CAMBRIDGE

# Cyber Secure: Protecting Your Business in the Digital Age

In today's rapidly evolving digital landscape, cyber criminals are growing more sophisticated and dangerous. This trend is particularly concerning for financial advisors, a group that regularly handles confidential financial data and sensitive client information. For advisors, protecting client trust is critical, and a single cybersecurity lapse can have severe consequences for their business.

So, how can advisors stay ahead of these increasingly complex threats and keep clients, and themselves, safe and protected? One word defines all effective cybersecurity approaches: prevention. Not only does a proactive approach prevent most cyber attacks from breaking through, it helps advisors and their teams mitigate the issue quickly in the event that a data breach does occur.

This whitepaper outlines strategies for developing a strong cybersecurity plan to protect advisors and their clients in today's evolving digital landscape. But first, it's important to understand how recent advances in technology have opened the door to a new era of cyber risks.

For advisors, protecting client trust is critical, and a single cybersecurity lapse can have severe consequences for their business.

# NEW TECH, NEW CYBER THREATS

**75%**
**OF GLOBAL KNOWLEDGE WORKERS ARE NOW USING GENERATIVE AI, ACCORDING TO MICROSOFT.**

Technology and cybersecurity are closely linked. When technology advances, cyber criminals often gain access to new contact points they can exploit to deliver devastating damage to individuals and businesses that don't have strong cybersecurity protocols in place. As it stands, we happen to be in the middle of arguably the most innovative technology period in history. Artificial Intelligence (AI) often draws most of the headlines, but Cloud Computing, Machine Learning, Blockchain Technology, and Fintech solutions now have a major presence in our daily lives. The AI and machine learning tools being used to build robots and power autonomous vehicles are the same technologies making their way into so many of today's everyday experiences, from asking Siri for a recipe to uncovering new Netflix show suggestions and tracking health data on a smartwatch.

The use of generative AI solutions like ChatGPT alone has doubled in the last six months, with Microsoft reporting that 75% of global knowledge workers[1] now use it to assist with assignments. At a more granular level, roughly 60% of financial advisors[2] are using AI-powered tools for portfolio management, client communication, risk assessment, and more. This number continues to climb compared to previous years as AI becomes more widely adopted: at the time of McKinsey Global's 2022 Survey on AI, only 50% of business professionals[3] reported using AI. Moreover, the cloud computing market is expected to grow to $1 trillion by 2028[4], and more than 90% of companies[5] say they use cloud platforms to store information in some way.

# THE COSTS OF A CYBER ATTACK

The rapid growth and integration of these technologies into daily life, and their ability to be exploited by bad actors, only increases the importance of developing and maintaining an ironclad cybersecurity strategy. This rings especially true for financial advisors, who operate in one of the most heavily-targeted industries in the world and are entrusted by clients to safeguard valuable bank account information and confidential personal data.

SiteLock's analysis of more than seven million websites found that the average site is attacked nearly 180 times every day[6], and the consequences of a successful cyber attack are often devastating for businesses: 66% of consumers in one survey[7] said they would not trust a company that falls victim to a data breach. For advisors, this means a breach will lead to lost clientele.

Consider these additional points from IBM's 2024 *Cost of a Data Breach* report:[8]

The average cost of a data breach is **$4.88 million**, and 80% of these breaches result in exposure of customers' personally identifiable information (PII)

**75%** of year-over-year increases in average breach costs are due to the cost of lost business and post-breach response activities. In other words, customers leave.

The average cost of a breach in the financial industry is **25% higher** than the national average, coming in at $6.08 million

**83%** of organizations in an earlier IBM study experienced more than one data breach in 2022[9]

Those are just the financial costs. The following costs are also significant and have a profound impact on any business compromised by a data breach:

**Clients lose trust and leave**

**Value of intellectual property falls**

**Operational and productivity losses**

**Costs associated with requiring lost business assets**

Bottom line: Data breaches have the potential to set a business back for years. The financial, emotional, and operational consequences extend well beyond what most business owners realize, impacting revenue, reputation, and team morale. Recovering from a breach often requires significant resources, time, and trust-building with clients — all of which can take years to fully restore.

# HOW CYBER CRIMINALS STRIKE

Make no mistake: today's cyber threats are real. Attack techniques are only becoming more complex, and bad actors are increasingly using AI and social engineering tactics to exploit vulnerabilities. AI-powered attacks can be highly targeted and difficult to detect, while social engineering tactics, like phishing, rely on human trust to gain access to sensitive information.

Let's briefly look at a few strategies commonly used to attack businesses in financial services and other highly-targeted industries.

## Phishing

Some phishing attempts may use humor, but there's nothing to laugh about when it comes to the serious threats these attacks pose. A form of social engineering, phishing is a method of deceiving users into exposing login credentials to gain access to an internal network. The most common form of phishing is email phishing, where an email posing as legitimate communication is sent to victims. Interacting with any of the infected links or attachments in phishing emails could initiate the installation of malware on the target computer system. Per Deloitte, almost all breaches — 90% of them[10] — begin with phishing emails. Regular training can help associates identify and respond to phishing attempts before they cause major problems.

## Malware

Malware is a piece of code that is capable of copying itself in order to damage a computer, including corrupting the machine's internal systems or destroying data. Malware is an umbrella term that includes a variety of malicious software such as trojans, spyware, worms, ransomware, and viruses. These are all designed to disrupt, damage, or gain access to a computer or system. In the case of ransomware, the attacker uses malware to encrypt or lock data, preventing the owner from accessing it. The bad actor then demands a ransom payment in exchange for unlocking everything. Sometimes the attacker doesn't hold up their end of the bargain following a ransom payment. Other times, the malware is so poorly constructed that the files are permanently damaged. In fact, the chances of things "returning to normal" after a ransomware payment are slim to none: Forbes reported[11] that 92% of those who pay the ransom don't get all of their data back. Attacks like these affect businesses large and small — in 2021, a cybercrime gang called REvil allegedly stole confidential Apple product designs and threatened to release the blueprints if Apple didn't pay a $50 million ransom. Although the group did release minor schematics as proof of a breach, the threat was largely a bluff, and Apple did not pay the ransom.[12]

# STAYING PROTECTED: CYBERSECURITY BEST PRACTICES

Prevention is the cornerstone of any effective cybersecurity plan. To defend against today's sophisticated cyber threats, it's essential to implement strong security protocols across the organization and keep clients informed about the measures safeguarding their information with regular communications. Organizing regular training sessions to keep associates educated on new technology impacting the industry and how they can be implemented safely is one of the most effective preventive cybersecurity strategies business owners around the world have adopted. According to Stanford University[13], 88% of data breaches are caused by human error. Many attacks begin when somebody inside the organization clicks on a link that has been compromised by bad actors. These links are loaded with malware and act as trojan horses, delivering damage once they are allowed inside the organization. Regular training helps associates recognize phishing attempts, malware infections, and understand the importance of strong passwords.

A few other best practices that contribute to a preventative cybersecurity approach include:

## Build Strong Passwords

The most used password worldwide in 2022 was "password." Just as unfortunate — 52% of people[14] use the same password for multiple accounts. Don't make these mistakes! At Cambridge, we recommend creating strong passwords that are 12-15 characters in length and include a combination of letters, numbers, and symbols. Password management services, such as LastPass, are also handy; these platforms are designed to remember passwords and keep them protected.

## Use Multi-Factor Authentication (MFA)

In today's world where cyber attacks are growing more and more sophisticated, passwords alone are not enough to protect data and files. All accounts and platforms storing sensitive client or business-related information should be protected with multi-factor authentication (MFA). This provides an additional layer of safety and security beyond passwords.

## Encrypt Data

Advisors handle a significant amount of sensitive information, such as personal details, bank account information, and other financial data. It's important to ensure this data is encrypted in storage. Encryption is a process that uses mathematical models to scramble data so only authorized parties can access it. A few practical ways to do this include:

- Use protocols like HTTPS for web communication and VPNs for remote access. These protocols encrypt the data during transit, which prevents interception by attackers.
- Use secure communication channels (encrypted emails and messaging portals) when sharing client information. For example, Microsoft products (e.g. Outlook and Teams) are encrypted communication channels.

## Secure the Cloud

Most companies now use cloud services to store data and files. Advisors who are already leveraging some kind of cloud platform should ensure that strong access controls are in place to prevent individuals outside of the company from accessing files saved in the cloud. Above all, avoid using personal devices or unsecured cloud services to store information, especially client data. These are easily exploited by attackers.

## Protect Devices and Avoid Public Wi-Fi

Leverage firewalls, antivirus software, and regular software updates to protect all of the firm's devices. Anybody working remotely will need to be hooked up to a VPN service. Avoid using public Wi-Fi unless connected to a VPN; attackers are always lurking on public Wi-Fi. In fact, nearly half of respondents in one Forbes cybersecurity study[15] reported having their security compromised while using public Wi-Fi. This is an important reminder for advisors who travel often and work in cafes, restaurants, airports, and hotels.

## Use Artificial Intelligence (AI), Intelligently

There's no doubt that AI is advancing at an increasingly rapid pace; businesses everywhere are adopting it. Used appropriately, AI can help advisors save a significant amount of time — but it should be handled with extreme caution. Use it to help craft emails, write social media posts, and generate business ideas. But DO NOT enter client information or confidential business data into AI programs like ChatGPT. The risks of interception are far too great, and entering confidential information into programs like these can compromise client privacy.

## Consider Cybersecurity Insurance

Cybersecurity insurance is a policy designed to help businesses mitigate the financial impact of cyberattacks and data breaches. It typically covers costs associated with recovery of these incidents, as well as legal fees, regulatory fines, and compensation to affected parties. While no one wants to find themselves in a situation where it needs to be used, having a policy in place adds another layer of protection. There are a wide variety of service providers that offer policies specifically tailored to financial advisors and their firms.

In the end, cybersecurity goes well beyond preventing bad actors from lend, accessing files and data; it's ultimately about protecting clients from harm and keeping their dreams, ambitions, and future safe.

At Cambridge, we take that responsibility seriously. Advisors partnered with Cambridge have access to a wide variety of educational resources, from FAQs answering some of the most important cybersecurity questions to detailed best practice guides covering topics such as mobile computing, phishing identification, wireless security setup, and more. Through Source, our in-house outsourcing solution, advisors can receive one-on-one support with cybersecurity monitoring, offsite cloud backup and restoration, remote machine management, Microsoft 365 account management, email filtering, and network protection.

The number of attacks on financial services firms are expected to increase in the years ahead as cyber criminals look to leverage the new technology available to them. By prioritizing cybersecurity, advisors can keep their clients safe, protect their reputation in the marketplace, and prevent significant business setbacks.

## About Cambridge

Cambridge Investment Group, Inc. is a financial solutions firm focused on serving independent financial professionals and their investing clients. Cambridge offers a broad range of choices for independent financial professionals regarding solutions for advice, growth, technology, and independence. Cambridge's national reach includes: Cambridge Investment Research Advisors, Inc. – a large corporate RIA; and Cambridge Investment Research, Inc. – an independent broker-dealer, member FINRA/SIPC, that is among the largest internally controlled independent broker-dealers in the country.

Cambridge Investment Research, Inc.
1776 Pleasant Plain Road | Fairfield, Iowa 52556
877-688-2369 | JoinCambridge.com

CAMBRIDGE

[1]Bishop, T. (2024). Microsoft Study: 75% of Knowledge Workers Using AI at Work, Nearly Doubling in Six Months. *GeekWire*. Find here.
[2]Business Wire Staff. (2024). AI Adoption Gains Traction Among Financial Advisors, Highlights Opportunities for Enhanced Client Service and Efficiency: Horsesmouth Survey. *Business Wire*. Find here.
[3]McKinsey & Company Staff (2022). The State of AI in 2022 — And a Half Decade in Review. *McKinsey & Company*. Find here.
[4]Edge Delta Staff. (2024). How Many Companies Use Cloud Computing in 2024? *Edge Delta*. Find here.
[5]Cloud Security Alliance Staff. (2023). State of Financial Services in Cloud. *Cloud Security Alliance*. Find here.
[6]SiteLock Staff. (2022). SiteLock Website Security Report. *SiteLock*. Find here.
[7]Vercara Staff. (2023). Vercara Research: 75% of U.S. Consumers Would Stop Purchasing from a Brand if it Suffered a Cyber Incident. *Vercara*. Find here.
[8]IBM Staff. (2024). Cost of a Data Breach Report 2024. *IBM*. Find here.
[9]Huang, K., Wang, X., Wei, W., & Madnick, S. (2023). The Devastating Business Impacts of a Cyber Breach. *Harvard Business Review*. Find here.
[10]Deloitte Staff. (2020). 91% of all Cyber Attacks Begin With a Phishing Email to an Unexpected Victim. *Deloitte*. Find here.
[11]Winder. D. (2021). Ransomware Reality Shock: 92% Who Pay Don't Get Their Data Back. *Forbes*. Find here.
[12]Winder. D. (2021). Ransomware Gang Demands $50 Million For Apple Watch And MacBook Pro Blueprints. *Forbes*. Find here.
[13]Breachsense Staff. Why Are So Many Data Breaches Caused by Human Error? *Breachsense*. Find here.
[14]Security Staff. The Most Used Password in 2022 was 'Password'. *Security Magazine*. Find here.
[15]Haan, K. (2024). The Real Risks of Public Wi-Fi: Key Statistics and Usage Data. *Forbes*. Find here.