life annuity specialist

Customers Consider Dumping Carriers Over Data Concerns

Data privacy is becoming a determining factor for consumer trust of insurers.

By Aaron Smith | December 4, 2023

Cybersecurity is a top concern for insurance customers, who worry about the fate of the personal information in the hands of carriers. It's also a concern for the carriers themselves, as the **U.S. Securities and Exchange Commission** gets ready to implement new rules on the disclosure of breaches.

"Regulators are pushing carriers, and carriers can't ignore it anymore," **Mitch Wein,** executive principal of **Datos Insights**, said in an interview, referring to state regulations like the California Consumer Privacy Act, and impending federal rules from the SEC regarding data breaches.

Wein said that insurers should be concerned about "reputational damage" if they experience a data breach, as well as the premiums they pay for cybersecurity insurance. But new research points to another risk to carriers: policyholders dropping policies if they don't trust how their insurer stewards their personal information.

A survey from the **Kennedys** law firm said that 78% of consumers are concerned about insurers selling their personal data to a third party without them knowing. This is no small matter, since many of these customers would consider dumping their carrier. The survey found that 91% of customers would "take some action" if they found out that their insurance company was tracking or using their personal data without their knowledge, including 41% who would end their contract with the insurer, and 33% who would complain to a regulator.

"Cyber and data privacy are always dynamic risks, and the risk landscape and the regulatory environment are evolving fast," **Sridhar Manyem**, senior director of industry research and analytics at **A.M. Best**, said in an email. "It is important for insurers to be on top of these risks. Knowing the data they collect, their clients collect and how they use this data, is a genuine concern."

Hacking Away at Trust

Cybersecurity, and the way that insurers handle it, is under a spotlight following a cyberattack revealed earlier this month against **Infosys McCamish**, which serves at least 34 U.S. insurers. In a separate incident earlier this year, dozens of insurers reported data breaches through another third-party vendor, **Pension Benefit Information** or PBI, and its use of MOVEit file-transfer software from **Progress Software**. The Kennedys law firm conducted its survey during May and June, when the MOVEit data breach was just starting to make waves in the insurance industry.

The survey asked 4,681 customers in nine countries (including the U.S.) about their concerns regarding insurers and their methods of data collection and automation. The results revealed that 70% were concerned about insurers protecting and storing their personal data, while 76% were concerned about their data being used to increase premiums.

The Kennedys survey also showed that 77% of respondents were concerned over privacy and the ethical use of their data, and 76% were concerned about the possibility of more data being collected than they were aware of.

"Insurers should look to ease any concerns by having complete transparency on data usage and storage with their customers," said **Manu Singh**, vice president of risk engineering at **Cowbell**, a cyber insurance company. He said they should also provide details on how they vet each third party that would have access to sensitive customer data.

Singh said this helps customers understand the level of risk they are facing and how well their privacy is being protected. He said that monitoring third parties may prove to be difficult on a continued basis, but audits are highly effective in determining the level of security to prevent exposure. "Insurers should always look to audit third parties, before they share data directly," he said.

Related Content

November 20, 2023
Three Dozen Carriers at Risk in Infosys Data Breach

November 20, 2023
Insurers Face Daunting Task of Vetting Third-Party Vendors' AI Use

October 27, 2023
Clouds Gather Over MOVEit Hack that Walloped the Industry

New Federal Rules

Carriers might not have a choice, because some of them will be subject to new regulations. **Gerry Glombicki**, senior director at **Fitch Ratings**, said the SEC will implement new rules on Dec. 15 requiring publicly traded companies to report data breaches in 8-K filings with the SEC. The SEC rules require those companies to file the reports within four business days of determining that a "material event" had occurred.

Glombicki said the SEC adopted the rule earlier this year when they noticed that some companies were announcing data breaches via press releases instead of 8-K forms. He said that after the SEC passed it earlier this year, some companies adopted it early. He added that the practice of reporting data breaches within the set time is "trickling down" to some non-public companies, even though they're not required.

"You'll see companies over-reporting it because they don't want to get sued," he said in an interview. "One of the ways to minimize getting sued is to protect the data in the first place."

He said that companies should encrypt their data and protect it with multiple layers of security.

State Regulation

The **National Association of Insurance Commissioners** released a model bulletin earlier this year on the use of algorithms, predictive models and artificial intelligence systems by insurers. The NAIC bulletin would be used as a model for insurance regulations in different states, in part to address the vulnerability of data to

hackers.

When the NAIC opened the bulletin to public comment, **Jim Hodges**, executive director of the **National Alliance of Life Companies**, complained that it would be difficult for small insurers to comply with requirements to audit third-party vendors.

Ranjan Pal, research scientist at the **MIT Sloan School of Management**, agreed that a small insurance company contracting with a large third-party vendor would not have the resources to conduct the rigorous audits proposed by the NAIC, even if they're necessary.

"It is just not economically feasible," said Pal, in an email. "On the other hand, it is hard to gauge from outside without strong audits whether a large third party has strong-enough security practices. But then in this case, I believe the responsibility should be transferred to the bigger third party."

Life Annuity Specialist is a copyrighted publication. Life Annuity Specialist has agreed to make available its content for the sole use of the employees of the subscriber company. Accordingly, it is a violation of the copyright law for anyone to duplicate the content of Life Annuity Specialist for the use of any person, other than the employees of the subscriber company.

FT SPECIALIST A service from the Financial Times