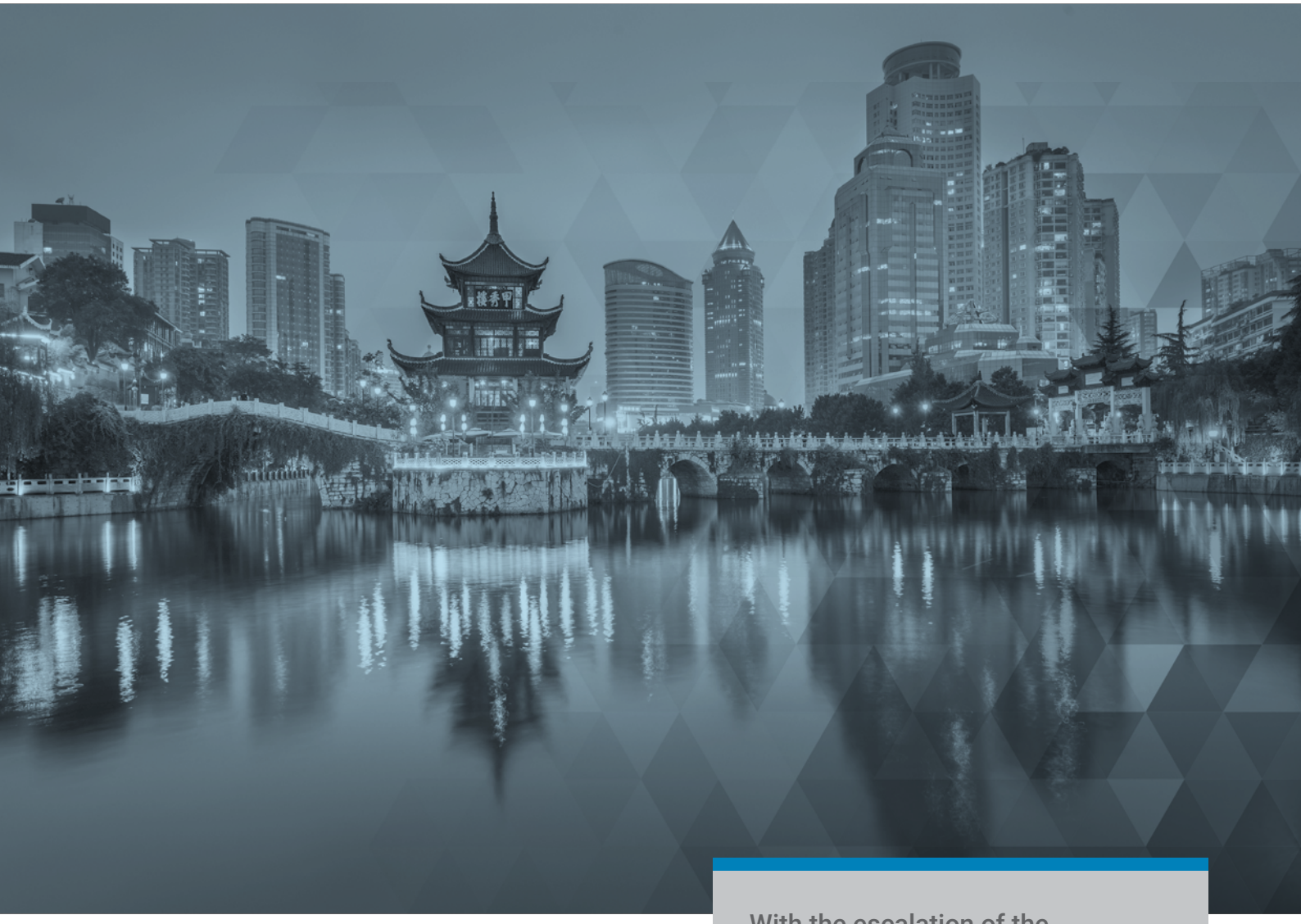
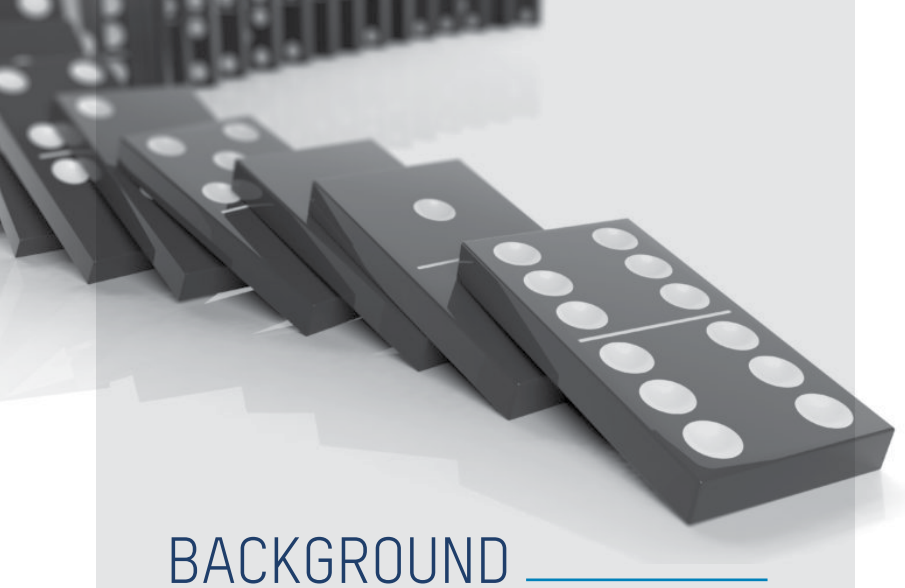
BITSIGHT
The Standard in SECURITY RATINGS

WHITE PAPER

MANAGING RISK IN AN INCREASINGLY REGULATED WORLD



With the escalation of the cybersecurity and compliance landscape in Asia Pacific and global unprecedented fines, what does this mean for FS firms in the region?



BACKGROUND

In 2019 there have been record fines of organisations such as Facebook, Marriott, and British Airways under new legislation, such as GDPR, which stand as a wake-up call to all businesses that regulatory authorities have teeth when it comes to cybersecurity. This means that no business can afford to not adhere to regulations as the fines, the financial and reputational impact and other knock-on effects are not only significant, but catastrophic for some organisations. Ultimately, executives and Boards around the globe are responsible and accountable for cybersecurity performance management in just the same way that they are accountable for managing other critical parts of the business.

This white paper looks at how emerging regulations will impact FS firms across the Asia Pacific region. In particular, it examines the common themes in many of the regulatory approaches -- including themes around executive and Board responsibility, measuring security effectiveness, and managing risk in the ecosystem. It explains why it has never been more important for security and risk leaders in FS firms to know their industry's security performance standards and how FS firms face legal liability for failing to meet customer requirements and industry wide standards of care for cybersecurity. It also explains why the Monetary Authority of Singapore Technology Risk Management (MAS TRM) guidelines and the Hong Kong Monetary Authority, who are also enforcing Third Party Vendor Risk Management guidelines, have brought about significant positive influence to the region in setting up their regulatory guidelines/frameworks. This has created a safer cyber environment for financial services in both Singapore and Hong Kong. Additionally, in the wake of major events in the region, such as the LandMark White third party data breach, which impacted a number of Australian Banks, it will also examine how this has put the spotlight on cyber hygiene.

THE ASIA PACIFIC REGULATORY LANDSCAPE

Asia Pacific continues to be a dynamic growth region, marked by world-leading innovation in financial services, continued strong GDP growth, and rapidly increasing financial inclusion. That said, cybersecurity has continued to be front-of-mind for FS firms. As the number of attack surfaces increases, and the sophistication of threat actors improves, so the cost to the economy increases, with estimates now reaching approximately USD $160 billion coming from the Asia Pacific region alone.

For example in January 2019, Australia's largest independent property valuation and property consultancy firm, LandMark White, suffered a major data breach, when approximately 137,500 sensitive customer records were compromised via one of its valuation platforms. This also hit a number of the Australian banks for whom LandMark White acts as a third party to conduct property valuations. Customers from Westpac, Commonwealth Bank of Australia, ANZ, St.George, Bank of Melbourne, BankSA, and RAMS were all potentially compromised.

This means many regional regulators expect firms to fully embrace managing culture and governance around cybersecurity and privacy. Financial crime and cyber risk are areas where a holistic approach to risk governance will be critical, while Asia Pacific regulators are shifting towards a dynamic supervisory model - especially in relation to third party risk management (TPRM). Regulators see the need to adopt robust privacy and cyber risk management as a key priority in 2019. In particular, honing in on executive and Board level responsibility is high on regulators' agendas.

UNDERSTANDING WHAT THE REGULATORS ARE LOOKING FOR

Breaking down this massive and escalating volume of regulation, into more simple and digestible terms, what the regulators are essentially asking FS firms to do is establish senior level accountability and responsibility to ensure that organisations are treating the issues around security strategically and that the firm has effective and appropriate levels of risk management in place to monitor not only its own performance, but the performance of its outsourcers or third parties.

SHINING A SPOTLIGHT ON SENIOR LEVEL ACCOUNTABILITY

Taking that first theme, strong governance has been a focus area in light of recent global issues, but a spotlight is being shone in the region through the Australian Royal Commission's investigation into banking misconduct, which has drawn significant attention. Likewise, the LandMark White third party data breach, which caught out a number of banks. These and other incidents have prompted regulators to take a close look not only at bad practices but also hone in on risk management, and the roles of senior executives and Boards. Individual accountability is already a reality in some countries and is likely to figure prominently as a topic across the region in 2019. Financial crime and cyber risk are areas where the need for a holistic approach to risk governance is being underscored.

HOW THE LANDMARK WHITE THIRD PARTY DATA BREACH AFFECTED AUSTRALIAN BANKS

As a result of a major data breach in January 2019, LandMark White, Australia's largest independent property valuation and property consultancy firm, is predicting a net loss of $2.3 million for the year, having been forced to take a three-month trade suspension from the Australian Securities Exchange (ASX).

HOW THE LANDMARK WHITE THIRD PARTY DATA BREACH AFFECTED AUSTRALIAN BANKS

Approximately 137,500 sensitive customer records were publicly exposed through a programming interface on one of its valuation platforms. Compromised information included property valuation and personal contact information of borrowers, lenders, homeowners, residents, and agents who had sought assistance from LandMark White between January 4, 2011 and January 23, 2019. Addresses, emails, and phone numbers were also affected. While the firm said that there had been no evidence of misuse, some of the dataset in question was later found for sale on the dark web.

LandMark White operates as a third party to facilitate property valuations – an outsourcing arrangement which may have exposed the personal details of customers at Westpac, St.George, Bank of Melbourne, BankSA and RAMS. At the time banking firm Westpac Group said names, addresses, and contact details may have been exposed through the third party breach and could impact Westpac property service customers. Westpac Group warned customers that those who had conducted a property valuation through its business may have been inadvertently impacted by the data breach affecting LandMark White.

Commonwealth Bank of Australia, WestPac and ANZ all suspended LandMark White from their panel of valuers.

Today regulators are questioning traditional methods of risk management and executive oversight and they are starting to shift away from point-in-time supervision towards a dynamic model that gives Boards and executives a more holistic picture of a firm and its third parties' activities.

FS Firms are now being held accountable for the performance of their cybersecurity programmes. As such, security and risk leaders need a way to continuously monitor, measure and communicate the efficacy of the controls they have in place to secure their valuable assets from threats in the digital ecosystem. In order to achieve this they need to take a risk-based, outcome-driven approach to manage performance through broad measurement, continuous monitoring, and detailed planning and forecasting in an effort to measurably reduce cyber risk.

To this point the **Australian Prudential Regulation Authority (APRA)** is strengthening both its resourcing and supervisory approach to make issues of governance, culture, and accountability a much more prominent and central part of its supervisory framework, with a particular focus on managing risk.

In **Singapore, the Monetary Authority of Singapore Technology Risk Management (MAS TRM)** guidelines, which have been in force since June 2013, outline the importance of the IT function in supporting a financial institution's business, and how the board of directors and senior management should have oversight of technology risks and ensure that the organisation's IT infrastructure is capable of supporting its business strategies and objectives. In particular it outlines how senior management are responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

In New Zealand the **Financial Markets Authority (FMA)** and the **Reserve Bank of New Zealand (RBNZ)** jointly initiated a Financial Services Conduct and Culture Review at New Zealand's 11 largest retail banks. The review emphasised that "a high bar will be set in meeting our expectations and demonstrating a sufficient level of assurance in regard to good conduct, oversight and culture." And, as they have identified weaknesses in the governance and management of conduct risks, they have made a number of recommendations to improve executive level oversight, controls and processes.

In the wake of several serious misconduct issues in Japan, the **Japanese Financial Services Agency (JFSA)** has made governance, oversight and accountability a central part of their regulatory strategy, expressing the need for Japanese financial institutions to get their house in order. In October 2018 they published a final paper that explained their new dynamic approach to compliance risk management and how they will oversee the Japanese Financial Services sector's approach to executive risk-based decision-making.

Both the **Hong Kong Monetary Authority (HKMA)** and the **Securities and Futures Commission (SFC)** in Hong Kong are placing increasing attention on senior management being responsible for conduct failures. No longer just "tone from the top", regulators are placing importance on the "tone from the middle" to ensure consistent messages are driven from both senior and middle management. In addition, firms are expected to consider how conduct risk affects their business and identify steps to mitigate those risks. Regulators are keen to see how a firm's security performance management strategy affects its business strategy and how existing controls and monitoring process are being adjusted accordingly to address it. Likewise the **Hong Kong Monetary Authority (HKMA)** is also enforcing **Third Party Vendor Risk Management (TPVRM)** guidelines particularly focused on FS Firms.

In essence, Asia Pacific regulators are sending a clear message to FS firms in the region: cyber hygiene is critical, Board and executive level oversight is a pre-requisite. They are espousing a new approach that includes dynamic supervision and executive accountability.

OUTSOURCING, THIRD PARTY RISK MANAGEMENT AND NEW PRIVACY LAWS

Today, the expansion of the extended enterprise has reached a tipping point, fuelled by cloud-based technology and outsourcing. In parallel, third-party data breaches are at an all-time high. There is a growing awareness in the region that third-party cyber risk must be managed. This means Asia Pacific FS firms need to manage the safety and soundness of their vendors and partners through third party risk management programmes and engage with them on forward-looking remedial measures and continuously monitor these.

While cloud providers will have their own security and resilience procedures, the regulators have made clear that firms are nevertheless expected to take responsibility for the security of data put in the cloud and any outsourced processes (including third parties) that may be seen as critical for the functioning of key services the firm provides to its customers. For example, the **Monetary Authority of Singapore (MAS)** is consulting on new proposals to expand its regulatory oversight of bank outsourcing arrangements. In particular under Section 3.0.2 it mandates: "the Board of directors and senior management have oversight of technology risks." Under the new regime, MAS intends to impose requirements for banks to conduct due diligence checks on technology partners, including customer data protection terms in outsourcing agreements, and put in place recovery plans in the event of service disruption. MAS will also be empowered to conduct its own inspections of third party providers and their sub-contractors and will have the right to terminate contracts that may endanger operational stability.

Likewise, as we increasingly live our lives online privacy is becoming a prominent issue, especially with the enforcement of GDPR in the EU, with the Asia Pacific region following suit. And as society becomes more connected, cyber risk is possibly one of the biggest issues the industry and regulators in this region are facing.

To this point the Asia Pacific region has seen a horde of new privacy laws and bills and they all focus on compliance and having a clear picture of personal data collection, processing activities, transmission, location and retention requirements within and across operating jurisdictions.

They also highlight the need for executive and Board level responsibility and accountability to ensure that FS firms have measures in place to safeguard the personal data elements from increasing risk of misuse and unauthorised access.

Within these laws they also recognise supply chain risk and the importance of having effective third-party risk management processes and robust and up to date contracts to support privacy obligations passed to third parties, this includes continuous and ongoing monitoring of those relationships.

HOW SECURITY RATINGS ARE AN INTEGRAL COMPONENT OF REGULATORY ALIGNMENT

If FS firms don't respond and prioritise these areas, the resulting impact could include fines and regulatory action. The FS firm could suffer oversight and loss of data, negative reputational impact resulting in further financial harm, legal liability, huge operational disruption and potentially other harmful issues.

NEW PRIVACY LAWS IN THE REGION

The **Australian Privacy Act** was recently amended to include mandatory data breach notification provisions that require certain entities to notify individuals and the regulator of 'eligible' breaches.

The Singapore government announced the **Data Protection Trustmark Scheme (DPTM)** in July 2018, following the theft of the personal data of 1.5 million SingHealth patients. The DPTM allows for official certification of a company's data protection methods and is unique in the Asia Pacific region.

The **Personal Information Protection Commission** was set up in 2016 under the **Japanese Privacy Law** whose primary duty is to protect the rights and interests of the individual. A subsequent amendment of the law in 2017 introduced the definition of "Special care required personal information" and FS firms are required to obtain express consent from the individual while collecting personal data elements that fall into this category.

The Information Technology Personal Information Security Specification was effective in China in May 2018. It provides a set of data protection rules for companies that obtain and use personal information. The specification also expands the definition of personal information to include a person's online activities.

New Zealand introduced a bill to amend its privacy legislation in March 2018 and this is currently being considered by Parliament. **The Privacy Bill** repeals and replaces the 25-year-old Privacy Act of 1993. Key changes proposed by the bill are the introduction of a mandatory data breach notification scheme, increased powers for the privacy commissioner, and increased fines.

This means that FS firms need to build a "trust but verify" strategy in order to effectively manage both first party and third party risk. Requesting documentation about a supplier's security performance is good – but how can you verify it? How can you continuously monitor performance? The organisation could be following every best practice in the cyber security book— but if its third parties are not following through with security obligations, then the supply chain is at risk. Therefore, FS firms need to continuously assess and monitor the security posture and performance of their own organisation as well as all partners, in order to gain visibility in the changing threat landscape, and to prioritise risk-mitigating actions.

Faced with these issues, how can FS firms better understand, monitor and manage first and third party risk?

Here at BitSight we recommend that security ratings become an integral component of regulatory alignment. Issuing daily ratings that are akin to a credit score for security, BitSight helps FS firms flag not only their own risks but also those of the companies they do business with, such as vendors, partners, suppliers and acquisition targets. In short, BitSight Security Ratings immediately exposes the existence of cyber risk within the organisation itself and the company's supply chain. This helps focus resources, and ratings can work alongside FS firms and their third parties to achieve significant and measurable cyber risk reduction.

Using security ratings FS firms gain insight into the riskiest issues impacting their own organisation as well as their third party outsourcers, backed by data that correlates to potential security incidents and context. BitSight provides visibility into the security environment to prove whether security controls are in existence and are effective (or not). Likewise, BitSight can provide alerting to changes in security and this insight facilitates third party communication for faster remediation.

WHY REGULAR REPORTING AND PERFORMANCE METRICS ARE NO LONGER "NICE TO HAVE" WHEN IT COMES TO CYBERSECURITY

Regardless of what definitive changes lawmakers and regulators might make, FS firms should continue to drive effectiveness and efficiencies across their risk and compliance programmes so they can meet applicable laws, regulations, and supervisory expectations. When it comes to cybersecurity, ongoing briefings, regular reporting, ongoing monitoring and performance metrics are no longer a "nice to have", they are required.

Armed with the real-time data and information they need, FS firms can gain a holistic picture of their security posture and risk management programme within their own company and their third and fourth parties. Security ratings give security and risk leaders continuous visibility into cybersecurity issues and allow them to proactively prioritise their remediation strategies to ensure alignment with current and future regulations as Asia Pacific requirements continue to evolve.

BITSIGHT®
The Standard in SECURITY RATINGS