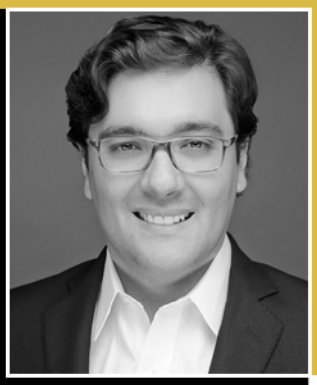
CYBER SECURITY & RISK MANAGEMENT

ANNUAL REVIEW **2019**

FINANCIER WORLDWIDE corporatefinanceintelligence



Mexico

DAVID GONZALEZ
Capital Bay Underwriting
Chief Underwriting Officer
+1 (786) 338 9805
david.gonzalez@capitalbayuw.com

Throughout his 15 year career in the insurance/reinsurance industry David Gonzalez has held a variety of positions with large multinational firms like AIG, Bupa and RSG. He spent 12 years at AIG in a multitude of underwriting and management roles in Ecuador, Colombia, Puerto Rico and the US. He has managed P&Ls in excess of $80m in yearly revenues with clients in over 15 countries. His latest project is Capital Bay Underwriting for which he is the chief underwriting officer.

Q. In your opinion, what are the major cyber threats to which today's companies are vulnerable? Could you comment on any recent, high profile cyber attacks in Mexico?

GONZALEZ: The number of successful cyber attacks has increased exponentially in recent years, especially in the financial services space. Hackers are becoming more sophisticated and are targeting larger sums of money. Mexico seems to have been specifically targeted in recent years by hackers from Asia and Eastern Europe. Furthermore, well-coordinated and sophisticated 'Trojan' attacks are more common than ever. These programmes monitor a user's activity and they have been known to be embedded inside the target institution's systems for up to a year. Recently, the Mexican central bank's payment compensation system SPEI was targeted. Several banks were involved and over US$15m was taken. Impersonation fraud is also becoming increasingly widespread. The *modus operandi* in these cases involves gathering intelligence on an organisation's senior management, via a number of different sources, including social media accounts. The perpetrators then impersonate the individual and use emails and telephone calls to conduct fraudulent money transfers to accounts they control.

Q. Given the risks, do you believe companies are placing enough importance on cyber security? Are board members taking a proactive, hands-on approach to improving policies and processes?

GONZALEZ: We do not believe companies are paying enough attention to cyber security, especially in the financial services space. Hackers are aware of this and are targeting institutions throughout Latin America (LATAM). Having said that, awareness has increased of late and most large company boards are beginning to look into cyber risks more actively than in previous years. However, response plans that test a company's vulnerabilities are not as common as they should be. Many organisations seem to be taking a 'wait and see' approach, unless they have already been the target of a significant attack. Cyber risk should be at the top of every financial institution's operational risk mapping. Investment in vulnerability testing and ethical hacking by third-party firms is one way of developing a best in class cyber fraud prevention framework. The insurance and reinsurance community also needs to play a more active role in pushing for the improvement of controls and investment in the space.

Q. To what extent have cyber security and data privacy regulations changed in Mexico? How is this affecting the way companies manage and maintain compliance?

GONZALEZ: Latin America is more exposed to major systemic cyber events than other regions of the world. This is due to underinvestment in cyber fraud prevention and unawareness. Regulators are likely taking note of this and moving faster than they have been in recent years. There is still a long way to go in LATAM in terms of liability to third parties for data and confidentiality risk. A new legal framework addressing this is required in most countries. For now, LATAM cyber risk is mostly a first-party loss exposure.

Q. In your experience, what steps should companies take to avoid potential cyber breaches – either from external sources such as hackers or internal sources such as rogue employees?

GONZALEZ: Companies should contract third-party consultants to identify and test their vulnerabilities and help them develop a cyber

breach response plan. Most firms do not have the internal expertise to do this alone. The plan should involve different components, such as crisis response, staff training, ethical hacking, transfer of funds procedures and a hardware and software component. Most firms believe they have state of the art controls and procedures, but the reality is that cyber crime is rapidly evolving. Some of the largest institutions in the world that invest billions of dollars into cyber fraud prevention have been the victims of serious hacking events. Everyone needs a second pair of eyes on their cyber prevention procedures and controls.

Q. How should firms respond immediately after falling victim to cyber crime, to demonstrate that they have done the right thing in the event of a cyber breach or data loss?

GONZALEZ: In the event of a breach, companies should call their insurer, if they have one. They would have contracted a crisis response firm that will walk them through the process. Financial institutions should notify the regulator. All firms should have a crisis plan with a specific action plan on how to handle a breach. The plan should have a public relations, client notification, regulatory notice and forensic IT component; however, the first priority initially should always be to minimise the potential withdrawal of funds. This task usually falls to the internal IT or cyber security team.

Q. In what ways can risk transfer and insurance help companies and their D&Os to deal with cyber risk, potential losses and related liabilities?

GONZALEZ: Computer crime policies cover most first-party losses in the cyber fraud space. Recent wording expansions have been brought into the market to actively transfer the impersonation fraud risk to the insurance industry. Historically, hacking activity has been covered under standard market policies; however, until recently the underwriting community has not been concerned or paid a lot of attention to computer crime exposures because losses were rare. This has changed dramatically over the last five years, and losses have increased exponentially. Pricing and underwriting practices need to adjust, and underwriters must play an active role in pricing risk more accurately and pressing companies to adopt stricter controls in order to make insuring this risk sustainable in the long term.

"Companies will be forced, either by losses, regulators, underwriters or their boards, to invest more in cyber fraud prevention."

Q. What are your predictions for cyber crime and data security in Mexico over the coming years?

GONZALEZ: The space will continue to evolve rapidly, most likely with a higher number of large fraud events occurring. Companies will be forced, either by losses, regulators, underwriters or their boards, to invest more in cyber fraud prevention. The most valuable assets in the coming decades will be digital. As we transition from a physical world to a digital world, data will move to the fore, becoming many companies' most valuable assets. Protecting those digital assets will be a top priority for most companies. However, due to budgetary constraints, a lack of awareness or neglect, in some cases, companies will only act if they are forced to do so. Regulators will also start demanding stricter standards as the number of large cyber fraud events increases. It will take a combination of all of the stakeholders to manage this risk moving forward. ■

DAVID GONZALEZ
Chief Underwriting Officer
+1 (786) 338 9805
david.gonzalez@capitalbayuw.com