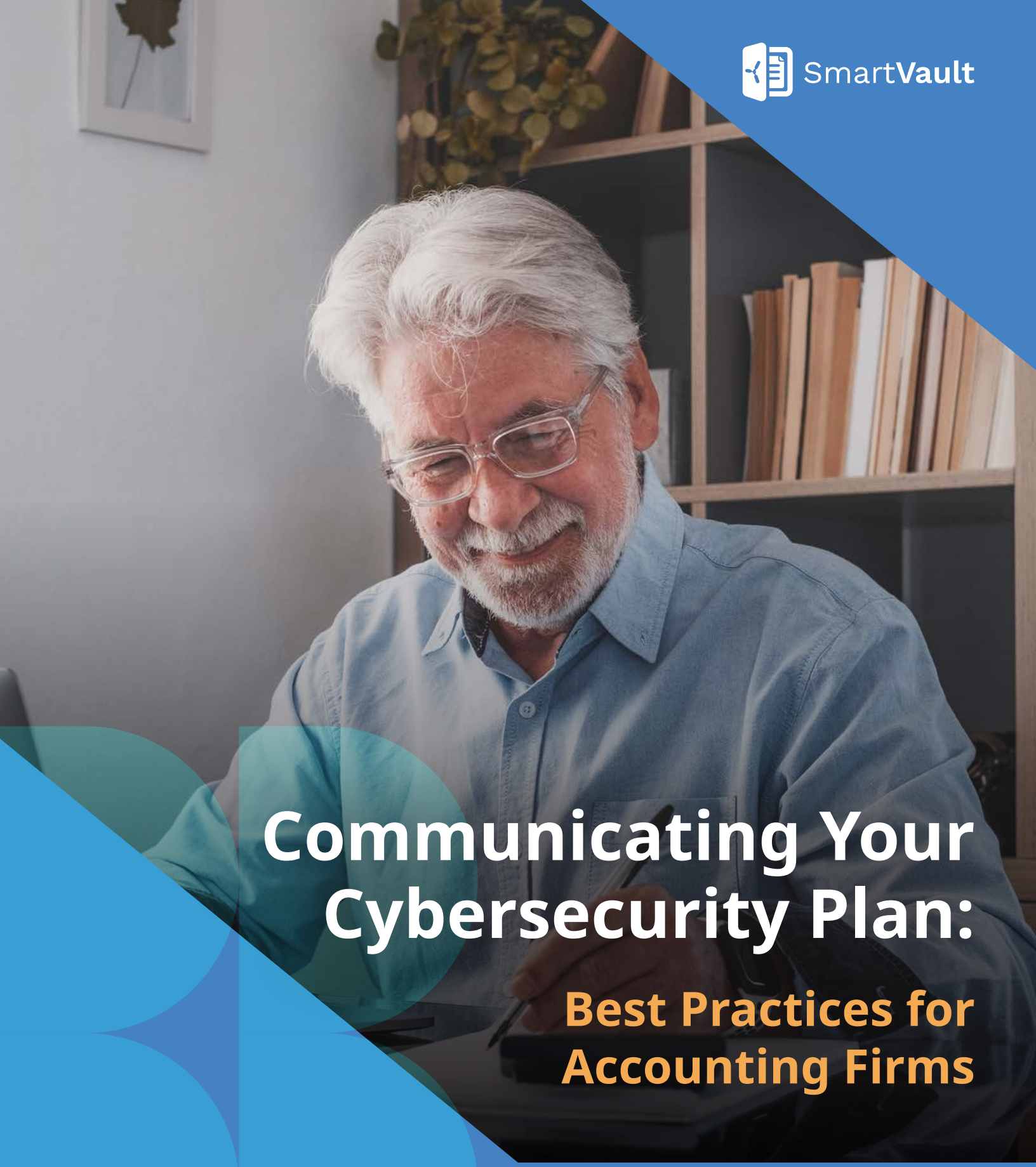
SmartVault



Communicating Your Cybersecurity Plan:

Best Practices for Accounting Firms

Whitepaper

Contents

Introduction

We know that robust cybersecurity programs are crucial. What's equally important – and often overlooked – though, is communicating your program to your staff and clients. You can have the strongest cybersecurity program, but the simple fact of the matter is: if no one knows their roles or follows your policies, your business will be exposed to unnecessary risk. In fact, the biggest threat to your cybersecurity is human error – these events account for nearly 90% of all cyber incidents.

And while cybersecurity measures like firewalls and antivirus software are essential, cybersecurity risks cannot be mitigated with technology alone. People – both internal (staff) and external (clients and vendors) – are key parts of the puzzle.

It's no surprise, then, that Luke Kiely, cybersecurity expert and SmartVault Chief Information Security Officer, says, "Educating people is the primary driver to ensuring they adopt your cybersecurity program and associated policies."

It's not as simple as asking people to read your program, though. You need to create a security culture, which the National Protective Security Authority defines as "the set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security."

Building and maintaining this culture requires effective, ongoing communication that ensures everyone understands and takes accountability for keeping data safe. It also needs to be a priority from the top down. Executives and managers must understand the importance of cybersecurity and lead by example.

This whitepaper summarizes key tips and insights from cybersecurity and accounting experts on how to communicate your program and build a security culture.

Key Takeaways for Communicating with Staff

Employee education and training is one of the most vital components of an effective cybersecurity program. “The biggest portion of insider threats is what I call the careless or negligent insider,” Luke explains. “That’s where you have employees or contractors who may accidentally compromise security by mishandling data, using weak passwords, or falling victim to a phishing attack.” Proper training following the principles below can help prevent these errors.

Keep Training Simple

“Having simple policies and procedures for staff to digest and follow is the starting point to a successful program,” Luke explains. Avoid overwhelming staff with technical jargon and too much information. Instead, Luke recommends “keeping it simple and focusing on key policies relevant to each person’s role.”

Elizabeth Manso, CEO of Brigade Accounting, agrees. “After going through [our cybersecurity program], I feel like I understand it from the IT company’s perspective,” she says – but that’s not what she expects from her team. She suggests “presenting a nice summary to make sure that they understand the crux of what’s in the program,” rather than requiring them to read and remember every detail.

Remember that “people learn in different ways,” Luke says. Don’t just rely on email, for example. Offer a mix of in-person training, videos, ‘how to’ guides, FAQ articles, and others.

Making Cybersecurity Practical

Learn how to make cybersecurity manageable and get practical steps you can implement to reduce risk and safeguard your business today.

DOWNLOAD THE FREE WHITEPAPER

Focus On the Why and the How

A common mistake businesses make is centering the training on why cybersecurity is important; while that's crucial for your team to understand, your training needs to be much more robust to be effective.

"You have to teach them what their specific role is and how they should respond to a cyberattack," Luke explains. "When you think about phishing emails, for example, it is critical that staff are trained to identify them and what to do if they receive one."

Luke also encourages businesses to take training further by rehearsing cybersecurity incidents and practicing their response plans. "These rehearsals include your staff, but also IT, legal, senior management, and potentially your HR and public relations teams...anyone who will be a critical decision-maker in the event of a cybersecurity incident."

> **"A well-structured, clear, and relatable cybersecurity training program or material is paramount." – Luke Kiely, CISO, SmartVault**

Educate and Train Multiple Times a Year

Cybersecurity threats constantly evolve, so it's important to ensure staff understand and follow the latest best practices. Quarterly or biannual training helps keep policies top of mind. If you think your staff will balk at multiple trainings a year, consider how it'll help them in their personal lives as well. Hackers, after all, don't just attack businesses. Your staff can implement what they learn through the training to protect their personal accounts.

Along with regularly scheduled training throughout the year, it should be integrated into your new hire onboarding. At Brigade, Elizabeth says this onboarding training "helps [new hires] see how we operate with cybersecurity in mind." This helps them adhere to the policies while building trust with the firm.

After all, staff have a vested interest in your cybersecurity processes. They want to confidently know the sensitive data they're handling is protected from breaches. Many staff also worry that the financial repercussions of a cyberattack could impact your profitability and stability, jeopardizing their job security. When you prioritize security and training, it helps reassure staff that their work and job are secure.

Avoid the Blame Game

When errors happen, you must balance accountability with learning. "Do not criticize, blame, and target people who don't do the right things," Luke says. "As soon as you start doing that, you create a bad culture," where suddenly people may be discouraged from reporting incidents.

Instead, focus on constructive feedback and improvement. Encourage staff to ask questions and report suspicious emails or activities without fear of reprimand – and always thank staff for voicing their concerns or reporting incidents. Use mistakes as an opportunity to improve your company's security defenses and maintain a blame-free response to encourage continued transparency.

Key Takeaways for Communicating with Clients

Educating clients about your cybersecurity processes will increase their trust in your firm. They'll recognize your commitment to keeping their personal information secure, leading to long-lasting relationships and referrals. Your clients also have a role to play in your program, and they'll need you to explain that role. Here are some recommendations.

Start on Day One

Cybersecurity awareness is part of Brigade's conversations with prospective new clients. "I share our best practices for cybersecurity to make sure they're aware," Elizabeth says. "They need to understand that it's very high on our priority list to ensure their information is safe." The firm then goes into more detail during new client onboarding. "This is when we communicate processes," such as how clients can send sensitive information to the firm.

When clients express frustration with security processes, explain why they are necessary and how they protect their data. As Elizabeth explains, you need to "understand that the processes may make the client experience a little harder," especially for clients who struggle with tech.

Your goal should be to make everything seamless. You'll need to train them directly on using security features, like your client portal and how to submit documents. Ideally, you're partnered with a vendor who provides free educational and training resources for your clients, so they can get up and running on your processes quickly.

Avoid Sharing Too Much

Just like experts advise not to overwhelm staff with your policies, you want to take the same mindset with your customers. Only tell them what they need to know to be successful.

You want to avoid making security complicated or confusing. Customers who become overwhelmed may shut down and decide not to continue their relationship with your firm, or maybe worse, not follow your security processes at all.

There's also the risk of sharing too much. Avoid revealing sensitive information and technical specifics that could aid hackers if it's compromised. Luke advises, "Be mindful about who you share the information to and why."

He continues, “Don’t share information like how you configure a firewall and what kind of traffic you’re going to let in and out.” But you can share “high-level security operations,” such as what technology you have in place and whether you have things like automatic data backup and 24/7 monitoring.

Position Security as a Value-Add

Clients value working with cyber-savvy firms. As Luke explains, “I think being proactive about your security approach, mindset, the kind of measures you’ve put in place…You should shout from the rooftops about it because it sends a really good message to your clients.”

It also helps with your digital trust. “A business’s reputation is influenced by digital trust, which can include online reviews, ratings, and word-of-mouth recommendations that people use to gauge trustworthiness,” Luke states.

You should also make it a partnership. Invite clients to ask questions and provide feedback to improve processes and make cybersecurity an ongoing conversation. As Luke suggests, “Give clients an element of trust about how you will support them and their relationship with your firm.”

SmartVault

Make Security Implementation and Adoption Easier with Tech

Staff and clients may see security rules and requirements as unnecessary obstacles that make their tasks more difficult. The right tech solutions can help overcome this challenge and simplify employee and client cybersecurity adoption.

Take, for example, a document management system (DMS) and client portal that secures how you gather, share, collaborate on, and store documents in the cloud. With cybersecurity controls and access restrictions built directly into the DMS, your staff and clients can focus on their tasks and responsibilities while the system applies cybersecurity policies behind the scenes. This makes implementing and adopting security practices much smoother and improves your compliance with regulations.

Over 30,000 accountants and their clients securely gather, store, share, and eSign documents in the cloud with SmartVault.

Online Document Storage

Standardize and centralize your business documents.

Secure File Sharing

Share files easy, compliant, and secure.

Branded Client Portal

Give clients a professional way to work with you.

Learn more or schedule a demo: www.smartvault.com