Getting a Handle on Handheld Risks

by Robert M. Horkovich, Cort T. Malone and Jorge Aviles

We are all aware by now of major cyberattacks on government and corporate databases. Hiding in plain sight, meanwhile, are risks associated with the use of personal mobile devices and their apps, including those connected to social media.

The rapid deployment and uptake of mobile apps and social media has created new, evolving risks for businesses that interact with customers through these platforms. Policyholders need to be aware of such risks and scrutinize the insurance coverage options available to them.

AN EXPLOSION OF APPS AND SOCIAL MEDIA

A growing number of transactions, both personal and commercial, are executed on smartphones and other portable devices. Analysts estimate that in 2016, mobile phone users downloaded some 90 billion apps and spent 900 billion hours using them. More than two million apps are available for download on the iPhone alone. According to eMarketer, people increasingly spend more time on their smartphones and tablets using downloaded apps rather than browsing the web. In-app usage was forecast to account for 89.2% of smartphone time and 76.8% of tablet time in 2017.

The average person now spends nearly two hours on social media every day, according to GlobalWebIndex, while a study by Mediakix recently calculated that Facebook users spend an average of 35 minutes a day on that platform and that 60% of the time spent on social media is via mobile device.

It only is a matter of time before all companies either are deploying their own mobile apps or relying on third-party apps to service customers or enable transactions. Most companies already have some social media presence or are figuring out how to best use the technology to their benefit. Social media ad spend alone is expected to reach $36 billion in 2017.

MOBILE RISKS

But as with any new technology, there are risks involved in the use of mobile apps and social media platforms. More than 1.5 million new incidents of mobile malware were detected by McAfee Labs in the first quarter of 2017 alone. While big mobile players such as Apple and Android continue to improve their platforms, it is impossible to keep up with the plethora of malicious actors that constantly introduce new forms of malware. A RiskIQ study found that every 60 seconds 818 pieces of unique malware are deployed, along with 1,214 ransomware attacks and more than 100,000 phishing emails.

At a recent presentation by the FBI, a special agent involved with the U.S. Secret Service's Electronic Crimes Task Force noted that malware in mobile devices may become mainstream in the next five years. When performing transactions using mobile apps, users often input highly sensitive data, including personal financial and confidential health details. Yet security still is not a top priority in app design, with some apps allowing users to store or pass credentials in the clear or by using weak encryption.

A CHANGING LEGAL LANDSCAPE

Mobile app and social media use by companies has triggered new waves of regulatory actions, as well as civil litigation. The Food and Drug Administration has provided insight on its views and specific examples of how its authority may apply to mobile medical apps, while the Federal Trade Commission and other regulators already have brought app-related enforcement actions based upon alleged violations of privacy.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

April 2018

Mobile app users have brought their own suits too. Tech giant Google has faced litigation from its Google Wallet users alleging violations of the Stored Communications Act and consumer protection laws. Companies also now face growing legal repercussions, such as lawsuits for defamation and copyright infringement, related to their social media presence.

"Any cyber event that significantly impacts a company's reputation and its share price could result in shareholder action," said Emy Donavan, global head of cyber for Allianz.

INSURANCE COVERAGE IMPLICATIONS

Faced with a changing regulatory landscape and the increased potential for liability, policyholders need to review the insurance coverage options available under both traditional commercial liability and developing cyber insurance policies that may cover the risks associated with mobile apps and social media.

Policyholders may be able to look to traditional commercial general liability insurance policies, which often provide coverage for personal and advertising injury and might afford coverage for claims such as defamation, libel and copyright infringement stemming from a company's social media presence.

Policyholders also can look to their directors' and officers' coverage and errors and omissions coverage. Shareholders now expect that good corporate governance and oversight must include safeguarding a company's cybersystems and data. Policyholders therefore should maintain responsive D&O insurance coverage for potential cyber claims that might affect the most senior levels of their companies. D&O policies may respond to a variety of cyber-related allegations because such claims can qualify as a "wrongful act" under D&O policies. Another potential source of coverage is E&O policies, which provide coverage for claims associated with a company's errors or omissions in rendering its professional services.

While standard commercial liability policies, D&O and E&O policies are potential sources of coverage, these policies now often have cyber exclusions. Further, insurance companies have become increasingly aware of the risks related to mobile apps and social media, and now are inserting exclusions meant to limit coverage for liabilities connected to such activities. This trend has made it important for policyholders to consider buying separate cyber insurance policies.

The landscape for cyber-specific policies still is emerging, with little consistency between the cybersecurity programs offered by the major insurance companies, including various exclusions specific to mobile devices. For example, some cyber policies include an exclusion barring coverage when a breach occurs through an unencrypted mobile device. Other cyber policies exclude coverage where the policyholder fails to follow "minimum required security practices," employ "best security practices," or comply with its own security policy. Insurance companies already have relied on such exclusions in cyber policies to disclaim coverage, and no doubt will continue to do so. Litigation has ensued where these types of exclusions were at issue, and surely will continue in the future as companies face unexpected liabilities related to mobile apps and social media.

Policyholders must be mindful of these evolving exclusions in order to maximize coverage and to avoid the gaps in coverage that such exclusions create.

A PATH FORWARD

While policyholders might be able to look to traditional policies as potential sources of coverage, insurance companies may continue to narrow that coverage. Policyholders must remain ever-vigilant and consider insurance options specifically tailored to liabilities arising from their use of mobile apps and social media platforms. In particular, policyholders and their advisers need to vet current and future policies to ensure they do not contain exclusions that might exclude coverage for the very risks they seek to insure. ■

Robert M. Horkovich is managing partner and shareholder in the New York office of Anderson Kill. He is a trial lawyer who has obtained more than $5 billion in settlements and judgments for policyholders from insurance companies. **Cort T. Malone** s a shareholder in the New York and Stamford offices of Anderson Kill and practices in the insurance recovery and the corporate and commercial litigation departments. **Jorge Aviles** is an attorney in the Anderson Kill's New York office. His practice concentrates in corporate and commercial litigation and insurance recovery, exclusively on behalf of policyholders.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com