Insurance Startups: Are You Really Security Ready?

OneShield SOFTWARE | Business Solutions. Simplified.

Chad Galgay, Chief Security Information Officer

A sound security strategy is critical from the start of launching any business. And the lifeblood of any technology roadmap for the future.

Most insurance startups born in today's digital world are well acquainted with the basics of cybersecurity, including multifactor authentication and firewall protection. But young companies are often at a disadvantage when it comes to long-term security planning.

For one thing, most startups don't have a role – let alone an entire department – dedicated to information security. Instead, a Chief Technology Officer may shoulder these responsibilities along with system design and architecture.

And, most startups are preoccupied with getting to market quickly. When your business is just getting off the ground, it's challenging to focus time, attention, and resources on long-term planning. But looking ahead is essential to ensure your platform can meet your business needs, customers' expectations, and regulators' demands over time.

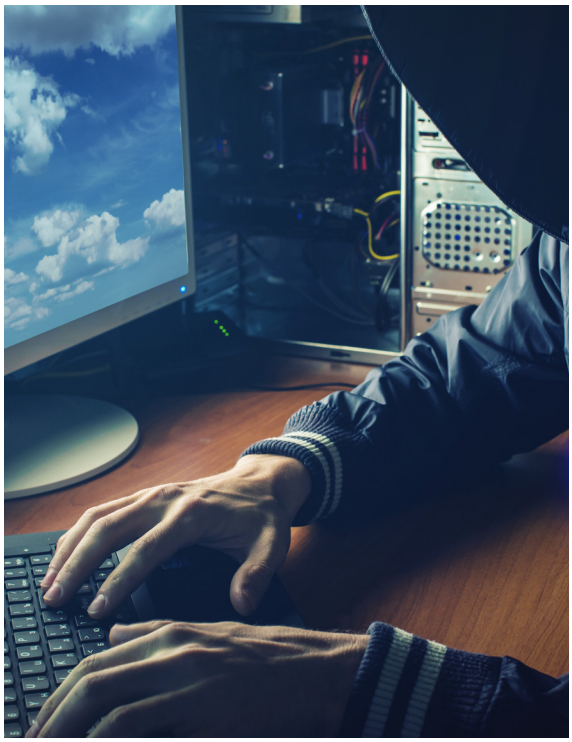
Here are just a few things for insurance startups to consider if they haven't yet planned for long-term cybersecurity exposures:

1. Know the privacy laws in states where you eventually want to do business.

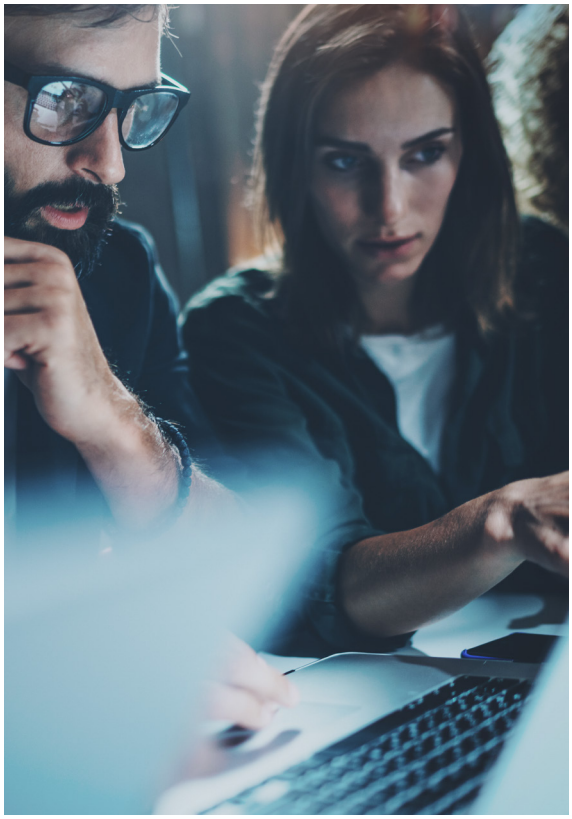
In 2020, at least 38 states were considering more than 280 bills or resolutions that deal with cybersecurity, according to the National Conference of State Legislatures. The details of these proposals vary widely, but many states are looking to establish minimum limits of cyber insurance to be carried by any agency doing business with the state.

Some specifically address insurers, requiring any licensed insurer operating in that state to regularly assess their cybersecurity exposures, evaluate and update security measures annually, and develop written information security programs.

To remain in compliance, startups should identify where they want to expand their business as it grows and get familiar with the rules in those states. Otherwise, they could find themselves playing catch-up and missing out on business opportunities.



2. Develop a strong controls effectiveness review process for potential partners.



Asking the right questions of potential partners is critical. If a vendor has any access to your system or data, verify the security measures they have in place. Ask how often they test and re-evaluate those measures and how much they invest in security upgrades. How do they store, protect, and eventually destroy data? And of course, how much cyber insurance do they carry?

Internally, establish your procedures for assessing vendor security and the requirements they need to meet. Most importantly, apply those standards consistently.

As laws continue to evolve, they will likely include more of these technical requirements that both insurers and their partners will need to adhere to – another reason to invest time in staying up to date on legislative changes.

Tracking all of these pieces can be a tall challenge for a CTO wearing many hats. This brings us to the third and final point.

3. Know what you don't know – and seek out expertise.

Partner with reputable firms with a broad knowledge of cybersecurity best practices who can fill in the gaps, especially during the implementation of your platform. An implementation partner with demonstrated cybersecurity expertise effectively acts as an extension of the startup's.

OneShield, for example, has gone beyond industry standards in testing the security of our APIs' business logic. In addition to both static and dynamic application security testing – common methods to root our vulnerabilities in software code – we also employ an automatic scanning procedure using artificial intelligence to generate hundreds of attack scenarios to expose cybersecurity threats in the API.

Regulators, business partners, and customers will all expect insurance platforms to be secure and dedicated to the protection of private data. Failure to be truly security ready could result not just in penalties and lawsuits, but the loss of trust that can take years to regain. Planning for increased cybersecurity exposures now will pay dividends as your business grows.

About OneShield

OneShield provides solutions for insurers of all sizes. Deployed in the cloud, our portfolio of standalone, subscription, and As-a-Service products includes enterprise-class policy management, billing, claims, rating, product configuration, business intelligence, and smart analytics. OneShield automates and simplifies the complexities of core systems with targeted solutions, seamless upgrades, collaborative implementations, and lower total cost of ownership. With corporate headquarters in Marlborough, MA, and offices in India and Canada, OneShield has 50+ products in production across P&C and specialty insurance markets. For more information, visit www.oneshield.com.

OneShield SOFTWARE | Business Solutions. Simplified.