axos ADVISOR SERVICES

ADVISOR INSIGHTS

Cybersecurity

How to Defend Your Digital Data

It seems that hardly a week goes by without news headlines about a major cyberattack or cyber security breach. Advisors should take inventory of their digital assets to determine where hackers might exploit points of entry or how data may be lost to system errors.

Cybersecurity is becoming less of an esoteric topic for advisors – something that's avoided or relegated to IT personnel to handle. Increasingly, it has become front-page news. Many clients have also picked up on the concern, and have begun asking their advisors questions like: "Where is my data being stored?" "Who has access?" "How are communications being secured?" "What happens to my data if our relationship ends?"

At the same time, cybersecurity risks have increased due to the COVID-19 pandemic. Out of those who suffered a breach in the last five years is 82%. There are multiple factors contributing to this such as: remote work using mobile devices, new digital tools being used for customer data and third-parties being directed by customers to access their data.

Before clients and regulators show up asking questions, you may want to review your business's protections and preparedness for potential data breaches.

Reasonable steps are required

As part of its Code of Ethics and Standards of Conduct, the CFP Board requires financial advisors to take reasonable steps to protect the security of all non-public client information they store electronically. Regulators like the SEC and FINRA also have their own guidance on cybersecurity for financial advisors. This means that advisors can no longer just respond after-the-fact to cybersecurity incidents. Instead, you need to take proactive steps to protect your firm and your clients' data from cyberattacks.

One out of five wealth managers have reported a data breach over the past five years.

– 2022 Arizent State of Cybersecurity Survey

New rules proposed by the SEC in February (https://www.sec.gov/news/press-release/2022-39) add some urgency to cybersecurity risk management for financial advisors. These rules would create cybersecurity risk management standards requiring advisers to adopt and implement written cybersecurity policies and procedures designed to address risks that could harm clients. They would also require advisers to report significant cybersecurity incidents to the SEC on a new section of Form ADV.

In addition, advisors would have to publicly disclose cybersecurity risks and significant cybersecurity incidents that occurred in the last two fiscal years in their brochures and

continued

registration statements. The rules would also set forth new advisor recordkeeping requirements designed to improve the availability of cybersecurity-related information and help facilitate the SEC's inspection and enforcement capabilities.

Evaluating your cybersecurity preparedness

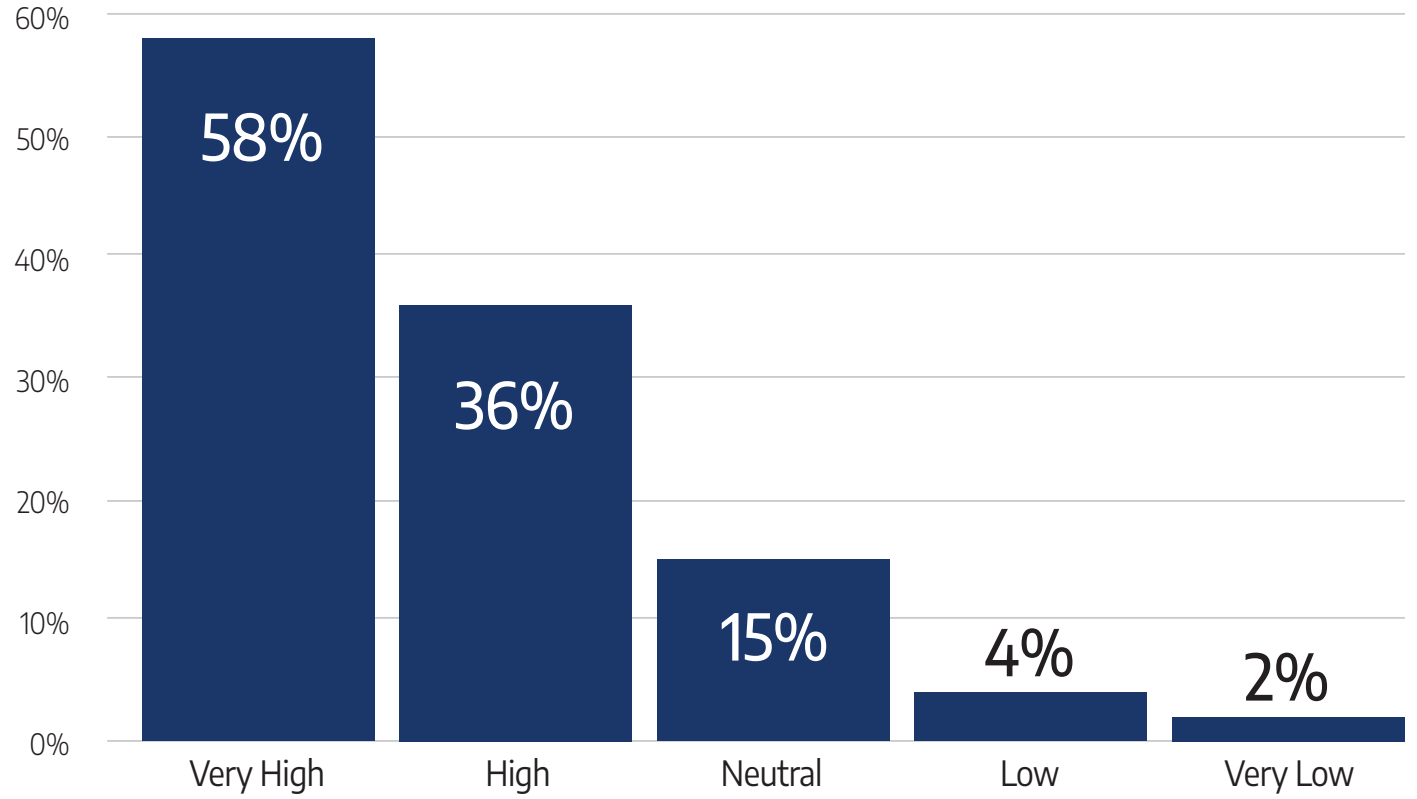
Ransomware is just one form of an outside attack. Threats to financial data also include natural disasters and power failures, employees stealing information and other hacker tactics, like phishing. The first step in measuring your cybersecurity is to track your metrics. Track your history of cyber attacks or attempts (distributed denial of service, network intrusions and data theft), procedures in place (encryption for all devices and email, Adobe Patch Coverage, Microsoft Patch Coverage, anti-virus coverage) and security awareness among employees.

There is a checklist from FINRA and a Cybersecurity Assessment Tool from the Federal Financial Institutions Examination Council (FFIEC) available for advisors to organize their data and determine risk levels. You can also take advantage of free web server encryption tests which probe and analyze communication security.

Of course, the complicated layers of technology connection types, delivery channels, online products and services and organizational structures within each practice make every advisor's risk unique. Consider hiring an outside IT advisor with credentials in cybersecurity and financial services to make the most of these assessments. Smaller operations where one person may be responsible for compliance, legal functions and the cybersecurity program are particularly advised to hire extra help.

As you evaluate how you'll protect client information and your own system operations, be sure to evaluate how your insurance will protect your business. Some firms and independent advisors leave it up to a cyber-coverage rider attached to their traditional errors-and-omissions coverage. These policies may not cover regulatory fines or all claims, therefore you may want to consider a standalone policy.

How important would you rank cybersecurity as a priority at your firm?



Source: *Arizent State of Cybersecurity Survey 2022*

Preparing for potential cyber attack threats

Once you've understood your digital strengths and weaknesses, it's time to document detailed policies and procedures for all areas of your business. Consider these six key cybersecurity areas:

1. Remote work

The accelerant behind these changes was the COVID-19 pandemic and the effects that the virus has had on how businesses operate and how consumers engage with them appear to be longer lasting. That is, once the pandemic fades into the history books, many of the changes brought on by the impact of the virus are likely to remain and grow in popularity due to the convenience and greater access they offer, such as employees working remotely.

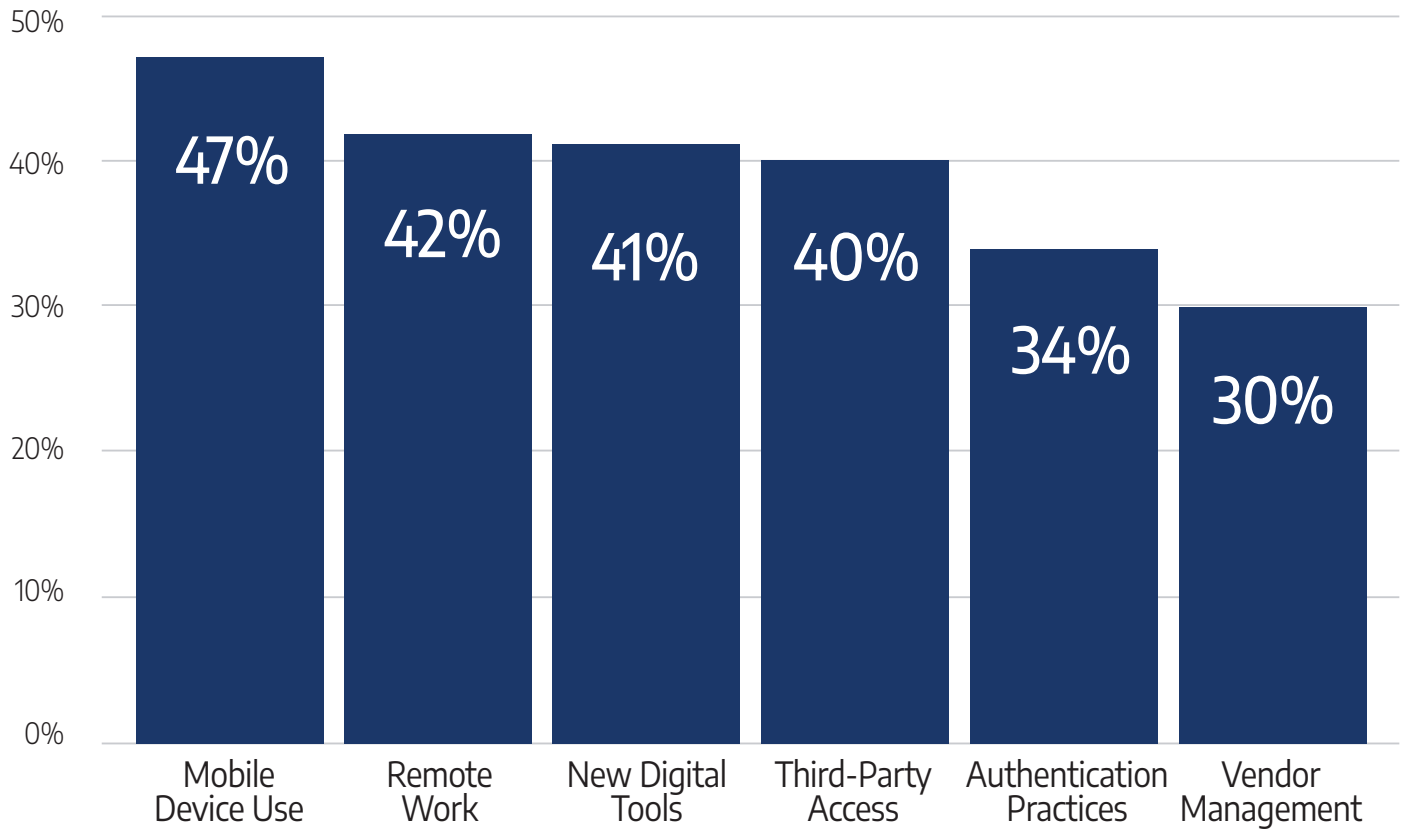
2. Authentication Practices

When it comes to strategies being deployed to serve their customers more safely, a majority of financial leaders (68%) report they are implementing two-factor authentication, followed by making customers register their own devices. Two-factor authentication usage is the highest among wealth management at 77%. Older methods such as one-time passwords (OTP) are not as popular, nor is requiring the use of geolocation. The OTP strategy has known security limitations, while geolocation is a more complex issue because it involves customer privacy and compliance. Although limiting the functionality that can be performed on mobile devices is being used by at least a third of organizations, it poses a customer experience challenge as the mobile channel grows, Introducing friction for the customer and increasing the risk of customer attrition.

3. Third-Party Access

Business leaders are keenly aware of the growing demands by customer-directed third-party applications seeking access to their data. Anytime a consumer uses an online tax service, e.g., H&R Block, a personal financial management app, e.g.,

Which elements of creating an overall cybersecurity plan do you consider the most challenging to implement?



Source: *Arizent State of Cybersecurity Survey 2022*

Intuit's Mint, or a digital mortgage provider, e.g., Rocket Mortgage, the third-party reaches out to a financial services company for access to the customer's own data. The challenge then becomes how to safely provide access and manage the process.

4. Vendor management

Find out about your vendors' technical safeguards, such as limits on data access, virus protection, idle browser session timeouts, strong password requirements and encryption of data at rest or in transit. They should have regularly updated software and firewalls, as well as accredited audits. Ask about their physical and administrative safety; for example, data backups and shredding and disposal procedures. You'll want to complete this due diligence with each vendor on a regular basis, requesting verifying information for your records.

5. New Digital Tools

Financial leaders expect that the rise in third-party data access will require them to adapt to this ever-expanding access point. More than half (58%) state that third-party data access will require new policies and practices to manage these third-party encounters. About half expect it will require changes in identity management practices and state it will require new customer validation procedures.

6. Mobile Device Use

Leaders are putting their resources into deploying two-factor authentication as a key strategy to serve their employees and third-party vendors more safely at 69% overall, followed by device registration at 51%, using OTPs at 41%, and geolocation and limiting mobile device functionality at 39% each. There are some notable differences within certain financial sectors in treating the different populations. In the insurance sector, device registration is the top strategy to serve customers more safely followed by two-factor authentication. However, when it comes to employees and vendors, two-factor authentication is the leading strategy, but device registration is second to last.

More than half (58%) state that third-party data access will require new policies and practices to manage these third-party encounters.

Training your staff and your clients

When SEC examiners evaluate a business' cybersecurity preparedness, they may focus on how well you've trained employees to be responsible and how the education is tailored to specific job functions.

Make training intentional and keep staff updated. Instead of two hours a year, you might consider implementing 30 minutes of training each month with varying topics such as recognizing phishing scams and fake calls from the IRS or client pretenders.

According to the Arizent survey, 4% of advisors have not invested in internal procedures, 52% have not invested in external help and 36% aren't aware of their firm's exact cybersecurity investment.

Get employees involved in writing and revising your policies and procedures for the six key cybersecurity areas. It may also help to set up leaders with specific knowledge and response roles for different kinds of security events your business faces.

Internal education and communication is necessary, but the responsibility extends to clients as well. The security of your operations is linked to the caution clients take with their information.

As you build client relationships, set some ground rules for secure communication, for example emailing to set up a phone call when discussing certain material. Teach clients how to recognize phishing scams and other threats that are beyond your business operation reach, but could still effect you in asset loss and data breach claims. Easy ways to educate clients and staff include sending articles and podcasts (try Cyberwire and Security Now), which outline cybersecurity news and practices.

Taking action in the event of a cyber attack

Even with extra meetings and careful measures by staff and clients, data encryption and software updates, errors can happen. A study by the Ponemon Institute found over a quarter of all data breaches in the financial sector were a result of human error.

There are several resources to review when planning, including FINRA's guide which outlines steps to take in case of a security event. You can first contain and mitigate an event by shutting down a system or disconnecting from a network, depending on the type of incident. Then, your team should identify affected assets within the organization, restore systems from clean backups or rebuild them from scratch, install patches, change passwords and tighten network perimeter security.

Investigate the extent of data and/or monetary loss and identify root causes, all the while keeping a log of this information for client communication and insurance claims purposes. And as soon as you think necessary, notify clients of the event and assure them you will make them whole by offering reimbursement or credit monitoring services. This is a way to assuage their future cybersecurity fears.

You may even want to visit your local FBI field office and get to know a nearby FINRA Regulatory Coordinator so you can plan collaboratively and proactively. It's useful to have investigators and regulators in your corner in the event of an attack or breach.

Use your resources by connecting with regulators and joining online groups (see the Financial Services Information Sharing and Analysis Center) to find threat and vulnerability information, conduct planning exercises and more.

Consider how investing in your cybersecurity plans can add to your value proposition. According to the Arizent survey, 4% of advisors have not invested in internal procedures, 52% have not invested in external help and 36% aren't aware of their firm's exact cybersecurity investment.

Allocating dollars and education, internally and externally, to cybersecurity measures could give your practice a competitive edge and the fortification your business needs to keep growing.

Protect your client data with Axos Advisor Services

At Axos Advisor Services we take our role as custodian seriously, providing several layers of state-of-the-art protection for investors and their financial advisors. We invest in industry-leading technology and ongoing employee training to help protect investor assets and ensure the integrity of our end-to-end security.

Our Information Security Program is reviewed by both an independent internal auditor and as part of the firm's ongoing regulatory examinations. Our comprehensive Information Security Program involves a three-pronged approach to digital security:

- **Channel protection.** We employ extensive security measures to block any attacker's attempts at entry to the Axos Advisor Services platform. First, we use the strongest firewalls available in the industry to guard the information housed in our servers. In addition, we require strong log-in credentials for authentication. Axos Advisor Services uses "challenge" and/or "response" tokens, as well as digital certificates to ensure appropriate verification. Whenever investor data is transferred digitally, it is protected with a high level of security protocols that leverage robust encryption tools, including 256-bit Secure Socket Layer (SSL) encryption.
- **Transaction monitoring.** Axos Advisor Services vigilantly reviews transaction data and scans for any abnormal or suspicious activity. We employ pattern analysis and other advanced analytical systems to detect suspicious account activity and deter unauthorized access.
- **Data privacy.** Axos Advisor Services' privacy policies and data governance procedures ensure that only the appropriate person who is servicing an account is allowed to view its data. All employees who handle sensitive information are pre-screened and trained in privacy and security.

At Axos Advisor Services, we have a strong culture of risk management. We continuously monitor our systems and controls, and work collaboratively with government agencies, law enforcement and other financial services firms to address potential threats. In addition, we regularly review, update and modify our policies and procedures to respond to new threats and to adapt to changes in technology.

For more information, email sales@axosadvisorservices.com, call 866-776-0218 or visit axosadvisorservices.com.