Frequently asked questions for AWS clients seeking cyber insurance coverage from Cowbell

Q: What does it take to qualify for coverage?
Applicants need to have their headquarters and the majority of their business operations in the U.S. with revenue up to $250 Million.

Q: What aspect of AWS is covered?
Assets including software and data deployed on the AWS cloud for the AWS account(s) specified in the policy can be covered.

Q: What's not covered?
Components of the cloud that are under AWS responsibility for operations, maintenance and security as defined in the applicable AWS user agreement(s) are not covered.

Q: Does the applicant have to activate the Cowbell Connector for AWS?
While not mandatory, this is highly recommended for AWS clients. This will provide additional insights into the risk profile of your company, potentially open additional coverage options, and make you eligible for a 5% premium credit if you are coverage by a Prime 250 policy.

Q: How do you calculate premium due?
Cowbell uses more than 1000 outside-in and inside-out data points to evaluate an organization for cyber risk. Activating the Cowbell Connector for AWS enables us to provide a refined assessment, potentially giving you access to additional coverage options, and in the case of Prime 250 making you eligible for a 5% premium credit.

Q: What can I do to reduce my premium?
Great cybersecurity hygiene is the first step to optimize your premium - multi factor authentication (MFA), patching, having a backup in place, cyber awareness training for employees, and an incident response plan will improve your risk profile and therefore help reduce your premium or provide additional policy options, for example, a lower deductible.

Q: What is AWS Security Hub?
AWS Security Hub is a service that helps organizations manage their AWS cloud security posture from one comprehensive view. It performs security best practice checks, aggregates alerts and enables automated remediation.

Q: Do you need to activate AWS Security Hub?
We highly recommend that all AWS clients activate AWS Security Hub and the Cowbell Connector for AWS to get a better handle on their cybersecurity posture on AWS and better cyber risk insights from Cowbell.

Q: What happens if you experience a cyber incident?
You or your broker must notify Cowbell as soon as you are made aware of a potential cyber incident. Cowbell's incident response team will immediately engage your team to scope the incident and allocate the best available resources with the cyber expertise to get your business back to normal operations as quickly as possible. Depending on the type of incident, this might include a breach counsel, forensic services, ransomware negotiation experts and more.

Q: How do I file a claim?
As soon as you discover a potential cyber incident, you can file a claim with Cowbell by calling the 24×7 hotline at (833) 633–8666 or by an email to claims@cowbellcyber.ai

The Cowbell in-house claims team is available 24×7 to help your organization recover.

Q: Can you cancel your policy at any time?
Yes.