The Shared Responsibility Model: Balancing Liability in a Matrix of Service Providers

Jordan L. Fischer, Partner, XPAN Law Group, LLC, Philadelphia, PA

As companies increasingly rely on an infrastructure supported by a spider web of third-party providers, ownership of the security and privacy risk is becoming blurred. Matrix-like infrastructures that rely on multiple third-party service providers present significant legal and practical challenges in navigating the risk environment. This roundtable will focus on the evolution of the “shared responsibility model” and its interplay with liabilities and contractual obligations.
Cyberspace Law Institute and Winter Working Meeting ("CLI/WWM")
January 25-26, 2019 in St. Petersburg, Florida

The Shared Responsibility Model:
Balancing Liability in a Matrix of Service Providers

OUTLINE

Key topics to be addressed:
- As companies increasingly rely on an infrastructure supported by a spider web of numerous providers, the owner of the security and privacy risk is becoming blurred.
- Determining the "risk owner" is key to understanding who is liable for a failure in protecting against that risk. And, a comprehensive risk mitigation program is completely reliant on understanding responsibilities and when and where those responsibilities can and are being transferred.
- As technologies continue to develop and build matrix-like infrastructures that rely on multiple third-party service providers, the evolution of the "shared responsibility model" and how it interplays with liabilities and contractual obligations is becoming increasingly complex.

I. What is the Shared Responsibility Model
   A. Background
      1. In general, the shared responsibility model ("SRM") divides the security responsibility between the provider and the customer.
      2. Growing trend among technology service providers
   B. Example of Platforms
      1. Amazon Web Services
      2. Google
      3. Microsoft Azure
   C. Example of Breaches
      1. Uber 2016 Security Breach
         a) Some commentators believe the 2016 Uber breach could have been prevented if the SRM was implemented.
         b) In the Uber data breach, hackers used an authorized username and password to access Github which is a popular repository that holds username and password information. The hackers used this information to access Uber’s driver and rider data which was stored on AWS.
         c) Since the hackers used an authenticated (but stolen) username and password, the failure was at the access control level--Uber.
d) Some commentators say that SRM would have clearly delineated the security roles of both Uber and Amazon, which would show that access control was the responsibility of Uber.

2. Dow Jones Breach of 2017
   a) New York-based Dow Jones & Company is a global provider of news and business information, delivering content to consumers and organizations via newspapers, Web sites, mobile apps, video, newsletters, magazines, proprietary databases, conferences, and radio.
   b) A cloud-based file repository owned by financial publishing firm Dow Jones & Company, that had been configured to allow semi-public access exposed the sensitive personal and financial details of millions of the company’s customers.
      (1) The exposed data includes the names, addresses, account information, email addresses, and last four digits of credit card numbers of millions of subscribers to Dow Jones publications like The Wall Street Journal and Barron’s.
      (2) Also exposed in the cloud leak were the details of 1.6 million entries in a suite of databases known as Dow Jones Risk and Compliance, a set of subscription-only corporate intelligence programs used largely by financial institutions for compliance with anti-money laundering regulations.
   c) The exposed data repository, an Amazon Web Services S3 bucket, had been configured via permission settings to allow any AWS “Authenticated Users” to download the data via the repository’s URL.
      (1) Per Amazon’s own definition, an “authenticated user” is “any user that has an Amazon AWS account,” a base that already numbers over a million users; registration for such an account is free.

II. Legal Implications
   A. Responsibilities of Stakeholders
      1. Platform providers protect the infrastructure of their web services and provide customers with the capabilities to configure security capabilities.
      2. Customers are responsible for, among other things, protecting customer data, custom applications, access policies, configuring firewalls, data loss prevention policies, and scanning for vulnerabilities.
      3. The service provider is responsible for securing computing, storage, networking, and database services. They are also responsible for, among other things, custom applications, network security, physical control of hardware and software, and patching.
   B. Regulatory Impact
      1. European Union’s General Data Protection Regulation (GDPR)
a)  
2. New York Department of Financial Services Cyber Regulations (NY DFS)  
3. California Consumer Privacy Act of 2018 (CCPA)  

C. Legal Theories of Liability  
1. Duty of Care  
2. Negligence  
3. Breach of Contract  
4. New theory of liability  

III. Advising Your Client  
A. Contractual Agreements  
B. Risk Mitigation  
C. Cyber Insurance