REVISED NOVEMBER 2025

Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies

CYBER RISK TOOLKIT

American Academy of Actuaries
Committee on Cyber Risk, Casualty Practice Council

American Academy of Actuaries
ACTUARY.ORG

The American Academy of Actuaries' Cyber Risk Toolkit, developed by the Academy's Committee on Cyber Risk, is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure. This toolkit is intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.

While the paper that follows stands alone, the complete toolkit offers a cohesive overview of the challenges posed in the cyber insurance market. The toolkit will be updated periodically to reflect new and emerging work from the committee.

The American Academy of Actuaries is a 20,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policy makers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues. The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

American Academy of Actuaries

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

© 2025 American Academy of Actuaries. All rights reserved.

Any references to current laws, regulations, or practice guidelines are correct as of the date of publication.

Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies

Revised November 2025

Introduction[1]

Data breach, hacking, and cyberattack are all common terms used frequently—especially in the media—but mainly when they pertain to large organizations or the compromised accounts of household names on X (formerly Twitter). However, individuals who use cellphones, computers, or any digitally connected devices face many of the same risks. In fact, in 2024 the FBI's Internet Crime Complaint Center (IC3) reported receiving 859,532 complaints, representing potential losses of $16.6 billion.[2] Much like business entities, individuals can't completely eliminate these risks without living completely off the grid. Both businesses and individuals can, however, take measures to help mitigate their risk from cyberattacks. This paper will help identify common entry points of cyberattacks from an individual's perspective and examine steps to minimize their risk of being hacked.

Personal Cyber Risk Profile

Types of Personal Cyber Risks

Attackers can infiltrate or gain access to an individual's information in many ways. Some of the most common ways include:

- **Phishing schemes:** Attackers can create emails, text messages, or phone calls that look and sound like they are from banks or other lending institutions that ask for specific account information to gain access. One common scheme impacting individuals who are buying a home includes attempting to convince victims to wire their closing costs to attackers. With the rise of GenAI tools such as ChatGPT, drafting these phishing emails has become easier for criminals to create, along with creating content that is hard to distinguish from legitimate messages for most individuals.

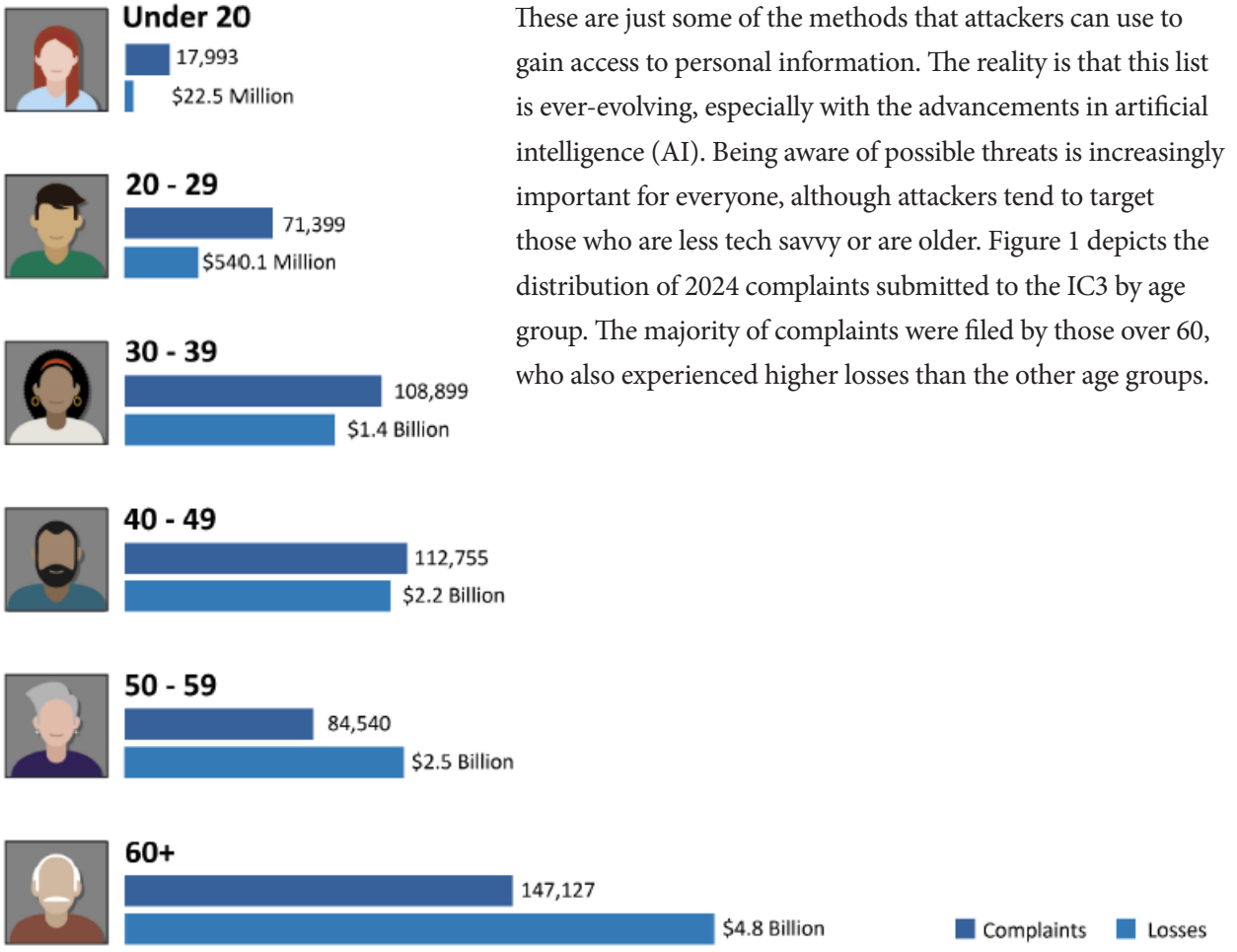
1 This paper references a few specific products and services. The Academy does not recommend or encourage the use of any particular service, company, or product. They are referenced as examples of what may be available in the marketplace. Individuals interested in a particular type of service should thoroughly investigate various providers and products for comparison and determine which, if any, meet their needs.
2 "Federal Bureau of Investigation Internet Crime Report"; Internet Crime Complaint Center; 2024.

- **Social engineering:** Attackers can scour social media sites to find personal information about potential victims. Attackers use this information to impersonate victims and extract trusted information from friends or family members. They then use this information to gain access to victims' or victims' acquaintances' financial accounts or other sensitive information.

- **Wi-Fi network hacking:** There are many tools available online that allow attackers to gain access to an individual's home Wi-Fi network. Once attackers have access to the home's network, they can access financial information and any other sensitive information the user may have on their computer.

- **Malware, spyware, and ransomware:** By clicking a malicious link on a website or in an email, a small piece of software can be unknowingly installed on a user's computer or phone. This software can track everything a user does on that device or even take it over completely. In ransomware attacks, the user may have to pay attackers to regain access.

Figure 1



These are just some of the methods that attackers can use to gain access to personal information. The reality is that this list is ever-evolving, especially with the advancements in artificial intelligence (AI). Being aware of possible threats is increasingly important for everyone, although attackers tend to target those who are less tech savvy or are older. Figure 1 depicts the distribution of 2024 complaints submitted to the IC3 by age group. The majority of complaints were filed by those over 60, who also experienced higher losses than the other age groups.

Personal vs. Commercial Risks

For the most part, the types of risks faced by individuals and companies are similar. For example, hackers may try to infiltrate an organization's network by sending a phishing email appearing to come from the CEO, requiring urgent action such as a wire transfer[3], or they may perform a brute-force attack, using trial and error to guess a password. Once inside the network, attackers can cripple a company's operations.

Attackers may use many of the same methods to gain access to a business's network as they would to gain access to an individual's network. Once they have accessed an individual's network, the type of losses that can occur are generally comparable to those experienced by corporations. A recent paper published by the Society of Actuaries' Research Institute[4] groups the risks associated with an attack on an individual's smart home system into the following categories:

- **Data breach:** Data breach risk is the exposure of personal private user data that can be collected from an individual through their electronic footprint. It can be caused by exploitation of vulnerabilities in smart devices or malware attacks.

- **Loss of use:** Loss of use risk refers to blockage of data recovery, repair to a device, and system restoration due to malware or denial-of-service (DoS) attacks.

- **Ransomware:** Ransomware risk refers to being locked out of your device until you pay a ransom.

- **Cyber extortion:** Cyber extortion occurs when there are threats to release an individual's private videos, photos, financial information, or activities for financial gain. Another variant of this attack is when bad actors gain access to a social media account and demand payment to return control of the account back to the original owner.[5]

- **Online fraud:** This risk is the direct financial losses (stolen account funds, unauthorized use of banking or credit cards, phishing schemes, etc.) caused by cyberattacks. One increasingly common example of this over 2024 and 2025 has been phishing text messages related to unpaid tolls.[6]

3 Business Email Compromise (BEC) & Healthcare; Department of Health and Human Services; May 16, 2024.
4 "Red Teaming Analysis of a Catastrophic Cyber Attack on Critical Infrastructure"; Society of Actuaries Research Institute; 2023.
5 "Account Takeover Incidents are Rising: How to Protect Yourself"; Jan. 2, 2025; Security.org.
6 Got a text about unpaid tolls? It's probably a scam; Federal Trade Commission; Jan. 17, 2025.

- **Theft:** Theft is the physical loss incurred by cyberattacks on security systems. An example of this would be if the attacker unlocks a smart lock and steals items from an individual's home.

- **Cyberbullying:** Cyberbullying is another potential risk for both individuals and organizations that may arise from being connected through social media or other types of digital communications. This type of attack does not involve hacking into an individual's or a company's devices or network. Instead, it comes in the form of bullying or intimidating someone online, by text, through apps, or on social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or malicious content.[7] This can result in potential financial losses (such as job loss), reputational damage, and health impacts, as cyberbullying has been associated with self-harm, mental and behavioral health issues, and social isolation.

Each of the loss types above can cause varying degrees of harm to an individual. While the size of any given loss in total dollar amount may not be comparable between individual and commercial cyberattacks, the impact on an individual may be greater and longer lasting. An individual could lose the entirety of their savings to a phishing scheme, whereas an organization may be better positioned to absorb the potential financial losses or have insurance that offers some protection.

With more employees working remotely, the line between personal and commercial cyber risks has increasingly blurred. For example, if an individual is using a company-issued laptop but is connected to their home router, the responsibility of a loss may depend upon how the attacker infiltrated the system. If someone hacks a home Wi-Fi network, the individual could be held responsible. Should an individual click on a suspicious link in a company email, the responsibility for any resulting fallout or financial loss may lie with the employer.

7 "What Is Cyberbullying"; StopBullying.gov; Oct. 7, 2024.

Personal Cyber Risk Mitigation Strategies

While it is impossible to completely eliminate all personal cyber risk, individuals can use many of the same mitigation tactics and strategies that businesses use to mitigate their risk and protect themselves online.[8] For example, individuals can:

- Keep software, hardware, and firmware up to date;
- Avoid opening suspicious emails;
- Use anti-virus and anti-malware software;
- Use a VPN to privatize internet connections;
- Change passwords often, avoiding easy-to-guess or obvious options;
- Enable two-factor authentication;
- Use biometric logins on mobile devices; and
- Connect IoT (Internet of Things) devices to secure networks.

What if an individual's home network or computer is hacked? Are there products or services that may help? There are two forms of protection that could assist: passive and reactive. Passive solutions constantly check a network for potential attacks or scour the dark web to check if any data has been leaked or sold. Reactive solutions are products that help monitor an individual's credit score to determine whether their financial accounts have been hacked.

Both options work well for alerting an individual after their information has been stolen or the network has been attacked, but the main drawback is that direct financial consequences may have already occurred. For example, having been made aware of the attack after it happens, an individual may not be compensated for any financial loss or the consequences of the network being attacked.

The products and services mentioned above can serve as indicators of potential loss. A personal insurance product could help provide protection should the individual experience a loss from such an attack. For example, suspicious credit score activity reported by credit monitoring companies may prompt an individual to take corrective action, including closing accounts, opening new accounts, or recovering funds that have been fraudulently spent on an individual's credit account.

8 21 Cybersecurity Tips and Best Practices For Your Business; TitanFile; 2021.

There are personal cyber insurance products currently available designed to help an individual recoup such losses. Some insurers offer a personal cyber insurance product that offers protection against cyberbullying and cyberattacks. These policies offer financial assistance coverage for the reimbursement of funds that have been taken and are nonrecoverable in full. Individual cyber insurance products that cover cyberbullying cover the costs of counseling, provide security measures to help stop the bullying, sometimes offer protection and emotional/physical support if the bullying is being done by an immediate family member, and in other situations, pay for the costs of damages (i.e. awarded through court proceedings) or the cost of the defense of an individual in a cyber bullying case if the insured was the person accused of bullying.[9]

Personal Cyber Insurance Policy Coverage

Personal cyber liability products tend to cover a variety of perils. Some of the main items covered include:

- Cyber Extortion
- Cyber Financial Fraud
- Deceptive Transfer Fraud
- Breach of Privacy
- Cyberbullying
- Loss of Use from Cyberattacks
- Identity Theft
- Data Restoration
- Device Replacement

As mentioned above, these coverages are designed to protect the customer and help them regain their data in the event that someone infiltrates their network or creates fraudulent online transactions. These coverages can also help recoup losses associated with fraudulent charges and pay ransoms when data is locked due to a ransomware attack.

Type of Personal Cyber Policies

The two most common ways to obtain personal cyber coverage are either purchasing a personal cyber endorsement to a homeowner's insurance policy or buying a stand-alone policy that covers cyber liability claims.

9 "Cyberbullying Protection"; Chubb; 2023.

Endorsement to Homeowners Policy

An easy way to add cyber protection to a risk management portfolio is to add a cyber protection endorsement to a homeowner's policy. Most standard homeowner's policies cover some forms of fraud, but not all cyberattacks are covered. These policies generally just broaden the coverages offered by the homeowner's policy to additionally cover cyberattacks.[10]

These types of policies are relatively easy to add and, for the most part, require a limited amount of additional information to write the endorsement. Some policies charge a set base rate with simple increased limits factors until the desired coverage amount is met. This process requires no additional underwriting information from the insured.

A potential downside to the endorsement policy can occur if a homeowner's policy uses prior claims as a rating indicator. If someone is the victim of a cyberattack, their homeowner's rates could increase due to the new claim. This could also be true for rating factors that apply to the whole homeowner's premium, including endorsements. For example, if a territory rating factor applies to the whole premium inclusive of endorsements, then the cyber premium would increase as well.

Stand-Alone Policy

An alternative to the homeowner's endorsement form of coverage is a stand-alone personal cyber insurance policy. These policies are generally more flexible and capable of covering a broader range of perils. For example, a search of personal cyber policies shows policies covering all the perils previously listed, as well as[11]:

- Crypto Currency Theft;
- Data Breach Coverage;
- Well-being Costs;
- Relocation Costs;
- Legal Service Fees;
- Smart Devices and Other Wearables Coverages.

These policies provide specialized coverage, offering a means to remain safe while online. Some policies offer the opportunity to speak with a cyber expert, who may answer any questions, as well as offer online protections such as anti-virus and malware protection.

10 "What Is Personal Cyber Insurance?"; *U.S. News and World Report*; Aug. 8, 2025.
11 "Personal Cyber Insurance: Peace of Mind Online and Off"; NFP.

These policies may be subject to more strenuous underwriting and the rating algorithms used may more closely resemble those of personal automobile products, with a base rate that may be modified by rating factors.

Personal Cyber Insurance Rating Characteristics

Given the relative infancy of the personal cyber insurance product and the low frequency/low severity nature of most cyber claims, creating a sophisticated rating plan that segments risk better is difficult. If an insurer were to introduce a new rating variable, most levels of that variable would have a limited number of claims. This would mean that the data would not yet be credible. Current rating plans used throughout the industry consider variables such as:

- Deductibles
- Limits
- Risk Reduction Techniques, which may include access to:
    - Credit Monitoring
    - Fraud Alerts
    - Dark Web Monitoring
    - Security Scoring
    - Security Education/Training
    - Software Patch Management
    - Antivirus
    - Firewall
    - VPN
    - Multi-Factor Authentication
    - Vulnerability Alerts
    - Endpoint Protection
    - Data Encryption
- Number of Named Insureds
- Annual Payment Discount
- Net Worth

Risk reduction techniques have some qualitative considerations, similar to schedule rating in a workers compensation policy. These are open to some level of underwriting judgment. Once personal cyber policies are in place for a longer period and more data has become available, rating plans will become more sophisticated, with more rating variables and nuanced rating rules.

Personal Cyber Trends

According to the 2024 IC3 study[12], the number and severity of personal cyber incidents are increasing rapidly. Investment-related cyberattacks—designed to entice individuals with the promise of lucrative returns on their investment—have experienced the biggest increase in incidence rates over the past 12 months. For example, an individual may receive a phone call or email offering a guaranteed large return on any monies invested in a specific opportunity.

Sometimes this opportunity is in the form of speculative investments or cryptocurrencies. The number of complaints for investment-related crimes doubled between 2022 and 2023, while most other crime types remained stable during the same time period. The chart below shows the number of complaints issued to IC3 for each of the past 4 years by each crime type, the total estimated claim cost by IC3, and the cost per complaint. Figure 2 shows both personal and commercial complaints. Some forms of crime are, by nature, more personal.[13] This includes investment schemes, harassment/stalking, and non-payment/non-delivery of online goods or services.

12 Federal Bureau of Investigation Internet Crime Report"; Internet Crime Complaint Center; 2024.
13 Federal Bureau of Investigation Internet Crime Report"; Internet Crime Complaint Center; 2023.

Figure *2*

	Complaint Count				Complaint Cost					Severity		
Crime Type	**2024**	**2023**	**2022**	**2021**	**2024**	**2023**	**2022**	**2021**	**2024**	**2023**	**2022**	**2021**
Advanced Fee	7,097	8,045	11,264	11,034	102,074,512	134,516,577	104,325,444	98,694,137	14,383	16,721	9,262	8,945
BEC	21,442	21,489	21,832	19,954	2,770,151,146	2,946,830,270	2,742,354,049	2,395,953,296	129,193	137,132	125,612	120,074
Botnet	587	540	568	N/A	8,860,202	22,422,708	17,099,378	N/A	15,094	41,524	30,105	N/A
Confidence/ Fraud/Romance	17,910	17,823	19,021	24,299	672,009,052	652,544,805	735,882,192	956,039,739	37,521	36,613	38,688	39,345
Credit Card/ Check Fraud	12,876	13,718	22,985	16,750	199,889,841	173,627,614	264,148,905	172,998,385	15,524	12,657	11,492	10,328
Crimes Against Children	4,472	2,361	2,587	2,167	519,424	2,031,485	577,464	198,950	116	860	223	92
Data Breach	3,204	3,727	2,795	1,287	364,855,818	534,397,222	459,321,859	151,568,225	113,875	143,385	164,337	117,769
Employment	20,044	15,443	14,946	15,253	264,223,271	70,234,079	52,204,269	47,231,023	13,182	4,548	3,493	3,097
Extortion	86,415	48,223	29,416	39,360	143,185,736	74,821,835	54,335,128	60,577,741	1,657	1,552	1,847	1,539
Government Impersonation	17,367	14,190	11,554	11,335	405,624,084	394,050,518	240,553,091	142,643,253	23,356	27,770	20,820	12,584
Harassment/ Stalking	11,672	9,587	11,779	N/A	10,611,223	9,677,332	5,621,402	N/A	909	1,009	477	N/A
Identity Theft	21,403	19,778	27,922	51,629	174,354,745	126,203,809	189,205,793	278,267,918	8,146	6,381	6,776	5,390
Investment	47,919	39,570	30,529	20,561	6,570,639,864	4,570,275,683	3,311,742,206	1,455,943,193	137,120	115,499	108,479	70,811
IPR/Copyright and Counterfeit	1,583	1,498	2,183	4,270	8,715,512	7,555,329	4,591,177	16,365,011	5,506	5,044	2,103	3,833
Lottery/ Sweepstake/ Inheritance	3,690	4,168	5,650	5,991	102,212,250	94,502,836	83,602,376	71,289,089	27,700	22,673	14,797	11,899
Malware	441	659	762	810	1,365,945	1,213,317	9,326,482	5,596,889	3,097	1,841	12,239	6,910
Non-Payment/ Non-Delivery	49,572	50,523	51,679	82,478	785,436,888	309,648,416	281,770,073	337,493,071	15,844	6,129	5,452	4,092
Other	12,318	8,808	9,966	12,346	280,278,325	240,053,059	117,686,789	75,837,524	22,754	27,254	11,809	6,143
Overpayment	2,705	4,144	6,183	6,108	21,452,521	27,955,195	38,335,772	33,407,671	7,931	6,746	6,200	5,469
Personal Data Breach	64,882	55,851	58,859	51,829	1,453,296,303	744,219,879	742,438,136	517,021,289	22,399	13,325	12,614	9,976
Phishing/ Spoofing	193,407	298,878	321,136	342,494	70,013,036	18,728,550	160,015,411	126,383,513	362	63	498	369
Ransomware	3,156	2,825	2,385	3,729	12,473,156	59,641,384	34,353,237	49,207,908	3,952	21,112	14,404	13,196
Real Estate	9,359	9,521	11,727	11,578	173,586,820	145,243,348	396,932,821	350,328,166	18,548	15,255	33,848	30,258
SIM Swap	982	1,075	2,026	N/A	25,983,946	46,798,103	72,652,571	N/A	26,460	43,533	35,860	N/A
Tech Support	36,002	37,560	32,538	23,903	1,464,755,976	924,512,658	806,551,993	347,657,432	40,685	24,614	24,788	14,545
Threats of Violence	1,360	1,697	2,224	N/A	1,842,186	13,531,178	4,972,099	N/A	1,355	7,974	2,236	N/A

SOURCE: FBI Internet Crime Report 2023

As seen in Figure 2, the severity of investment attacks is significantly higher than phishing schemes and malware attacks. The severity of a personal cyberattack can vary greatly by the type of attack and with the amount of connectivity we currently enjoy, it is likely that the number of attacks will increase and the methods that bad actors use will continue to evolve.

Future of Personal Cyber Risks and Cyber Risk Insurance

While it is difficult to determine the number of cyberattacks that have impacted individuals, a blog post by Check Point Research notes that the number of cyberattacks increased by 38% year-over-year in 2022.[14] With emerging technologies like ChatGPT, and other generative AI tools, such as Gemini, Bard, and Grok, the number of attacks is predicted to rise. Additionally, as cyberattacks on organizations increase, the number of cyberattacks experienced by individuals is also expected to increase. There are many contributing factors to the rise in cyberattacks on individuals, but it can be simplified into one common point: interconnectivity. Any time a digitally connected device—cellphones, smart home devices, self-driving vehicles—is used, the owner may be at risk. As technology advances, the world becomes increasingly connected.

Certain advances, while making life more convenient, also make it easier for attackers to access important data. One such convenience is the widespread adoption of single sign-on (SSO) websites. Some websites now allow the user to use their social media credentials to create and log into the site. *Wired*[15] addressed how the use of these SSO mechanisms allows for a single point of entry for potential attackers. Consequently, rather than needing to compromise several passwords, an attacker only needs access to an individual's social media account, which then allows access to all the information stored behind the SSO login credentials.

14 "Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks"; Check Point; Jan. 5, 2023.
15 "Think Twice Before Using Facebook, Google, or Apple to Sign In Everywhere"; *Wired*; Sept. 21, 2020.

Conclusions

Currently, the amount of data pertaining to cyberattacks targeting individuals is limited. However, as the popularity of personal cyber insurance coverage grows, the availability of relevant data is expected to increase. The current range of products offered as additions to an individual homeowner's or renter's policy may be rated by applying an increased-limits factor to a base rate. As the volume of available data grows and the products mature, insurers may be able to develop more nuanced rating plans where risks can be priced with greater accuracy.

AMERICAN ACADEMY OF ACTUARIES
1850 M STREET NW, SUITE 300, WASHINGTON, D.C. 20036
202-223-8196 | **ACTUARY.ORG**

© 2025 American Academy of Actuaries. All rights reserved.