MassMutual Ascend

Beyond Annuities: Understanding cybersecurity for financial professionals

For producer use only. Not for use in sales solicitation.

Not a bank or credit union deposit or obligation • Not FDIC or NCUA-Insured • Not insured by any federal government agency • May lose value • Not guaranteed by any bank or credit union

With evolving technology, growing threats and a constant learning curve, cybersecurity can be difficult to navigate as a financial professional. But it doesn't have to be. In 2025, **60% of data breaches were the result of human error[1].** Taking simple steps to understand common cybersecurity threats and how to combat them can significantly reduce your risk of cyberattacks.

In this brochure, we'll look at common cyber threats, prevention strategies and cybersecurity best practices.

[1] 2025 Data Breach Investigations Report executive summary. (2025). https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

For producer use only. Not for use in sales solicitation.

The impact of cybersecurity incidents

Cybersecurity attacks are costly. Between lost money, time, resources and even trust, there's a lot at stake. Consider the following ways a cybersecurity incident could impact your practice.

Financial losses

On average $4.4 million is lost during a cyberattack[2]. This includes everything from stolen funds, lost revenue and remediation costs.

Diminished client trust

When client data is compromised, so is client confidence in your ability to protect their personal information.

Operational disruptions

It takes time to reset after a cyberattack. Business productivity can be impacted by system outages, data loss and more.

Regulatory consequences

You could face legal or regulatory consequences for cyber security incidents, especially for preventable attacks.

[2] Cost of a data breach 2025. IBM. (2025). https://www.ibm.com/reports/data-breach

For producer use only. Not for use in sales solicitation.

Understanding common cyber threats

From suspicious emails to fake text messages, cyber threats are everywhere. But having a basic understanding of the most common cyber security concerns can prepare you to recognize, report and avoid potential cyber threats. Let's look at some of the most common cyber threats, and how they happen.

Social Engineering is an umbrella term for when a hacker tricks someone into giving up information or access, and typically plays on human emotions like trust, fear or urgency. Social engineering can be done physically and digitally, including the methods listed below.

Threat	Description	Additional Information
Phishing	Fake emails or messages that look real, ask the user to click a link or share information.	Phishing is the most common type of social engineering, accounting for more than 90% of successful cyberattacks[3] .
Baiting	The promise of free items or deals that lead to malware.	Infected flash drives are also commonly used in baiting.
Spoofing	Faking an identity, website or phone number to look trustworthy.	Attackers often spoof email addresses, IP addresses GPS signals, and caller ID as well.
Scareware	Pop-ups suggesting a computer is infected and urging the user to download fake software.	These attacks often appear to be from real companies or offering real products.
Shoulder surfing	Watching someone's online activity while in public stealing login details.	Using a privacy screen to block your screen from others can limit these attacks.
Deepfakes	A new type of social engineering attack that uses AI or machine learning to fabricate pictures, videos or audio recordings.	Unlike other types of social engineering, deepfakes can be extremely difficult to detect.

[3] Be cyber smart: Get your "Shields Up" Simple Steps for Safety Online . (n.d.). https://www.cisa.gov/sites/default/files/2023-02/cisa_fact_sheet_4_things_cyber_english_508.pdf

But not all cyberattacks rely on social engineering. Rather than tricking an individual to obtain access, some cybercrimes target weak technology or outdated software. Below are some examples.

Threat	Description	Additional Information
Account takeover (ATO)	Attackers gain unauthorized access to someone's online account, then make changes to the account, authorize transactions, or use it as a launchpad for other scams.	Account takeovers are conducted using stolen credentials from emails, bank accounts, social media profiles and more.
Denial of Service	A threat actor prevents legitimate users from accessing a web services such as websites or account log-ins.	Attackers slow or shutdown their target by overwhelming it with traffic.
Insider threats	The actions of an authorized user intentionally or accidentally harming the organization through a cyber incident.	This can come from Malicious Insiders, who deliberately cause harm and Negligent Insiders, who unintentionally cause harm.
Ransomware	Attackers gain access to a system then encrypt and lock users out of their files. Then they can demand payment or other favors in exchange for reinstating access.	These attacks can be costly and often cause major operational disruptions and loss of critical data.

WHO COMMITS CYBERATTACKS?

The most common sources of cyberattacks are cybercriminals (financially motivated), hackers or 'hacktivists' (promoting a political agenda), nation-state actors (government funded) and insider threats.

For producer use only. Not for use in sales solicitation.

Combating cyber threats

Your people are your most important asset

People are the first line of defense against cyber threats and play a crucial role in maintaining strong cybersecurity. With social engineering attacks steadily rising, taking steps to mitigate potential human error is an essential first step in building your cybersecurity toolkit.

- **Prioritize education.** Ensuring your team can identify and avoid the most common threats mitigates your risk of falling victim to them.
- **Create a culture of cybersecurity.** Empowering team members to take ownership of their role creates an essential layer of security against potential attacks.
- **Require regular training.** Regularly training your team on Cybersecurity will ensure your employees are equipped with the most up-to-date information, and keeps best practices top of mind.

Consistency is key

Cybersecurity is a practice, not a one-time event. Performing regular maintenance and establishing routines are necessary for maintaining good cyber hygiene and preventing potential breaches. Let's explore some cyber hygiene best practices.

Passwords

DO

- Use a combination of letters, numbers and special characters to form your password
- Include eight or more characters in your password

DON'T

- Reuse old passwords
- Share your password with others
- Use personal information such as birthdates or pet names in passwords

Data Backups

DO

- Follow the 3-2-1 rule
  - Three copies of data
  - Two storage types
  - One copy of data stored in an alternate location

DON'T

- Use only one backup type. Instead, use a combination of backups such as cloud storage, internal hard disk drive, and removable storage media

Secure Devices and Networks

DO

- Protect your WIFI with a strong password
- Lock your devices, with biometric tools if available
- Apply "patches" (software updates) as soon as they become available to ensure security

DON'T

- Use public Wi-Fi for work tasks without a VPN (virtual private network)
- Share sensitive information with AI tools

For producer use only. Not for use in sales solicitation.

Take a layered approach

It's important to supplement your cybersecurity framework with technology that can match the speed and scale of attackers. There are a variety of options on the market that offer around-the-clock cybersecurity monitoring, threat prevention, and other specialized program management. These tools provide essential oversight and can help ease the burden created by overwhelming digital threats.

Consider using one or more of the following tools to bolster your cybersecurity efforts.

Tool	What?	How?
Multifactor Authentication	Requires users to verify their identity in more than one way.	Users are verified using methods such as passwords, phones/tokens, or biometrics.
Firewall protection	Software or hardware that protects your computer from attackers.	Restricts unnecessary traffic and blocks potential threats.
Data encryption	Secures data through information masking.	Converts information into an unreadable code (ciphertext) that requires a key to access.
Email filters and anti-phishing software	Blocks emails with malware, spyware, phishing attempts, etc.	Scans and filters out harmful emails, preventing them from reaching users.
Remote monitoring and management software	Provides oversight and administrative assistance for online systems.	Software monitors activity, triggering alerts and running programs as needed.

For producer use only. Not for use in sales solicitation.

The impact of cybersecurity incidents

Like many parts of the financial industry, there are certain requirements financial professionals must meet when it comes to cybersecurity. These requirements (or standards) ensure client data is protected and that the appropriate steps are taken when an incident occurs.

Let’s review some common cybersecurity regulations, and how they might play a role in your practice.

Gramm-Leach-Bliley Act: This law ensures customer privacy by requiring financial institutions to maintain an information security program, explain third-party information-sharing practices and report data breaches to consumers.

Cybersecurity guidance from FINRA: The Financial Industry Regulatory Authority (FINRA) provides cybersecurity guidelines and conducts evaluations of member organizations’ cybersecurity risk management efforts.

State-specific regulations: Cybersecuritylaws provide guidance and set regulations on issues such as data security, data breach notifications, incident response and reporting cybersecurity incidents.

Cybersecurity insurance: Coverage typically includes a combination of first-party coverage to pay for business costs (incident response, operational disruptions, ransom payments) and third-party coverage to pay for external costs (legal defense and settlements, regulatory penalties).

[4] Cybersecurity 2025 legislation. (2025, October 10). https://www.ncsl.org/technology-and-communication/cybersecurity-2025-legislation

For producer use only. Not for use in sales solicitation.

In today’s ever-evolving, digital-first environment, it’s clear that cyber threats are here to stay - and will continue to grow more intelligent and complex.

By taking intentional, proactive steps to recognize and thwart potential cybersecurity threats, you can help ensure the security of your practice, uphold your reputation, and most importantly, maintain client confidence.

At MassMutual Ascend, we have educational tools and resources to help facilitate conversations with your clients about obstacles they may face as they plan ahead. The Beyond Annuities value-add program was designed to help your clients as they plan for a secure financial future. **Learn more and find additional resources at MMAscendConnect.com/BeyondAnnuities.**

For additional cybersecurity resources, visit the Cybersecurity Infrastructure & Security Agency at CISA.gov.

For producer use only. Not for use in sales solicitation.

For producer use only. Not for use in sales solicitation.

This information is not intended or written to be used as legal or tax advice. It was written solely to provide general information and support the sale of annuity products. A taxpayer should seek advice on legal or tax questions based on his or her particular circumstances from an attorney or tax advisor.

For use with contract forms, P1020203NW, P1020212ID, ICC25-P1174525NW, P1138919NW, P1138919ID, ICC24-P1172524NW, P1088011NW, P1088011ID, P1088111NW, P1088111ID, ICC25-P1174925NW, ICC24-P1172024NW, ICC21-P1151621NW, P1074514NW, P1074514ID, ICC25-P1470025NW , ICC21-P1152021NW, ICC21-P1152121NW, ICC21-P1476721NW, P1140119NW, P1140119ID, P1140219NW, P1140219ID, P1146620NW, P1146620ID, P1110416NW, P1110416ID, ICC20-P1144420NW and ICC20-P1144420NW-NoMVA, ICC20-P1144520NW and ICC20-P1144520NW-NoMVA, ICC20-P1474420NW and ICC20-P1474420NW-NoMVA, P1134618NW, P1134618ID and P1134618ID-NoMVA, P1112916NW, P1112916ID, P1129918NW, P1129918ID and P1129918ID-NoMVA, ICC24-P1825224NW, ICC24-P1833624NW, ICC24-P1850824NW, ICC24-P1841724NW, and ICC24-P1841624NW. Contract form numbers may vary by state.

Products issued by MassMutual Ascend Life Insurance Company^{SM} (Cincinnati, Ohio), a wholly owned subsidiary of Massachusetts Mutual Life Insurance Company (MassMutual).

All guarantees subject to the claims-paying ability of MassMutual Ascend Life Insurance Company.

This content does not apply in the state of New York.

For producer use only. Not for use in sales solicitation.

NOT A BANK OR CREDIT UNION DEPOSIT OR OBLIGATION • NOT FDIC OR NCUA-INSURED • NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY • MAY LOSE VALUE • NOT GUARANTEED BY ANY BANK OR CREDIT UNION

MassMutual Ascend