SCORviews

March 2016

By Clarke Rodgers
CISO – Director, Cybersecurity
SCOR Velogica
crodgers@scor.com

Data Protection and the Cloud

Meeting Growing Security Needs

Executive Summary

The risk of data breaches, either accidental or through malicious hacking, is an unfortunate consequence of electronic commerce. To ensure the highest standard of data protection, SCOR Velogica has invested in a state-of-the-art data security environment.

Clarke Rodgers discusses SCOR's decision to move Velogica® to the cloud, and explains how SCOR, and other insurers, can take advantage of the expertise that cloud vendors provide while ensuring that cybersecurity remains paramount – allowing each partner to focus on their core strengths.

At SCOR Velogica, we are constantly pushing the boundaries of innovation in automated underwriting – working with data providers, fine tuning our algorithm and developing insights to ensure that our platform remains at the forefront of the industry.

Investments in technology, processes and people help us deliver a best-of-breed offering to our clients. However, in today's hyper-connected world, none of this matters if we can't deliver security that meets (and exceeds) our client's data protection requirements. We handle some of the most sensitive data available on our clients' insureds – and we treat and protect it as if we collected it ourselves.

Protecting Sensitive Data

Implementing a strict data protection protocol while allowing business users to do their jobs is an expensive endeavor with many moving parts and detailed technical configurations. Any misstep in this multilayered approach to security could potentially expose sensitive data to malicious actors. Finding and hiring skilled security analysts, purchasing expensive hardware/software solutions and implementing strict security policies make information protection a complex part of doing business.

While the above outlines what most organizations *should* be doing to protect sensitive data, it is not what all organizations *are* doing, primarily because of the complexity and maintenance of required configurations. In the "on premise" world of a company's own data center, staffing is charged with not only protecting assets from compromise, but also matters such as ensuring the data center has enough capacity, redundant power feeds, appropriate cooling, etc. None of these efforts are core to a company's business; instead, they add overhead that prevents 100% focus on the delivery of business solutions – like automated underwriting.

Sharing Responsibility

To achieve gold standard data protection while keeping resources and energy focused on automated underwriting, SCOR moved Velogica to the cloud in 2015, and we have

Editor
Matthew Hughes
704.344.4210
mhughes@scor.com

www.scor.com/SGLA

SCOR Global Life

Data Protection and the Cloud

Meeting Growing Security Needs (cont.)

not looked back. In addition to high availability and operational agility, we have significantly increased our security posture while reducing operational overhead. How is this possible? Cloud benefits from its sheer scale, propensity towards automation, explicit logging and commitment to security. The major cloud vendors know that if there is ever a data breach on their platforms (where they are at fault, not due to a customer misconfiguration), there will be a significant impact to their business. They invest heavily in security, the auditability of their platforms and compliance offerings – more so than most organizations can afford to do.

The customer-cloud relationship is one of shared responsibility for security. As one moves up the cloud stack, the responsibility for security transitions from 100% provider to 100% customer, which allows organizations to focus on protecting what they know very well (e.g., the Velogica offering and underlying data) and allows the cloud provider to do what they do best: protecting the underlying infrastructure and providing tools and services for the customer to use (if they choose) to further protect their data.

We found the following tools/services especially valuable features of the cloud that others in the insurance industry could find helpful:

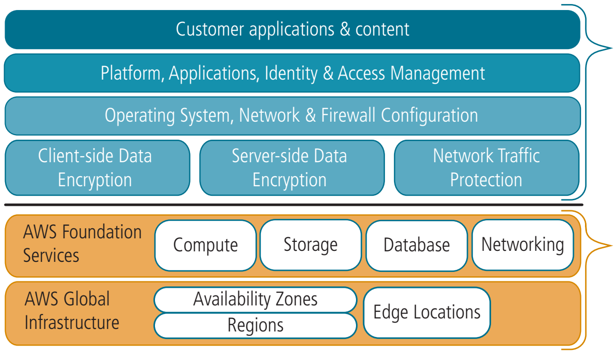
Ubiquitous Encryption. Data is fully encrypted over the network, at the disk level and within the database, and the cloud customer controls the encryption keys. While encryption can be done in an on-premises environment, it often takes a team to maintain and tune the hardware and software required (PKI isn't easy) to do this. In the cloud, it is all handled via a single console or API call.

Logging & Auditing. All calls related to infrastructure (e.g., create a server, add a user, grant/deny permissions, add storage, start a database) and applications (file transfers, services starting/stopping) are logged. While this in itself is nothing special, the cloud platform allows analysis and alerting of these activities in real time, with the ability to set thresholds and alert mechanisms not only to monitor infrastructure performance, but also to add visibility to the age old question of "Who did what, when?"

Segregation/Localization of Data. To be compliant with data protection laws, it is important to know where regulated data resides, and ensure that it does not move unless the transfer is initiated by the authorized entity. Cloud providers are very sensitive to data localization issues and put controls in place so that data stays in the local region (with no automated transfers to other regions) until purposefully moved.

Authentication and Authorization. Defining who has access to what resources, as with other aspects of cloud administration, is a matter of clicks and/or API calls. Choosing to enforce multifactor authentication, ssh key-based logins and getting detailed, real-time access reports typically do not cost anything more than the per-use charges.

Moving to the cloud is not an easy endeavor. However, when planned correctly and using trusted partners, validated migration techniques and best-of-breed architectures, most organizations should find that they can be more secure in the cloud than in their own data centers. The business, information technology


Customer applications & content
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption
Server-side Data Encryption
Network Traffic Protection
AWS Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Availability Zones
Regions
Edge Locations

Security/Compliance **IN** the Cloud
The insurer knows the required security/compliance needs, the cloud provider does not. The carrier can leverage tools from the cloud provider, purchase/bring its own third-party tools or create its own to achieve specific security & compliance needs.

Security/Compliance **OF** the Cloud
Unless the insurer has expertise in datacenter management, it can leave this to experts who are not concerned with running an insurance business. The company can leverage their third-party assurance reports to address any risks and require regular audits and reviews.

and security benefits are clear to support such a move, freeing company resources to concentrate on improving the core competencies of the carrier's business initiatives.

If you would like more information on Velogica and its data protection environment, please contact either Dave Dorans (ddorans@scor.com) or myself. ∞

Velogica® Achieves SOC2 – Recognizes Security, Confidentiality, Availability

Earlier this year, SCOR announced the receipt of its SOC2 Type 1 report regarding the effectiveness of its controls over the Velogica life underwriting system. The report, based on the AICPA's Trust Services Principles and Criteria for Security, Confidentiality and Availability, is an independent third-party examination that demonstrates how SCOR achieves key compliance controls and objectives as they relate to the Velogica system.

"We have increased our focus on our security and compliance protocols over the past few years," said Dave Dorans, Senior Vice President of SCOR Velogica. "This report gives confidence to current and prospective Velogica clients that the Velogica platform incorporates stringent security, confidentiality and availability practices to protect client data from compromise."

Velogica has processed nearly 2.5 million life insurance applications and continues to build on 10-plus years of experience. "We have been at the forefront of innovation in automated life underwriting for more than a decade," said J.C. Brueckner, CEO of SCOR Global Life in the Americas. "SOC2 demonstrates that we are equally committed to being at the forefront of security and confidentiality issues that automated life underwriting solutions demand."