TravelTech, EdTech, and so on. Remember back in the day when you had to go to Best Buy and buy a box of software that came on floppy disks or CDs and had to be manually installed 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 to do faster from anywhere. And these next-gen technologies only live in the Cloud.

However, the most important reason we highlight today's tech companies that continue to win and "disrupt" the market is that today's marketplace focuses primarily on the customer and the customer experience. Ask yourself the same burning questions 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

In today's banking climate, the market – like all technology companies – is customer-focused and driven. If your institution does not provide the products and services that your customers want and need, the customer will find another institution that provides those products and services. According to Consumer Affairs, in 2024 the average US consumer has an account at over five different financial institutions. Consumers also utilize about 14 financial apps on average, which may include apps to invest, manage multiple banking accounts, budget their finances, and more.

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 account opening over the last few years, a consumer can set up an account with ANY financial institution online or via mobile app in just a few minutes. If your customers take their money to other financial institutions because your institution is not meeting their needs, you are in trouble.

So, what should your institution do? **Focus on the customer!**

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

Additionally, there is no shortage of Fintech partners available to integrate into your ecosystem these days. Many financial institutions have taken a Fintech-centric approach to meeting customer needs and demands by partnering with a variety of Fintech apps and integrating these apps into their mobile banking platforms. However, Fintech partners require a strong level of Vendor Management and due diligence to ensure both the security of the data being shared with Fintechs (it's your responsibility to protect YOUR customer information, no matter who stores, transmits, or processes this data) and the long-term viability of the product (many Fintechs are either acquired or fail, so make sure you are confident in the sustainability of any Fintech or app you provide your customers).

Another way to evaluate your institution's sustainability is to understand your ability to retain your youngest customers. While customers between the ages of 25-44 are the prime acquisition targets of financial institutions, as that's when customer spending takes off, it's not as simple as specifically targeting these age groups. A financial institution must set its sights on the younger generations.

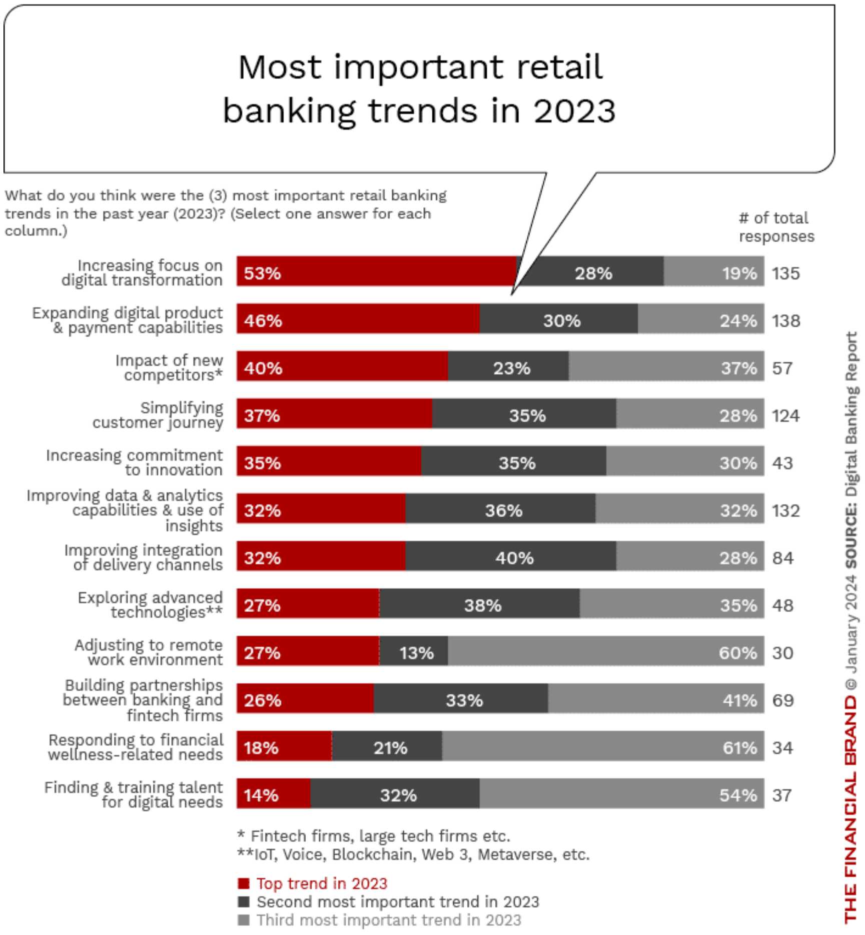
By the time a customer reaches the age of 25, they have already selected their primary financial institution of choice. The primary institution is where the customer holds most of their money, receives their paycheck direct deposits, and through which they spend most of their money (checking account). While switching primary financial institutions today is certainly not impossible, it is inconvenient – especially if the customer has automatic bill payments set up. The most common reason customers switch primary institutions is that another institution offers more simplicity, convenience, and time-savings for their everyday banking needs. Better rates don't hurt, but rates are not the most important factor these days. The most important reason cited by customers for choosing a bank account is fees – specifically a lack thereof – according to Forbes. Customers can set up an account with most financial institutions in about 10 minutes and move money from one institution to another in a day or two. Instead, focusing on the younger generations of banking customers allows you to provide them with the simple, convenient, and time-saving experiences they desire.

At the risk of making a sweeping generalization, nearly everyone under the age of 30 is technology and mobile-savvy, and they expect services to be technology-based. Providing technology-based products and services that appeal to the younger generation of customers will make it much easier (and more cost-effective) to retain these clients when they hit their prime-spending years than attempting to acquire clients that already bank with other institutions.

While your efforts to acquire new customers earlier should undoubtedly be a focus of your strategy, you can't ignore your long-term customers either. But there's a secret to those long-term customers: 99% of 50+ consumers own a tablet, laptop, or desktop device. They also happen to be the fastest-growing segment of digital product users. In fact, according to Forbes, over 70% of ALL banking customers access their bank accounts via either online banking (website) or mobile application. Don't let your long-term customers be an excuse for your organization not to embrace digital products and services; they want simple, convenient, and time-saving as much as anyone.

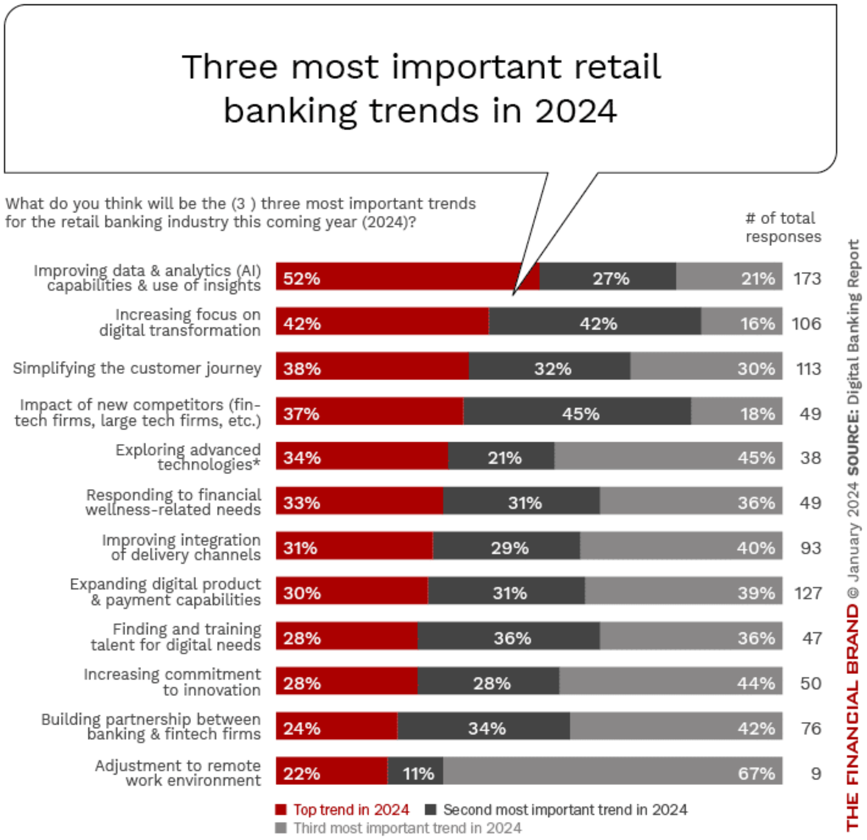
Banking Trends for 2024 and Beyond

According to The Financial Brand, the top three trends in retail banking from 2023 continue to be focused on digital banking products, including 1) increasing focus on digital transformation; 2) expanding digital product and payment capabilities; and 3) the impact of new competitors (including Fintech and other competitors). Simplifying the customer journey checks in at #4, which was #1 back in 2018. Most of the top retail banking priorities are still on the board from six years ago, though the industry has clearly been working hard to mitigate these issues.



Source: The Financial Brand: https://thefinancialbrand.com/news/banking-trends-strategies/2024-retail-banking-trends-and-priorities-174327/

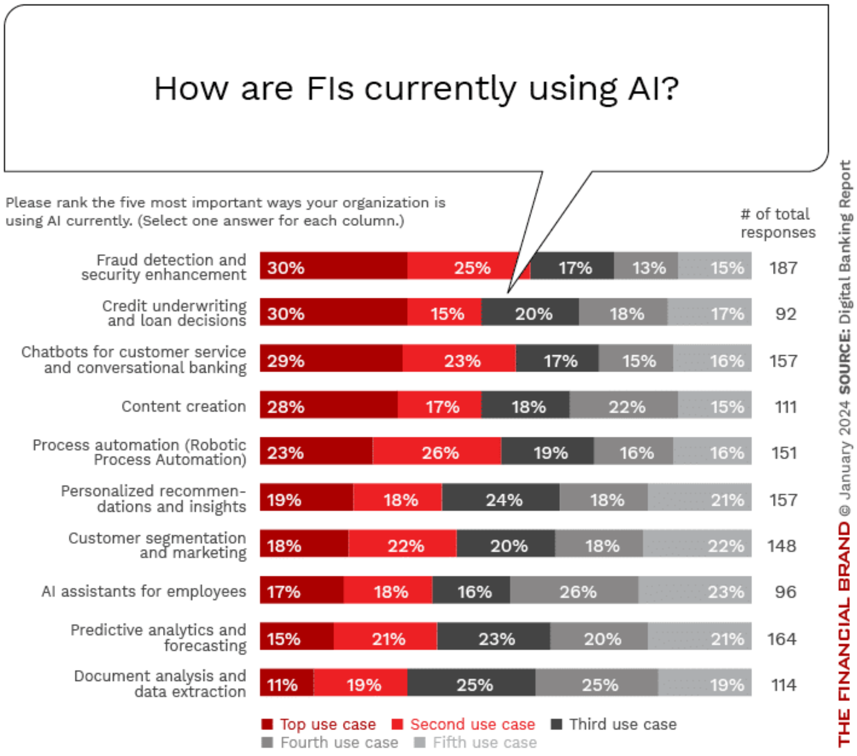
The biggest trends for 2024 for retail banking are similar, but with a twist: the advent of AI, as it relates to data analytics, has taken the top spot for 2024 (it was #3 in 2018). Digital Transformation (#2) and Simplifying the Customer Journey (#3) round out the top three, and interestingly enough – these were the same Top 3 Trends for Retail Banking in 2018 (just in a different order).



Source: The Financial Brand: https://thefinancialbrand.com/news/banking-trends-strategies/2024-retail-banking-trends-and-priorities-174327/

These top trends line up directly with the key messages of being customer-centric with products and services and acquiring and retaining customers, as we discussed previously. How can our organization make it easier for our customers to accomplish what they want from a variety of different devices? How can we make them feel like valued customers the whole time? How can we keep customers happy with our digital banking offerings? Those are the million-dollar questions. One thing is for sure: the answer does not lie in more manual processes.

Speaking of automating manual processes, AI continues to be a major opportunity for financial institutions on various fronts, and the use cases are plentiful. The widespread adoption of Generative AI (like ChatGPT or Microsoft Copilot) has opened financial institutions to the possibilities of how AI can help their digital transformation processes and increase customer satisfaction. Not to mention AI being leveraged in cybersecurity risk mitigation and fraud detection. Here's a snapshot of how banks are currently leveraging AI:



Source: The Financial Brand: https://thefinancialbrand.com/news/banking-trends-strategies/2024-retail-banking-trends-and-priorities-174327/

Investment in digital transformation also continues to grow. Nearly 80% of financial institutions have either already or are planning to complete their digital new account opening and new customer onboarding processes within the next year. Most financial institutions are also either implementing or planning digital transformation projects around small business mobile banking apps, chatbots, virtual or video agent chat capabilities, end-to-end digital consumer personal loans, end-to-end mortgage lending, predictive advisory alerts, small business lending, and even AI-based communications. There's a lot going on regarding digital transformation and technology to take the business of banking to the next level over the next year or so.

To that same end, smaller institutions are finding out quickly that investing in technology that simplifies the customer experience, builds convenience into the process, and saves time allows any organization to compete for valuable clients beyond their traditional geographical footprint. Technology-based products and services have truly leveled the playing field for banks. Still, many smaller institutions have been slow to invest and find themselves even further behind the curve. If a financial institution can't acquire new clients in today's market, they're in trouble. The technology curve is part of the reason we're seeing M&A activity begin to pick up once again.

Not Just Banks

While technology is taking over the world of financial institutions, technology and automation are not critical only to banks and credit unions but to nearly every business operating today. As we mentioned regarding technology companies previously, healthcare organizations, municipalities, utility companies (specifically telecoms), government agencies, manufacturing, and agriculture (to name a few) are industries that are becoming wholly dependent on technology to perform their day-to-day operations and gain efficiencies to make money. You don't have to look too hard to find examples of each of those organizations in the headlines for the wrong cyber-related reasons, including hospitals and ransomware, government agencies and data leaks, and numerous other small businesses getting compromised due to their lack of security.

The point – again – is that if you rely on technology and the internet to perform your day-to-day operations and serve your customers, consider yourself a technology company. Additionally, if the technology or internet connectivity you rely on were to go away and your customers would be substantively harmed, consider yourself a technology company.

Why should you consider yourself a technology company? Because technology companies pay more attention to securing their networks and customer information than companies that romanticize the "old ways" and cling to the notion that technology is simply an expense.

Technology Companies Pay Attention to Cybersecurity

Once you shift your thinking and buy into the idea that your organization is a technology company, you will begin to think differently about how you protect your organization. Technology and cybersecurity can no longer be considered an expense or a "necessary evil" but must be viewed as a critical component to doing business, without which you can't operate. There is a return on investment for technology and cybersecurity, and while it's different for each organization, "not going out of business" is a pretty solid ROI for anyone.

Here are three ways that tech companies think differently about their organization and security:

1. They Understand the Risk

Being able to truly mitigate your risk starts first with how well you can understand and quantify risk. If you perform a risk assessment and your results only state that you have "low" risk, how do you know that's right? How do you know what you need to do next?

The primary job of a risk assessment is to help you make decisions. When it comes to IT or Cybersecurity Risk Assessment, the output should provide you with a clear understanding of what you have (technology systems and assets), how important the things you have are, how risky your systems and assets are, and where you should spend your next information security dollar to mitigate additional risk. Don't just perform a risk assessment to check the box; really know and understand your risk so you can secure your organization more effectively.

2. They Test Their People, Processes, and Technology

There are 3 ways to protect your information:

1. People **2.** Processes **3.** Technology

Your organization must implement risk-mitigating controls to protect your networks and customer information from those three categories. In turn, so that you are confident those controls are in place and working correctly, you must test the effectiveness of those controls.

Testing your **People** involves Social Engineering Assessments (phishing emails, physical impersonation, phone impersonation, dumpster diving, etc.). Testing your **Processes** involves an External IT Audit. Finally, testing your **Technology** typically involves technical scans around the inside (Vulnerability Assessment) and outside (Penetration Test) of your network.

Finally, out of those three processes, your **People** are your greatest attack vector and risk. Here's the big secret: cybersecurity is a fundamentally HUMAN thing. Humans programmed the technology we use. Humans marketed that tech and sold it to us. We bought it, and we use it. We can't remove the human element from cybersecurity!

Knowing that our **People** are our biggest attack vector, we must also choose to include our **People** in our cybersecurity actions. We've got to educate, motivate, and activate our people to become our greatest line of defense against cyber threats! Have regular conversations about cybersecurity threats – don't just ask your **People** to watch one 60-minute video per year and expect them to do good cybersecurity things for the other 364 days.

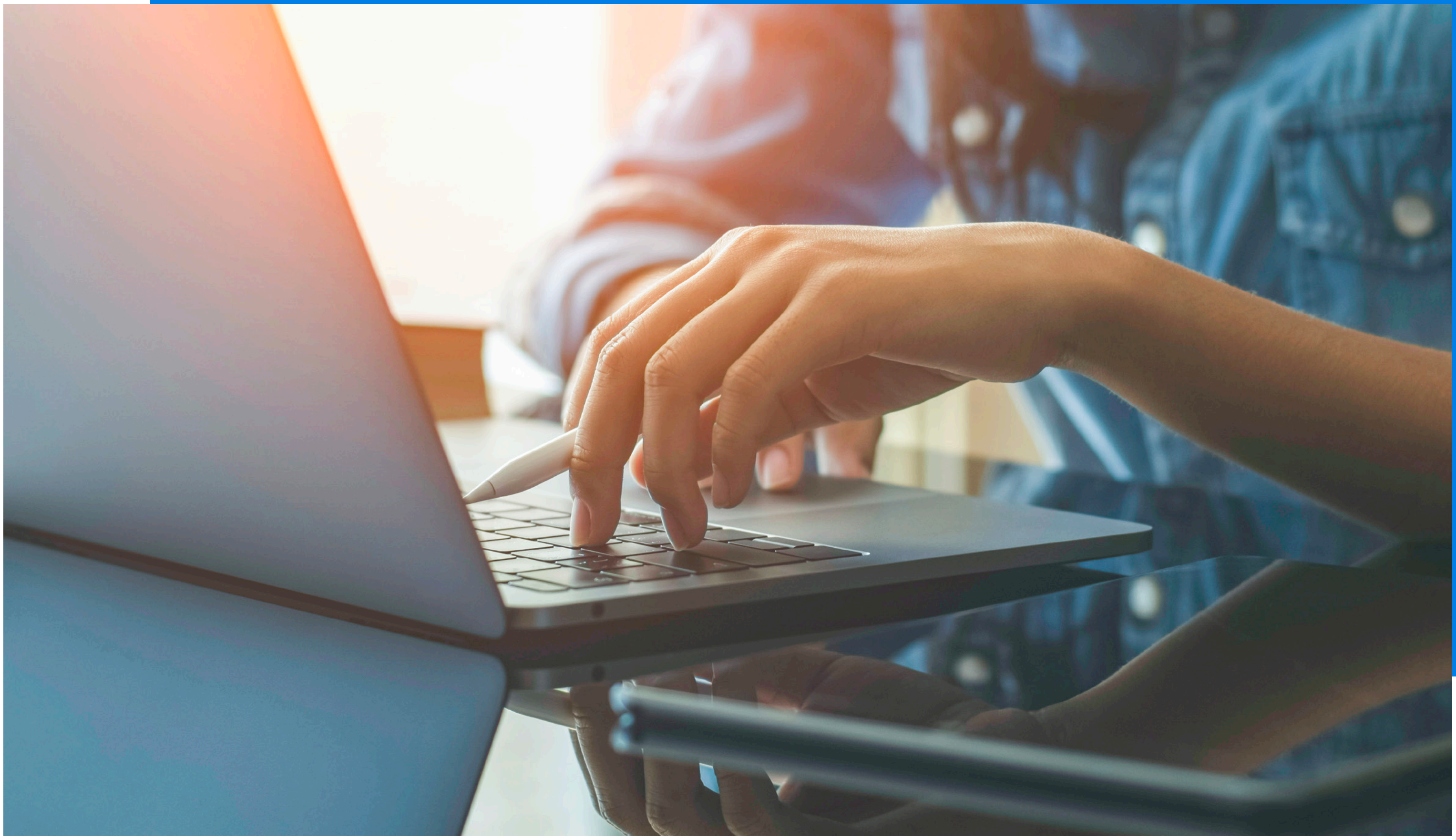
Finally, knowing that your **People** are your biggest attack vector, you should test this area of your organization MOST frequently, not least frequently. For most organizations, that means regular security awareness training followed by phishing email assessments to make sure the training and education sticks. The most popular phishing email testing software in the world, KnowBe4, tells us that frequent phishing email testing can dramatically reduce the number of employees clicking on emails, and that's a very good way to prevent data breaches, ransomware, and a variety of other cyber attacks.

3. Cybersecurity Starts at the Top

To truly ensure your organization is on-board in thinking you are a technology company, the message must be consistently portrayed from the top down. If the Board of Directors, the CEO, and senior management are constantly preaching a cybersecurity-focused mentality but not walking the walk (i.e., asking to be removed from phishing test emails or skipping cybersecurity training), the message will become a joke. Starting at the top means sharing the technology-focused message and vision with the whole organization, then backing up the message with appropriate investment into not only the technology but also the resources needed to deploy the technology, including the roles and responsibilities of the staff. A shift from treating technology as an expense to a critical business function means aligning your actions with your message.

Training and education of not only your employees, but also your customers, is another key component to building a cybersecurity culture. It shows everyone that you mean what you say and are committed to doing what's best for your employees and customers. It's also important to test your **People** to ensure they are adequately trained and prepared to defend your confidential customer information from cybersecurity and social engineering attacks.

The last component of building a cybersecurity culture is holding **People** accountable for their actions. If you are testing your **People's** cybersecurity awareness with regular phishing email tests, accountability must be built into the process for it to be effective. Phishing is the #1 attack vector used by attackers to compromise your network and steal customer information. Allowing employees to fail phishing assessments by clicking on links repeatedly sends a very loud message to the organization that cybersecurity doesn't matter. The same goes for testing your employees but not your senior management or directors. Everyone should be on an even playing field when it comes to testing your **People**. Remember, attackers don't discriminate between employees and directors or executives.



Act Like a Technology Company

By thinking of your organization as a technology company and acting accordingly, you will set yourself up for success in the future on numerous fronts. Customers are demanding that the services you offer become simplified, convenient, and save them valuable time. If your organization cannot fulfill these three basic customer needs, they will find an organization or services that will. It's that simple.

Additionally, viewing your organization as a technology company will change your perspective on how you protect your networks and customer information. Once you realize that your organization's very existence depends on the technology you deploy via the internet to serve your customers, your focus will shift from "it's a necessary evil and an expense" to "we really need to do our best to protect our networks and customer information because our very existence depends on it." Once you make that shift and invest in cybersecurity, you dramatically reduce the likelihood of a cybersecurity attack that could shut down your business. Implementing even a basic level of security at your organization will put you ahead of 90% of other small-to-medium-sized businesses that treat cybersecurity as an expense.

We all know that technology continues to change and grow rapidly. It took two months for ChatGPT to reach 100 million users. For context, it took the internet itself seven years to hit 100 million users. Taking advantage of today's (and tomorrow's) technology is key to simplifying the customer experience, making doing business convenient, and saving time for everyone. This remains the key to winning in the business world, still in 2024 and moving forward. Once you start thinking and acting like a technology company, barriers fall away, and opportunity will abound. Change your mentality today!

How SBS Can Help

Suppose you want to shift your mentality to that of a technology company, but you don't know where to start. Well, we've got your back! SBS CyberSecurity has developed our Virtual CISO (vCISO) program to help organizations like you. The vCISO program is designed to help organizations build a strong Information Security Program (ISP) that empowers you to make better decisions around information and cybersecurity, such as where to spend your next information security dollar. vCISO clients are assigned their own Information Security Consultant to bring training and education, tools, frameworks, and templates to your organization to build an ISP that works for you, rather than simply checking the box for compliance and alignment with today's cybersecurity frameworks. We will be your partner and guide you as you mature your security posture, as well as keep you up-to-date on the ever-changing regulatory and threat environments.

To learn more about the vCISO program, please visit: https://sbscyber.com/services/virtual-ciso.

SBS CyberSecurity's training division, the SBS Institute, also offers the Certified Banking Security Manager (CBSM) certification program for financial institutions and the Certified Business Security Manager (also CBSM) for non-financial institutions. The CBSM is designed to help Information Security Officers and IT professionals learn how to build a comprehensive, valuable, and repeatable Information Security Program 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: https://sbscyber.com/education/certifications.

Free Resources

available at: sbscyber.com

Hacker Hour Webinar

Join our free monthly interactive webinar series focused on discussing cybersecurity issues and trends.

Product Demos

Discover the power of our offerings with live demos scheduled each week highlighting individual products and services.

Security Awareness Training

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

TRAC™ Action Tracking

Remain diligent with your remediation tracking and follow up by creating security plans associated with your risk assessment.

Join Our Email List

Follow the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity.

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.

For more information:

sbscyber.com | 605.923.8722