FALL 2017

Insurance
EXECUTIVE BRIEF

GLOBAL INSURANCE SERVICES

IN THIS ISSUE

CLIENT GUIDANCE
KEY EXPERT PROFILES
IN THE NEWS / QUICK TAKEAWAYS

EXPERTS WITH **IMPACT**

FTI CONSULTING

In this issue

What Insurance Companies Need to Know About Part 500 Cybersecurity Compliance

BY JIM WRYNN and ANTHONY J. FERRANTE

If there were any remaining doubts about the vulnerability of our online systems, they were dispelled in September when giant credit-reporting company Equifax revealed it was breached in July by cybercriminals, compromising the personal identifiable information (PII) of roughly 143 million Americans – approximately half the country.

With PII – Social Security and bank account numbers; passport and health-related information; driver license and student information – criminals can apply for loans and credit cards, withdraw money from bank accounts, and fraudulently obtain a variety of goods and services. And these criminals know insurance companies store large volumes of PII on their policyholders, making the insurance sector a prime target for cyber crooks.

For example, Anthem Blue Cross Blue Shield and Premera Blue Cross suffered data breaches in 2015 that exposed the PII of approximately 78 million policyholders and cost those companies hundreds of millions in remediation costs. In June 2017, Anthem agreed to pay $115 million to settle lawsuits arising from the breach. However, the total cost Anthem incurred was over triple that amount and included $230 million for costs associated with incident response and $128 million on post-incident cybersecurity enhancements.

The threats to insurers, and all organizations, are growing due to the increasing reliance of business activity on global Internet connectivity, as well as the commercialization and professionalization of cybercrime. This potent combination is driving the increased frequency and severity of cyber incidents. Accordingly, in late 2014, the National Association of Insurance Commissioners (NAIC) Executive (EX) Committee established the Cybersecurity Working Group to create a regulatory framework for cybersecurity. At about the same time, New York's Department of Financial Services (NYDFS) began the process of drawing up its own cybersecurity regulations for the financial services industry, and took effect in March 2017. These regulations are Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, and all financial services organizations licensed, registered, chartered, or otherwise authorized in New York must comply. And it has become clear that the NAIC will incorporate many provisions of the New York regulations into its own framework.

Part 500, designed "to promote the protection of customer information as well as the information technology systems of regulated entities,"[i] requires all companies covered by the regulation to conduct a rigorous assessment of their information systems and risk profiles, and to design and maintain cybersecurity programs commensurate with their risks. Although some companies (including but not limited to those with fewer than 10 employees, less than $5 million in gross annual revenue and less than $10 million in year-end total assets) are exempt from some of Part 500's provisions, all companies are required to have robust cybersecurity programs and policies in place protecting technology systems and "non-public information"[ii] (which includes PII) that, if disclosed, could cause material harm to any individual, business or either entity's operations. And all companies, no matter their size, are required to ensure the security of information held by or accessible to the third-party service providers they engage.

More specifically, and in addition to the above, Part 500 proposes that institutions:

- Appoint a Chief Information Security Officer (CISO) who, among other duties, will be responsible for achieving compliance with Part 500;
- Deploy key technologies, including encryption and multifactor authentication (or risk-based authentication), among others;
- Conduct regular security assessments, including penetration testing, and vulnerability and risk assessments;
- Ensure that senior management (or the board chair) files an annual certification confirming compliance (much like reporting on internal controls under Sarbanes-Oxley);
- Provide regular cybersecurity awareness training for all personnel;
- Create a written incident-response plan;
- Maintain a system that includes audit trails for reconstructing financial transactions and confirming obligations, and retain these records for not fewer than five years; and
- Report to a governing authority (such as the NYDFS) on any cybersecurity event "that has a reasonable likelihood of materially harming any material part" of the organization's normal operations.[iii]

THE COMPLIANCE CHALLENGE

Compliance with Part 500 will require resources – personnel and money – that may need to be diverted from core business activities, plus expertise that not all organizations possess.

Client Guidance
Continued

Overall there is a lack of cybersecurity talent, experience, and expertise in the market. For example, in 2015 over 200,000 cybersecurity positions went unfilled in the United States, according to a Stanford University analysis of data from the U.S. Bureau of Labor Statistics. Some reports expect the global security labor shortfall to reach 1.5 million by 2020. This shortage means that companies – not just insurance firms – have to pay top dollar to recruit and retain this workforce.

CISOs with the requisite experience and knowledge of the data security world are scarce and, not surprisingly, expensive to retain. Under Part 500, firms are required to maintain a CISO, and as demand for their services increases, so have their salaries, with total CISO compensation at large firms reportedly approaching or topping $1 million.

Beyond the talent crunch, the continuous monitoring required by Part 500 is not specifically defined and therefore will require skilled experts to implement technically. However, this implementation is not just a technical issue – it must be folded into a holistic cybersecurity risk management decision that also considers the requirements of business. This demands talent, experience, judgment, and appropriate policies and procedures.

Finally, the type of reporting mandated by Part 500, and the responsibility it places on the board and senior management, necessitates a focus that makes cybersecurity and cybersecurity awareness a more organic part of the company's culture. And that kind of organizational change is always hard, especially in today's difficult market environment in which insurers are under intense pressure to lower costs while modernizing their information technology (IT) systems to create new products and services to boost top-line revenue. It will require a level of training, awareness, and involvement across the entire company.

The underlying financial investment that will be required for achieving compliance will certainly not be small. While larger firms should be able to manage the costs, the costs could be overwhelming to small-to-midsize insurance firms. However, no matter the difficulties, if financial services organizations and insurers wish to do business in New York, they must work to overcome these challenges.

TOWARD A HOLISTIC SECURITY PROGRAM

A compliant, effective cybersecurity program should be an integral part of an organization's enterprise risk-management strategy. Minimizing cyber risk means an organization should:

- Identify critical data assets and protect them appropriately;
- Conduct a thorough organizational review to find and remediate gaps between written policies and procedures and business operations and transactions;
- Examine the processes that will produce reporting in case of an incident;
- Create an actionable, written data-breach response plan that includes both internal and external communication strategies;
- Implement processes for continually updating security systems, including patch management. (The May 2017 WannaCry/WannaCrypt ransomware attack used a vulnerability that took advantage of unpatched and outdated systems. Britain's National Health Service was one such victim, and this ransomware attack brought many of their systems' operations to a halt, potentially placing lives at risk.)
- Conduct cyber awareness training throughout the enterprise at least once a year.

These and other actions should be conceived as part of a holistic security program, founded upon a comprehensive understanding of cybersecurity risk, with written policies and procedures broadly communicated to all parts of the operation. These policies and procedures should always be accessible and available to regulators to demonstrate the organization's adherence to its own written policies. There must also be a confirmatory audit trail designed to allow companies and regulators to reconstruct material financial transactions, as well as a record of cybersecurity events and the company's processes of detection and response. Boards of directors should prioritize making risk determinations and ensuring compliance with the various requirements of Part 500.

As insurance companies modernize their IT systems, cybersecurity must be baked into their plans, not treated as an afterthought. That means properly trained security experts must be a part of any modernization effort, sitting side-by-side with developers, planners, and line-of-business leaders.

If in-house expertise is lacking, firms may consider outsourcing various elements of cybersecurity preparedness and monitoring to experienced and well-vetted third parties. However, organizations must understand that, although Part 500 permits the outsourcing of penetration testing, vulnerability assessment, and other cybersecurity risk-mitigation activities, even including engaging a third party to fill the CISO role, the covered entity ultimately remains responsible for security and for compliance with Part 500. Therefore, while outsourcing arrangements can be enormously beneficial in helping firms fill gaps in personnel, experience, and expertise, they should be entered after a rigorous due-diligence process and with a

Client Guidance
Continued

well-considered plan for governing and monitoring this critical relationship with full transparency and a robust reporting process.

THE COMPLIANCE OPPORTUNITY

Compliance does not in and of itself equal security, and if complying with Part 500 is approached as a check-the-box exercise, it won't enhance security. A company that can see the compliance process as an opportunity to not only become a more secure organization, but also a more efficient one, is primed to reap the full benefits of becoming both more secure and more operationally efficient.

For example, some organizations have invested in deploying security applications for two-factor authentication on mobile work phones. This allows their people to access the information they need to conduct business on a more secure connection, even in an insecure environment such as an airport. In this case, security is enhanced while also increasing workforce efficiency and the organization's profitability.

The process of thoroughly examining existing procedures and policies and developing more secure ones can enable a firm to learn about and incorporate up-to-date best practices and operational controls, not only in security but also in organizational governance. This is the opportunity that compliance affords, and all firms may benefit from it in many ways if they embrace the cultural transformations it entails.

New York State Department of Financial Services, 23 NYCRR 500, "Cybersecurity Requirements for Financial Services Companies," Introduction.

Ibid. Non-public information is defined in Section 555.01, Part g, 1 – 3.

Ibid., Section 500.17, Part a., 1 – 2.

ANTHONY J. FERRANTE

Senior Managing Director,
Leader of the Cybersecurity practice

+1 202 312 9165
AJF@fticonsulting.com

JIM WRYNN

Senior Managing Director
Global Insurance Services

+1 212 841 9366
Jim.Wrynn@fticonsulting.com

*This article first appeared in *Insurance Journal* on October 10, 2017

Key Expert Profiles

PAUL BRAITHWAITE, FCAS, MAAA

Senior Managing Director, Co-Leader of Global Insurance Services and Head of Actuarial Services

+1 212 499 3659

Paul.Braithwaite@fticonsulting.com

As a past president of the Casualty Actuarial Society with more than 30 years of industry experience, Paul Braithwaite brings deep knowledge and understanding of actuarial science, underwriting, and insurance and reinsurance company management to the practice. He has more than a decade of executive and operational experience within the reinsurance industry, playing such critical roles as chief actuary as well as senior vice president and chief underwriting officer across several global specialty business lines.

Paul serves as appointed actuary to insurance companies, provides expert testimony and dispute resolution support, loss reserve reviews, reinsurance commutations, underwriting audits, due diligence, finite risk/structured product pricing analysis, and regulatory services. He also has extensive reinsurance pricing and underwriting experience, including the specialty areas of professional liability, workers compensation, umbrella liability, accident and health, agriculture, surety and various other lines of property-casualty business. He consults with companies on capital standards for life, health and property-casualty business and recently advised a major multi-line insurance group about issues related to a potential strategic acquisition.

Prior to joining FTI Consulting, Paul was the leader of the insurance services team of a major consulting company, where he also served as the global actuarial practice leader. He has also held high level executive roles in the industry. He has both testified as an expert and served as an arbitrator in insurance and reinsurance disputes, and he provides expert advice to insurance companies, captives, self-insureds, brokers, and investment firms.

Paul is well-respected in the insurance and reinsurance industry, holding prominent positions with the Casualty Actuarial Society and other actuarial organizations. He is an oft-requested speaker at industry events and conferences on topics including actuarial professional standards of practice, Solvency II, capital requirements and capital modeling, reinsurance risk-transfer and reinsurance pricing. Paul has also published several articles on these topics.

JOHNNY ENRIGHT

Managing Director, Global Insurance Services and head of the Data Analytics Center, Dublin

+353 1 765 0800

Johnny.Enright@fticonsulting.com

Johnny Enright heads the Data Analytics Center in Dublin, an "Analytics Center of Excellence" where GIS develops and delivers innovative solutions that leverage the Center's data quality improvement; embedded data analytics; predictive modeling; process and performance improvement; and customer value management capabilities. Johnny is an experienced Program Manager with 15 years of experience and expertise delivering large-scale, multi-year change programs that leverage data assets and advanced analytics to drive growth and achieve cost savings for large clients in the insurance and other industry sectors. Johnny holds a Degree in Commerce and a Higher Diploma in Computer Science from University College Cork. He also holds a Diploma in Management from the University of Limerick and has completed the Project Management Professional (PMP) Certification Program.

IAIN WHITTINGHAM

Managing Director, Global Insurance Services, London

+44 20 3727 1577

Iain.Whittingham@fticonsulting.com

Iain Whittingham has a deep understanding of the Lloyd's and global commercial insurance market and is focused on business performance improvement and transformation. He has over 20 years of experience across all dimensions of change; strategy development; target operating model design and delivery; business performance improvement using analytics and big data; outsourcing/BPO; shared service center set up; proposition development; regulatory change; and growth strategies. Iain also has expertise in the development and implementation of Target Operating Models and process re-engineering programs within the insurance sector. He has delivered over 50 enterprise-wide insurance projects and programs that have contributed in excess of GPB 200 million of benefits to customers. Prior to joining FTI Consulting Iain was an executive at a global insurance carrier. He is also a veteran of the British Army, serving from 1989 to 1997. Iain holds a B.A., (Honours), University of York.

In The News / Quick Takeaways

Jim Toole, Managing Director, GIS Actuarial group, and Pratyush Lal, Managing Director, GIS Performance Analytics group, were speakers at the Society of Actuaries Annual Meeting October 16 – 18. Jim discussed pandemic preparation as follow up to an article he co-authored with Cristina Stefan from Metabiota on the same topic. Pratyush disscused successful applications of analytics in the P&C industry, with an emphasis on actual case studies.

Jim Toole traveled to Colombia in October on behalf of the Society of Actuaries (SoA) Latin America Committee where he gave a talk about the SoA to the Colombian Actuarial Association. Members of the Committee visited with universities, regulators and quasi – governmental agencies, and hosted a joint reception for actuaries attending the conference and local students taking SoA exams. The goals of the committee include enhancing actuarial skills, increasing the profession's visibility, and heightening the reputation and influence of actuaries in Latin America. Mr. Toole has served on the committee since 2014 and as chair since 2016.

Quick Takeaways

Insurance Industry Challenges and Opportunities

FTI Consulting continuously assesses marketplace developments that are important to our existing and potential clients. The topics summarized below underscore the need for insurers to view their insurance operations and product portfolio in terms of being more interconnected with the changing digital landscape, perhaps taking a broader perspective and a more critical strategic view of the challenges and opportunities.

CATASTROPHIC EVENTS: MANAGING THE AFTERMATH

Recent catastrophic events across the globe not only underscore the need for improved warning and preparation, but also the need for better capabilities to manage the aftermath. This includes the full range of requirements related to addressing the impact to life and property. To learn more about these important challenges, please visit http://info.fticonsulting.com/FTIConsulting_Crisis_Recovery

GENERAL DATA PROTECTION REGULATION: ADDRESSING A COMPLEX GLOBAL CHALLENGE

General Data Protection Regulation (GDPR), the European Union law to be effective May 25, 2018, impacts any company anywhere in the world if it holds data on EU citizens. GDPR requirements extend beyond the internal organization to the company's supply chain, making compliance more difficult and more critical considering the severe fines for non-compliance. Key changes to the original GDPR adopted in 1995 as outlined by GDPR.org (http://www.eugdpr.org/the-regulation.html) include Increased Territorial Scope, Penalties, Consent, Breach Notification, Right of Access, Right to be Forgotten, Data Portability, Privacy by Design, and Data Protection Officer.

Required: Organizations must maintain a plan to detect a data breach, regularly evaluate the effectiveness of security practices, and document evidence of compliance. Essentially, organizations must embed data security requirements throughout the organization at every stage of each business process. Accordingly, there are five primary capabilities that must exist for achieving compliance – process insight, data governance, data management, data quality and data security. Organizations may have problems achieving all five at the optimal levels needed to ensure compliance. Therefore, an assessment of capabilities should be conducted to inform the board and executive management of what is required to upgrade these capabilities. Also to be considered is the possibility that all or part of the GDPR will be adopted into other regulatory regimes, making its impact more widespread. Contact: Jim.Wrynn@fticonsulting.com, Michael.Ennis@fticonsulting.com

PROCESS AUTOMATION: RAPIDLY GAINING MOMENTUM

Process automation is rapidly gaining momentum, fueled by artificial intelligence and other enriched digital technologies, and driven by the urgent need to more aggressively achieve cost reductions while improving performance across the insurance value chain.

Required: Advanced process automation is not simply dropping an AI Bot into a work stream. To take advantage of advanced process automation, companies need to achieve a degree of organizational and system transformation that ensures integration with other core services and the enterprise target operating model. This includes objectively assessing requirements, developing plans, and adopting the right technology and personnel capabilities to ensure and manage quality data and to apply advanced analytics. For example, by taking this approach to customer value management, a multinational insurance client of FTI Consulting was able to improve its quote-to-win ratio by 40 percent and increase its annual gross written premiums by 10 percent. Contact: Iain.Wittingham@fticonsulting.com, Paul.Prior@fticonsulting.com

CUSTOMER CENTRIC INNOVATION: EMERGING AS CORE COMPETENCY

Customer management is emerging as a core competency within the insurance value chain, which now extends beyond traditional boundaries and into the digital ecosystem. This includes the virtual marketplace model, in which companies

offer products and services to their customers through third party teaming arrangements, many of which are with insurtech startups. The virtual marketplace is a near-real-time "pull" environment enabled by smart phone apps and other technology, where customers seek desirable products and services, as opposed to products and services being "pushed" to them. The virtual marketplace model helps minimize costs and enhance the customer experience. The external peer review was requested before the platform was made available to clients.

Required: Carriers must achieve a data-rich single view of the customer in order to understand customer needs/desires. Knowledge of the customer enables matchups with third party offerings. In addition, to be functional and attractive to third parties, carriers need to develop open APIs that enable customer enriching Apps (think the smartphone App ecosystem). These initiatives require multidisciplinary teams that combine technical and business skills with innovative thinking and action, supported by senior executives that have clearly articulated strategic and business objectives.
Contact: Johnny.Enright@fticonsulting.com

ACTUARIES: EMPOWERED IN EXPANDED ROLES

Are you applying predictive analytics to increase M&A and customer value, or do you want to examine problems from a difference perspective? Actuaries have long been at the forefront of applying statistics and analytics to large data sets in order to understand past performance and anticipate future trends related to insurance products. Today, the role of actuaries is expanding, as actuaries become more involved in the converging disciplines of risk management, regulatory compliance, and financial analysis. Renowned for their statistical, and analytics and reasoning skills, actuaries are playing an increasingly important role in multidisciplinary teams, developing innovative new products, examining process issues and operational and financial metrics.

Required: To gain increased value from actuaries, boards and senior executives (including the chief actuary) should take the lead in communicating various ways that actuaries can add innovative thinking and approaches to various problems. Start with educating key management, followed by encouraging projects that demonstrate and reinforce the value-added contribution of actuaries, some of which may be related to new coverage opportunities such as those identified below.
Contact: Paul.Braithwaite@fticonsulting.com

EMERGING BUSINESSES: NEW COVERAGE OPPORTUNITIES ABOUND

Digital technology has advanced an abundance of needs that enter uncharted coverage territory; all with challenges that include increased underwriting capability, identifying risks and exposures, liability issues, and government and regulatory requirements. Examples include drones, self-driving cars, 3D printing, gene modification, embedded artificial intelligence, and myriad Internet of Things (IoT) devices and data.

Required: In addition to meeting traditional requirements such as capital adequacy, risk appetite and regulatory compliance, insurers must be capable of embracing a broad, long term perspective and strategy, with access to sufficient data to properly interpret and price coverage. Also worth considering is the ability to achieve operational innovation and agility that helps transcend legacy performance constraints, especially since these marketplace opportunities will most likely be dynamic, requiring coverage and pricing adjustments to meet changing needs. This may include the use of artificial intelligence and aggregation models that help ensure there is no inadvertent coverage/price discrimination.
Contact: Wendy.Shapss@fticonsulting.com

RETIREMENT RISK: MITIGATION THROUGH COORDINATION

Plan sponsors, corporate or public, need the services of many different vendors in order to manage the day-to-day operations of their retirement plans. In addition to managing multiple vendors for day-to-day operations, sponsors must also focus on achieving broader goals related to the plans. These broader goals involve human capital strategy, income statement and balance sheet items, asset risk, liability risk, funded status risk, compliance risk and fiduciary risk among others. Many sponsors are finding it difficult to create the organizational synergy necessary to effectively achieve both operational efficiency and strategic objectives related to plans, thus increasing risk and expenses.

Required: Sponsors need to first ensure that their business and plan goals and objectives are clearly articulated and communicated. Once that is accomplished sponsors should assess their organization from a holistic perspective, taking into account how disparate operational resources can best function collaboratively to support business goals and objectives. With this information, sponsors can build specific action plans for coordinating and managing execution of targeted projects to deliver results. Execution will require leadership by a person with multidisciplinary expertise and experience that combines technical and business skills. Using this approach, one of our clients for example, that had historically managed several pension plans, was able to minimize the number of plans, lower costs, and reduce risk.
Contact: Jeffrey.Leonard@fticonsulting.com

Insurance
EXECUTIVE BRIEF

Actuarial Services

- *Appointed Actuary & Statements of Actuarial Opinion*
- *Expert Testimony*
- *Independent Compliance, Performance and Actuarial Audits*
- *Modeling, Pricing, Reserve Estimation & Predictive Analytics*
- *Pension Plan Restructuring*
- *Pension Valuation*
- *Pricing & Ratemaking*
- *Reinsurance*
- *Retirement Plan Sponsor Risk Assessment*
- *Captive and Alternative Market Advisory Services*
- *Risk Transfer*
- *Strategic Financial Assessment and Risk Analysis*
- *Implementation & Support - Actuarial & Modeling Tools*

Corporate Advisory Services

Mergers & Acquisitions

- *Target Identification & Diligence*
- *Post Merger Integration*
- *Product/Market Analysis/ Planning*
- *Restructuring & Integration*
- *Strategic Communication*
- *Liquidation & Receivership Strategy and Management*
- *Exit Strategy Management*

Strategic & Financial Risk Management

- *Alternative Risk Financing Structures*
- *Business Resilience*
- *Capital Modeling*
- *Enterprise Risk Management*
- *Risk Governance*
- *Cybersecurity*
  - *Governance*
  - *Readiness Assessment*
  - *Data Breach*
  - *Response Services*

Litigation & Dispute Resolution

- *Claims Litigation & Dispute Resolution*
- *Contract Dispute Resolution*
- *E-Discovery Readiness, Management & Compliance*
- *Expert Testimony*
- *Intellectual Property*
- *Trial Services*
- *Forensic Investigations*
- *Early Dispute Resolution*
- *Damage Analysis*
- *Assisting Witness Preparation*
- *Assessment of Opposing Expert Testimony*
- *Effective Presentations to Judges, Juries and Arbitrators*

Forensic Accounting & Investigations

- *Accounting Malpractice*
- *Asset Tracking and Recovery*
- *Audit Committee Investigations*
- *Compliance and Internal Investigations*
- *Embezzlement & Misappropriation*
- *Fraudulent Claims*
- *Independent Monitorships*
- *Internal Investigations*
- *Ponzi Schemes*
- *Political and Corruption Risk Assessments*
- *U.S. Foreign Corrupt Practices Act*
- *UK Bribery Act*
- *Whistleblower Allegations*

Governance, Regulation & Compliance

- *Compliance Programs*
- *Governance Frameworks*
- *Internal Audit and Internal Controls Risk Assessment*
- *Regulatory Interpretation & Remediation*
- *Sarbanes-Oxley*
- *ORSA*
- *Board Effectiveness*
- *Financial Crime*
- *BSA/AML*
- *Sanctions Risk Assessments*
- *Regulatory Change Programs*
- *Captive Advisory*
- *Feasibility*
- *Strategy*
- *Funding / Tax Compliance*
- *Operations*
- *FATCA & FCPA*

Claims & Underwriting Analytics

- *Claims & Underwriting Leakage*
- *Reserve Analysis*
- *Business Metrics & Analytics*
- *Technical Reviews*
- *Re-engineering*
- *Expense Containment*
- *Asbestos Environmental & Mass Tort*
- *Third Party Vendor Process Improvement*
- *Business Transfers and Schemes of Arrangement*
- *Operating Model and Organization Design*
- *Claims Cost Analytics*

Performance Analytics

Performance Excellence & Delivery

- *Strategic Design & Transformation*
- *Business Architecture*
- *Business Integration & Restructuring*
- *Business Process Management*
- *Cost Management*
- *Change Management*
- *Knowledge Management*
- *People Development*

Predictive Analytics

- *Customer Segmentation & Lifetime Value*
- *Campaign Analytics & Channel Propensity*
- *Churn Analytics*
- *Cross / Up Sell Analytics*
- *Credit Risk & Fraud Analytics*
- *Claims Analytics*
- *Workflow Analytics*
- *Cost Variance & Anomaly Detection*

Customer Value Management

- *Data Driven Growth*
- *Customer Segmentation*
- *Customer Lifecycle Mapping*
- *Customer Base Management*
- *Contact Center Management*
- *Customer Experience Improvement*
- *Campaign Management*
- *Omni Channel Effectiveness*

Enterprise Data Management

- *Enterprise Data Strategy*
- *Data Management Services*
- *Business Intelligence & Management Information*
- *Merger and Acquisition Technology Services*
- *Data and Information Security*

FTI Consulting Global Insurance Services Leadership:

Paul Braithwaite
Senior Managing Director
Co-Leader of GIS
Paul.Braithwaite@fticonsulting.com
+1 212 499 3659

Wendy Shapss
Senior Managing Director
Co-Leader of GIS
Wendy.Shapss@fticonsulting.com
+1 212 841 9374

Mark Higgins
Senior Managing Director
Leader of Performance Analytics
Mark.Higgins@fticonsulting.com
+353 01 672 9025

Jim Wrynn
Senior Managing Director
Leader of Governance, Risk and Compliance
Jim.Wrynn@fticonsulting.com
+1 212 247 1010

About FTI Consulting

FTI Consulting, Inc. is an independent global business advisory firm, dedicated to helping organizations manage change and mitigate risk: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTI_FLC), Facebook and LinkedIn.

www.fticonsulting.com

FTI CONSULTING