US Financial Institutions Industry

Global Risk Management Survey: Summary Findings

December 2018

AON
Empower Results®

Table of Contents

Introduction

We have entered an era of unprecedented volatility as the world is grappling with a dramatic and rapid political, social and economic transformation. While these new forces, along with the exponential pace of technological development, are converging to create a new reality and new opportunities for financial services organizations, they also bring a host of new and non-traditional risks, which must be managed in innovative ways.

Against this backdrop, Aon's 2017 Global Risk Management Survey is designed to offer organizations the insights necessary to compete in this increasingly complex operating environment. With input from nearly 2000 respondents at public and private companies of all sizes and across a wide range of industries, the survey has been Aon's largest to date and one of the most comprehensive surveys globally.

Topics in Aon's 2017 Global Risk Management Survey include:

- Current and projected top risks
- Risk readiness and losses
- Techniques utilized to identify and assess major risks
- Organizational risk maturity
- Risk management department and function
- Risk financing
- Cyber risk coverage
- Multinational programs
- Captives
- Market insights
- Financial insights

The 2017 findings from this biannual web-based study underscore that companies are tackling new risks and that we lack consensus on how to best prioritize and respond to them.

In this FI report, we focus specifically on the top 10 risks that face financial services organizations. For the second time, damage to reputation/brand is the top-ranked risk in our survey mostly because of a succession of high-profile scandals and investigations involving money laundering, customer accounts and data breaches that hit the industry over the past year.

Meanwhile, survey participants rank regulatory and legislative changes as the number two risk because stringent oversight that came out in the aftermath of the global financial crisis continues to create tremendous burdens for financial services organizations with complex reporting and disclosure requirements.

In the survey, another risk worth mentioning is cyber crime/hacking/viruses/malicious codes, which has jumped from number five in 2016 to number three in the current survey. The new ranking reflects concerns over the rising number of organized cybercrimes against financial institutions over the past few years.

This FI report will also discuss the interconnected nature of different risks. For example, a large-scale data breach not only damages a firm's reputation and dents its credibility, it also elicits more regulatory and public scrutiny, diminishing its ability to attract and retain customers and top talent. Conversely, at a time when companies are under intense pressure to attract and retain talent and to maximize the productivity of their people, those that cannot appropriately motivate and incentivize their workforce will quickly fall behind their competition. The list goes on. This interdependence among risks illustrates that organizations can no longer evaluate risk in isolation, but must consider their interconnectedness.

I hope you find this year's results insightful and actionable. At Aon, we believe in the power of data and analytics and we strive to provide clients with innovative solutions that help manage volatility, reduce risk, and realize opportunity.

At the moment, Aon's 2019 Global Risk Management Survey is well underway. I strongly encourage you to participate in the study. Your valuable input will help shape our perspectives, enabling us to complement this data driven insight with robust business intelligence. In return, we will share the findings with our clients and other interested organizations so that they can benchmark their risk management and risk financing practices against those of their peers, and help identify practices or approaches that may improve the effectiveness of their own risk management strategies.

If you have any questions or comments about the survey, or wish to discuss the survey further, please contact your Aon account executive, or visit aon.com/industry-expertise/financial-institutions

Jacqueline Quintal
Managing Director & Practice Leader
US Financial Institutions Practice
Commercial Risk Solutions
Aon

Overview

Nearly a decade after the global financial crisis, market conditions for the financial industry have finally begun to stabilize. Among major advanced economies, the U.S. leads the pack, with real GDP reaching 18 percent above the pre-crisis level in 2018. Moderate hikes in base interest rates in North America and the tapering of asset purchases in the euro zone have led many economists to predict that the healthy economy, with a strong job market and inflation near two percent, could last for three years.

Meanwhile, 2018 marks the start of a turning point in financial regulation. The industry is finally getting a much-needed respite after nearly a decade of tightening that began in 2009. The U.S. Congress passed reform legislation in May 2018, rolling back parts of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which contains complex and sometimes inefficient requirements, including far-reaching requirements even for small and medium sized institutions.

Despite this upbeat outlook, the stakes for the sector remain high and financial institutions continue to face increasingly complex risks in a new economic context. Uncertainties over trade wars and fiscal policies loom large in advanced economies, as globalization and nationalistic forces compete. In the U.S., while new laws should benefit community banks and smaller financial institutions, Congress has failed to revoke or revise many of the key provisions in the Dodd Frank Act. At the same time, regulators have also moved to tighten supervision of many innovative financial practices, including mobile banking, peer-to-peer lending and payments, on-demand insurance, investment robo-advisers and crowd-funded ventures.

Within the industry, lingering low-interest rates, wavering public confidence and fierce competition from non-traditional competitors could potentially affect corporate profitability and, for some, survival. Moreover, new advances in technology have created easy access to consumers and increased operational efficiency, but also present the challenge of keeping up with technological innovation itself. Lastly, the prevalence and frequency of cyber breaches highlight the danger that all businesses face, particularly as they become increasingly reliant upon technology.

In today’s globally interdependent environment, risks to businesses, no longer isolated by industry or geography, are becoming more complex in nature, interconnected, and global in consequence. Even the most seasoned risk managers find it a challenge to anticipate and respond effectively to the increasingly expansive and evolving threats to their organizations. Managing and mitigating risk has become a necessity for survival, driving a company’s success in this diverse, competitive and intricate marketplace.

As part of Aon's efforts to help companies stay abreast of emerging issues and learn what their peers are doing to manage risks and capture opportunities, we have compiled this report, which is based on Aon's 2017 Global Risk Management Survey. The report contains some detailed facts and analyses gleaned from more than 180 global financial services companies.

Top 10 Risks

Aon's 2017 Global Risk Management survey has revealed a host of daunting challenges driven by today's divisive, yet interdependent environment. Respondents are provided a list of more than 50 risks and asked to select 10 that they believe to be the top risks facing their own industries and organizations. We'll focus on the Top 10 risks selected by financial institutions for detailed discussion, which is one of the perennial highlights.

1 Damage to reputation/brand
2 Regulatory/legislative changes
3 Cyber crime/hacking/viruses/malicious codes
4 Economic slowdown/slow recovery
5 Failure to innovate/meet customer needs
6 Failure to attract or retain top talent
7 Increasing competition
8 Disruptive technologies/innovation
9 Growing burden and consequences of corporate governance/compliance
10 Technology failure/system failure

Damage to reputation/brand

Before discussing this risk, it is worth examining a few major news events that dominated the headlines during the 12-month period before Aon's survey was conducted. Such comparison will make it easier to see their correlations.

For example, in the fall of 2016, a large financial institution in the U.S. grabbed the headlines when it fired several thousand employees for opening accounts for customers who didn't want or need them. Many set up fake accounts by impersonating their customers and using false email addresses. The news sent shockwaves through the industry. Subsequently, a federal review triggered by this scandal found similar incidents at other banks, where employees opened accounts without proof of customer consent. Meanwhile, the televised hearings of the Royal Commission into Australian banks caught international attention. The public inquiry, led by a retired judge with broad coercive powers, uncovered what the media called a "litany of wrongdoing" including poor lending practices, lying to regulators, providing poor and inappropriate investment advice, charging fees without providing any additional services, forging customers' signatures on documents, and failure to act on legitimate client grievances.

Such high-profile scandals, which took place right before Aon conducted our biennial global risk management survey, help illustrate and explain why damage to reputation/brand has once again ranked as the number one risk for financial services institutions in Aon's 2017 Global Risk Management Survey.

In an age when a crisis could spread globally within hours or even minutes thanks to instant social media, the risk of reputational damage has exploded exponentially. It could occur because of an inappropriate tweet by an executive or a posting by an employee who complains about sexual harassment or discrimination. In addition, “fake news,” which started by political parties as a way to influence elections, has begun to spill over into the corporate world. Since social media platforms have no fact checkers, fake

news is gradually becoming rampant. At the same time, the U.S. election in November 2016 spawned a new trend—many companies with politically outspoken owners or CEOs are being increasingly caught in political crossfire that could threaten their corporate brands.

Even though brand equity, mostly comprised of customer loyalty, prestige and positive brand recognition, is considered part of a company's intangible assets, it directly impacts a company's bottom line. Past studies by Aon suggest that there is an 80 percent chance of a public company losing at least 20 percent of its equity value in any single month over a five-year period because of a reputation crisis.

Given that reputational events often arrive with little or no warning, and could be linked to any combination of other Top 10 Risks, organizations are forced to respond quickly and effectively in real-time. It is important for companies to have a comprehensive reputation risk control strategy in place to preserve consumer and employee trust. Meticulous preparation and executive training could prevent a critical event from turning into an uncontrollable crisis, and help maximize the probability of recovery.

Regulatory/legislative changes

Speaking of regulations, experts in the U.S. always reference the Dodd-Frank Act of 2010 to illustrate the costly burdens that regulators have imposed upon businesses. The Dodd Frank law came out in the aftermath of the global financial crisis with a noble intent— stopping banks from taking excessive risks to prevent another financial disaster. But at nearly 281 pages, the law, laden with complex reporting and disclosure requirements that involve five federal agencies, has become a key financial risk for businesses.

In 2016, Bloomberg quoted American Action Forum as saying that the cost of implementing the legislation, the most expensive in the law's history, soared to USD 36 billion and 76 million paperwork hours over a period of six years. From 2000 to 2007, Forbes says the developed economies' top performing banks had achieved an average return on equity of 26 percent.

Today, returns for many of these same banks are in the single digits; as a result, most are forced to reduce their size/footprint and increasingly rely on digital customer platforms. A study by Harvard University's John F. Kennedy School of Government concludes that the Dodd Frank Act accelerated the decline of America's community banks.

Businesses in other industries and other parts of the world face similar hurdles in the post-recession world. For example, in July 2016, the EU adopted legislation that imposes cyber security and reporting obligations on industries such as banking, energy, transport and health, and on digital operators like search engines and online marketplaces. Similar laws are being implemented in other countries, such as Australia and the U.S. (i.e. the State of New York). That explains why participants in Aon's Global Risk Management surveys have consistently ranked regulatory and legislative changes as a top risk during the past decade.

Fortunately, 2018 marks the start of a turning point in financial regulation. In May, Congress passed a bill that dilutes some of the stringent regulations imposed by the Dodd-Frank Act on the U.S. financial system, and is primarily aimed at making things easier for small- and medium-sized U.S. banks, which were seen as being affected by the tougher rules in a disproportionate manner. In fact, in Europe and Asia/Pacific, regulations have generated so much backlash that many pro-business politicians have made it a centerpiece in their political platforms. Britain's effort to leave the EU was partially driven by what many perceive as controls of "the meddling governments and dictates from Brussels."

Regardless of how the regulatory landscape will evolve, companies have increasingly recognized that regulation is no longer a secondary concern, but is now a primary consideration in their business strategies. Rather than seeing it as a burden, they look at this risk as an opportunity to create a competitive advantage over their peers who do not manage this process effectively.

Cyber crime/hacking/viruses/malicious codes

In July 2017, during one of the worst data breaches of all time, cyber criminals penetrated a large credit bureau and stole the personal data of 145 million customers in the U.S. The hacking could have an impact for years because the stolen data could be used for identity theft.

Incidents like this have no doubt changed the perceptions of Aon's survey participants (financial institutions), making them more aware of the deadly consequences of this rising risk. In the current survey, cyber crime/hacking/viruses/malicious codes jumped from number five to number three.

These concerns are justified. According to ITSP magazine, the number of data breaches has increased exponentially over the past few years, culminating in a record 1,579 breaches in the U.S. alone during 2017.

While these breaches pose an ever-increasing threat to any business, the financial sector has been disproportionately affected. Last year, 8.5 percent of data breaches involved the financial sector. Moreover, Forbes magazine claims that financial services firms fall victim to cyber security attacks 300 times more frequently than businesses in other industries.

The cost of cyber breaches is rising as well. A study by Accenture found that the average cost of cyber crimes for financial services companies globally has increased by more than 40 percent over the past three years, from USD12.97 million per firm in 2014 to USD18.28 million in 2017 – significantly higher than the average cost of USD11.7 million per firm across all industries. In fact, a 2016 survey showed that because of unauthorized activity on their accounts, 12.3 percent of people left their credit unions and 28 percent left their banks.

As cyber crimes become more rampant, costlier, and take longer to resolve, companies need to improve their risk readiness. This, according to experts, will require companies to recruit and build best-in-class red teaming capabilities, and accept that cyber security risk management is a critical part of doing business across industries. By being proactive through identity protection and resolution services, financial institutions can be better prepared to manage post-breach fallout and quickly pivot to customer retention outreach if they do fall victim. Cyber resilience requires a holistic approach to reduce the impact of a catastrophic cyber attack, including cyber threat analysis and better integration of business continuity and disaster recovery programs.

Insurance specifically designed to cover the unique exposure of data privacy and security can act as a backstop to protect a business from the financial harm resulting from a breach. According to a recent Aon Benfield report, there has been a significant uptick in demand for cyber insurance, particularly in the wake of high-profile cases. With approximately USD 1.7 billion in premiums, annual growth for cyber insurance coverage and product is running at 30 to 50 percent. However, risk management programs must be dynamic, pragmatic, and flexible in order to keep up with continuous and rapid innovation in technology and operations

While some categories of losses might be covered under standard policies, many gaps often exist, unless coverage is tailored to a financial institution’s unique exposures. Risk managers should work with their

insurance brokers to analyze such policies and determine any potential gaps in existing coverage because cyber events can impact numerous lines of insurance coverage, and coordination is essential.

Economic slowdown/slow recovery

In its January 2018 report, the World Bank forecasts global economic growth to edge up to 3.1 percent in 2018 after a much stronger-than-expected 2017. The growth was largely driven by recovery in investment, manufacturing, trade and farming commodity prices. In the U.S., the economy had a blockbuster second quarter in 2018, with growth surging to a 4.1 percent pace. That figure nearly doubled the first quarter rate of 2.2 percent, the strongest pace in nearly four years.

These moderate growth stats offer organizations some reasons for cautious optimism. Economic slowdown/slow recovery, which was consistently ranked as the number one risk facing companies worldwide since 2009, has understandably dropped for the second time to number four. For insurance and investment firms, this risk is listed at number six. For respondents overall (all industries), only three out of 10 respondents say they have a plan for, or have undertaken a formal review of, this risk and the percentage of organizations suffering a loss of income in the last 12 months has dropped slightly from 46 in 2015 to 45 in the current survey.

Due to current trade tensions and uneven growth prospects in other parts of the world, concerns over the global economy may not go away soon. The World Bank claims that the current upswing is largely seen as short-term. As central banks gradually remove their post-crisis accommodation and as an upturn in investment levels off, the World Bank predicts that growth in advanced economies is expected to moderate slightly to 2.2 percent in 2018. Over the next two years, global growth is expected to edge down, global slack to dissipate, trade and investment moderate, and financing conditions tighten.

The same sentiment is echoed by Mark Carney, the governor of the Bank of England, who, on the 10-year anniversary of the global financial crisis that the led to the worst economic downtown since the 1940s, warned the global financial community not to become complacent. In an interview with the BBC, Carney said major risks remain, even though a large part of the work to "fix" the financial system had been done.

To cope with the risk, organizations should learn from lessons in the past and embrace a long-term global perspective. We are no longer sitting on an island by ourselves. What happens on the other side of the world can have a direct impact on every organization, whether you have international operations or not.

Failure to innovate/meet customer needs

In May 2016, AOL Finance posted 30 nostalgic photos that depict some of America's most iconic companies and brands that have vanished over the past three decades— Woolworths, Polaroid, Alta Vista, Kodak, Blockbuster, Borders, Compaq, MCI and General Foods. The list goes on. There is an underlying factor in the featured companies— they believed that their product or service had an unlimited shelf life, but when they lost their competitive edge, they closed. These pictures convey a stark message—innovate or fail.

In an era when digital technologies play an ever-greater role in the way that businesses interact with customers and their workforces, the financial services sector can no longer rely on traditional channels. The industry is becoming increasingly competitive, with product development, delivery and consumer engagement all being driven by the need for a more mobile, social and data driven experience.

The urgency for innovation illustrates why respondents in the financial industry have listed failure to innovate/meet customer needs as a top five risk, jumping from number nine in the previous survey. Surprisingly, respondents from the banking sector list this risk at number 14. The result is consistent with surveys conducted by other organizations.

The Disruption House, a UK-based benchmarking and analytics firm, has recently released a report based on a survey of 150 financial institutions as to why banks fail to grasp innovation. The report concludes that banks, particularly systemically important banks, have a low innovation capability when compared with companies overall (lagging by 10-15 percent in a comparison with a generic all companies index). While the capacity for banks to make strong strategic moves in the market is high, it is not being consistently deployed. The main reason for this is that leadership has been slow to develop a vision of what the banking industry might look like in 10 or 20 years. There is little real thought leadership in terms of a vision of the future and a narrative to support people on the journey to creating a new industry.

The report also points out that banks appear to be working hard to develop innovative capabilities; however, these are still targeted at product, rather than process, which would help organize, structure and accelerate change. Many banks are suffering from gaps in intergenerational leadership dialogue, IT-business dialogue and a lack of coherence between strategy and innovation initiatives.

“We spend most of our time in this industry fixing today, and making incremental improvements,” said Kevin Hanley, director of design services at the Royal Bank of Scotland. “Innovation is different, it’s thinking about what tomorrow holds. Fail to do this and firms risk becoming disenfranchised from customer bases and losing market share to smaller, more agile players that can better harness technology to deliver a customer experience more aligned to customer expectation.”

Failure to attract or retain top talent

A report by Randstad, a global recruitment firm, underlines the reason why Aon's survey participants list failure to attract and retain top talent as a top risk, at number six. According to Randstad, financial institutions have been struggling to fill jobs, especially in the part of the market that has been impacted by increasing regulation and emerging geopolitical risks. Areas that are currently experiencing greater levels of demand include compliance, financial crime, regulatory projects, technology risk and enterprise-wide risk. Talent strategies must align to evolving businesses, as new and changing roles require a review of job profiles, selection, and performance management.

In addition, the macro-environment has also impacted the way organizations perceive the risk of failure to attract and retain talent. For example, population aging in industrialized countries has taken skilled employees out of the workforce at a faster rate than they can be replaced. Meanwhile, the workplace is changing with the rise of contingent workers, shifting work boundaries, and the addition of millennials who have different expectations about work.

These factors have no doubt deepened concerns for companies, adding more complexities to addressing the risk, which threatens to undermine future economic productivity and jeopardizes a company's competitiveness and profitability.

While many external factors are beyond the control of businesses, experts say companies should take proper measures to boost their efforts to mitigate this risk. One of these measures should be creating an ethical and employee-friendly work culture that helps attract and retain talent. According to Corporate Responsibility Magazine, 86 percent of surveyed females and 67 percent of males indicated that they would not join a company with a bad reputation. Conversely, many would be tempted by significantly

lower pay if a company possessed a stellar reputation and corporate culture. This distinction is particularly important in the context of financial services competing for technology talent. Pay levels for most roles are similar when comparing tech and banking, but tech firms have an advantage when looking at the full employee value proposition. Specific tech advantages are equity premium, innovative culture, and alternative work arrangements.

In short, organizations that fail to strategically and aggressively address the challenges in attracting and retaining talent could lose the competitive edge needed to thrive, especially as technology and digital drive change across financial services. At the same time, those who effectively incorporate talent strategies in their overall business planning can certainly gain an edge in the war for talent.

Increasing competition

A decade ago, people relied heavily on traditional intermediaries, such as a bank, to conduct their financial transactions. While the all-in, one-stop-shopping experience offered by large financial services providers remains an option that many still favor, new players are reshaping the financial system at an unprecedented pace.

This transformation, driven by technology innovation, is luring new non-bank competitors into providing financial products and services previously offered by established financial institutions. These non-traditional entities are now attracting customers with their convenience, digital experience, and competitive returns, while operating in a different regulatory context.

According to Forbes Magazine, Internet giants such as Amazon, Alibaba, Google and Walmart are offering an array of mobile and online payment solutions, digital wallet capabilities and other financial solutions that leverage brand trust, technology and scale. The increasing popularity of these fintech companies is disrupting the way traditional business has been done, creating a big challenge for financial institutions. To cope with the risk, companies need to adjust quickly to the changes – not just in technology, but also in operations, culture, and other facets of the industry.

Disruptive technologies/innovation

In the 2017 survey, we added disruptive technologies/innovation as a new risk category. Surveyed financial institutions have ranked it number eight. In many ways, this risk is interconnected with increasing competition, which we have discussed in the previous section.

The term disruptive technology first appeared in a book written by Harvard Professor Clayton Christensen, who categorized technologies as "sustaining" and "disruptive." While the former produces incremental improvements in the performance of established products, Christensen said the latter "tends to reach new markets, enabling their producers to grow rapidly, and with technological improvements to eat away at the market shares of the leading vendors."

A report by the McKinsey Global Institute recently identified 12 technologies that could drive truly massive economic transformations and disruptions in the coming years. Among those listed are advanced robotics, energy storage, 3D printing and the Internet of things.

For the financial services industry, one of the most talked-about disruptive technologies today is blockchain. If fully adopted, it will enable banks to process payments more quickly and more accurately while reducing transaction processing costs and the requirement for exceptions. However, to capitalize

on this potential, banks need to build the infrastructure required to create and operate a true global network using solutions based on this transformative technology.

The McKinsey Global Institute report estimates that applications of these technologies could have a potential economic impact of between USD 14 trillion to USD 33 trillion a year in 2025. Some of the innovations, said the report, could profoundly disrupt the status quo, alter the way people live and work, and rearrange value pools.

With such significant impact, it is not surprising that participants from all sectors project this risk to be number 10 in three years. For financial institutions, digital is no longer a strategy; it is part of the business, requiring investment in technology and transformation.

According to Jeffrey Baumgartner, who authored “The Way of the Innovation Master,” far-sighted companies do not ignore radical new inventions that threaten to disrupt their markets. It is critical that business and policy leaders understand which technologies will matter to them, and prepare accordingly. They either chase the market by quickly changing their strategies and products to maintain their place in the same marketplace, or explore new markets based on their expertise.

Growing burden and consequences of corporate governance/compliance

The financial crisis of 2007 and 2008 revealed severe shortcomings in corporate governance for financial institutions. When most needed, existing standards failed to provide the checks and balances that companies need in order to cultivate sound business practices. Concerns for corporate governance in the recovery period are reflected in Aon's 2017 global risk management survey. Surveyed financial services companies list it as a number nine risk. It was ranked at number eight in 2015.

According to The Organisation for Economic Co-operation and Development, corporate governance involves a set of relationships between a company’s management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means for attaining those objectives, as well as how monitoring performance is determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders, and should facilitate effective monitoring.

The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy.

Effective corporate governance practices are essential to achieving and maintaining public trust and confidence in the financial systems, which are critical to the proper functioning of the global economy. Poor corporate governance may contribute to company-wide failures, which can pose significant public costs and consequences. In addition, poor corporate governance can lead markets to lose confidence in the ability of a financial services company to properly manage its assets and liabilities.

Technology failure/system failure

In June 2018, a computer failure at a large retail and commercial bank in the United Kingdom left nearly two million customers without access to online banking services. The incident left the group

“overwhelmed” and unable to properly assist consumers. In the aftermath, the bank lost more than 10,000 customers and experienced more than 10,000 incidents of fraud.

With a heavy reliance on technological infrastructure, businesses are becoming more vulnerable to system failures. When we look at the list of banks hit by outages in the past few years alone, the common theme is that they are all well-respected, long-established players within the financial services sector with vast customer bases of both consumers and businesses alike.

Chris Dutta, an expert at the U.K.-based Piccadilly Group, a leading Test and Intelligence Agency within Financial Services, contributes IT failures to the following factors:

First, financial institutions have multiple and diverse applications, messaging protocols and data warehouses, all of which make the process of maintaining and testing an end-to-end platform incredibly difficult. The complexity has been further exacerbated by large fragmented legacy systems dating back decades.

Secondly, across all transactions, there are now multiple parties originating from different countries. These result in a tangled web of overlaying systems supported by globally dispersed teams, further widening the margin for error.

And finally, there is the lack of cohesion and conversation between the financial services firms and intermediaries, as well as within the organizations themselves. In the digital race to win market share, some organizations are creating closed, independently developed technical and data models without fully understanding the risk profile of these models.

Across financial services sectors, significant security breach and incident activity has involved service providers, other third parties, and members of the supply chain. Establishing a robust third-party risk management framework and governance program is critical to the identification, analysis, remediation, and monitoring of threats, vulnerabilities, and risks inherent in the financial services industry and introduced by outside entities. Without a marked change in investment and management, there may be more frequent disruptions, damaging the functionality and ultimately the credibility of businesses and loss of customers.

Financial Institutions vs. Technology/Telecommunications

Recent years have born witness to the introduction of technology solutions that have accelerated the transformation of the financial services industry. Today, almost every type of financial activity — from banking to payments to wealth and risk management — is being shaped and re-imagined by technological innovations. Due to its tremendous impact, it is necessary to compare the top 10 risks chosen by participants from these two sectors:

Technology/Telecommunications	Financial Institutions
1. Cyber crime/hacking/viruses/malicious codes	1. Damage to reputation/brand
2. Damage to reputation/brand	2. Regulatory/legislative changes
3. Failure to innovate/meet customer needs	3. Cyber crime/hacking/viruses/malicious codes
4. Disruptive Technologies/Innovation	4. Economic slowdown/slow recovery
5. Failure to attract or retain top talent	5. Failure to innovate/meet customer needs
6. Increasing competition	6. Failure to attract or retain top talent
7. Loss of intellectual property	7. Increasing competition
8. Regulatory/legislative changes	8. Disruptive technologies/innovation
9. Technology failure/system failure	9. Growing burden and consequences of corporate governance/compliance
10. Merger, acquisition and restructuring	10. Technology failure/system failure

For technology companies, computer crime/ hacking/viruses /malicious codes has jumped from number five in the 2015 survey to number one. This same risk has also entered the top three list for FI.

While new technologies such as cloud computing, social media, mobile devices and big data analytics have helped companies achieve profits and reach operational goals, they also face an increasingly diverse and sophisticated array of threats to the security of their information management systems. Each time the industry develops or adds a new feature to a system, the chance of cyber risks rises. Each time it comes up with new potent tools, a new crop of hackers emerges with more damaging cyber attack techniques. As hackers and anti-hackers remain locked in a fierce arms race, this risk will continue to be ranked highly by both tech and financial services companies.

It's worth noting that such concerns have prompted organizations across all industries and geographies to either adopt cyber risk assessments (53 percent), transfer greater risk to the commercial insurance market (33 percent), or evaluate alternative risk transfer measures (captive use is projected to rise from 12 percent to 23 percent by 2020). However, only 23 percent of companies currently employ any financial quantification within the cyber risk assessment process.

Without measuring the actual financial impact of identified cyber threats, companies will not be able to adequately prioritize their capital investment in risk mitigation, financing, and transfer, or link cyber to the risk appetite, and risk managers will not obtain sufficient attention from their boards.

Furthermore, Aon's 2017 survey reveals a lack of cross-functional collaboration in risk management decision-making. When cyber risk assessment does take place, about 38 percent of respondents say risk control strategies involve the risk department (this low number could be influenced by the fact that many surveyed organizations do not have a risk management department), and 86 percent within the technology group, 13 percent within the legal department, and five percent within the HR team.

This is troubling. As sweeping cyber regulatory changes related to privacy and disclosure are occurring throughout the EU and Asia, and social engineering—whereby hackers trick people into offering them access to sensitive information through phone calls, emails or social media—is becoming one of the most effective attack paths into an organization, companies need to broaden their collaboration with other functions to ensure an integrated approach to the cyber challenge.

Another risk that both sectors rank very high on the top 10 list is disruptive technologies/innovation, a new entry introduced in Aon's 2017 Global Risk Management Survey. Participants across all industries list this risk at number 20, but it is ranked at number four and number eight by the tech and financial services sectors respectively.

When mentioning disruptive technologies/innovation, one might assume that it merely applies to the tech industry. In fact, they're closely interconnected and each industry has its own potential disruptors. For the financial services sector, artificial intelligence and blockchain have caught the attention of many large institutions.

Hailed as one of the biggest disruptors on the market, artificial intelligence, or AI, is now being used across a number of industries, from research and consulting to transportation and medicine. It has already become part of many daily lives - Siri, Alexa and Google Assistant are perfect examples. Within the business world, AI will give companies the ability to forecast trends as well as customer behaviors and needs, which can quickly result in more tailored product development.

Another relevant disruptor is blockchain technology. Blockchain is the technology underlying cryptocurrencies, which allow people to invest and exchange on online marketplaces and to purchase physical goods, but it also has a variety of non-payment use cases. Since blockchain consists of a set of digital ledger systems applied in a distributed fashion without a central depository or authority, it enables users to record transactions in a public ledger within their community, yet no changes can be made once published. The technology aims to eliminate centralized control and promote an even distribution of power over information across community members.

While blockchain is touted as a blockbuster innovation for the tech sector, it is also becoming popular among large financial institutions, which see the technology as an effective tool to keep confidential information, contracts and deals secured and unchangeable, enabling more efficient record keeping and reducing administrative expenses.

Regardless of what disruptor each industry faces, it is critical that corporate leaders and risk managers understand these technologies and embrace disruption to reinvent themselves.

Lastly, we want to mention two risks that are ranked low by participants overall, but highly by those in the tech and financial services industries. First, IT companies consider loss of intellectual property as a

serious threat. Intellectual property is the lifeblood for many companies in the high-tech industries, yet steep competition with developing economies has led to sabotage and theft. A recent Verizon study says that counterfeiting and piracy cost companies as much as USD 630 billion per year.

Secondly, FI participants are deeply concerned about corporate governance, which, they believe, lack proper checks and balances to protect the well-being of companies and encourage sound business practices.

Projected Risks

Risk	Rank
Regulatory/legislative changes	1
Cyber crime/hacking/viruses/malicious codes	2
Failure to innovate/meet customer needs	3
Economic slowdown/slow recovery	4
Failure to attract or retain top talent	5
Damage to reputation/brand	6
Increasing competition	7
Disruptive technologies/innovation	8
Growing burden and consequences of corporate governance/compliance	9
Political risk/uncertainties	10

Since the 2017 survey was conducted in October 2016, political events such as the Brexit initiative in the United Kingdom and the U.S. election introduced a new level of uncertainty into the challenging regulatory environment for financial institutions. That explains why surveyed financial services companies project regulatory and legislative changes to be a number one risk in 2020.

Since then, the regulatory landscape has improved slightly. In the U.S., the Trump administration's deregulatory push has led to the passing of legislation in May 2018 that dilutes some of the stringent regulations imposed by the Dodd-Frank Act on the U.S. financial system. Similar reforms are happening in Europe and Asia/Pacific regions. Despite these encouraging trends, financial institutions have not experienced a substantial lessening of regulatory challenges. We agree with survey participants that regulatory/legislative changes will loom large on the horizon and the cost of compliance will remain significant.

On a related note, damage to reputation/brand, which has been ranked number one by FI participants in the past two surveys, is projected to drop to number six. Such confidence might be driven by the belief that the financial services industry has recovered its reputation, which was among the worst hit during the 2008 financial crisis. There are plenty of reasons for optimism. In June 2017, American Banker released the results of its 8th Annual Bank Reputation Survey, which revealed that the banking industry overall extended its multiyear reputation recovery among U.S. consumers, achieving a reputation score that qualified as "strong" for the first time since 2011.

However, with the exponential increase of cyber crimes and enhanced regulatory enforcement in many parts of the world, we believe that damage to reputation/brand will remain a top FI risk.

Lastly, FI participants have added political risk/uncertainties to the projected top 10 list. Given the current political turmoil around the world, this new addition is hardly surprising. Among the contributing factors to political uncertainties, globalization is seen by many as a chief, if not a sole culprit. In the past,

globalization has brought greater connectivity to the world, enabling people, goods and services to move freely, and improve the quality of life, especially for people in the developing world. However, it has also triggered backlash from those who have been left behind, prompting populist leaders in the West to pull back and protect what they believe is in their national interest. Thus, the rising economic and ideological nationalism in the West, coupled with different brands of nationalistic fervor stoked up by political leaders in Russia, China, the Philippines, Venezuela and Turkey, have sparked concerns for potential trade wars, stock and currency market crashes, territorial disputes, and military conflicts.

Interestingly, developed nations, such as the United States and United Kingdom, which were traditionally associated with political stability, are becoming new sources of volatility and uncertainty that worry businesses, especially those in the emerging markets.

Divergence in Participant Role Priorities

This year's survey has revealed some divergent perspectives. For example, based on the overall results by surveyed financial institutions, failure to innovate/meet customer needs and failure to attract/retain talents are ranked number five and number six respectively. However, when we break the data down by specific firms, we notice that banks are more concerned about capital availability/credit risk (number five); crime/security crime/theft/fraud/employee dishonesty (number seven); and directors and officers personal liabilities. Therefore, it is important to risk managers to customize their solutions and address risks specific to their own firms or sector.

In the overall survey, CEOs and CFOs rank as very high those risks with strong concrete financial implications— economic slowdown/slow recovery and damage to reputation/brand, while risk managers worry more about cyber security and political risk/ uncertainties. Such diverse views illustrate the importance of gathering a cross section of stakeholders in the decision-making process, since each one can bring a different perspective. It is also imperative that senior executives and the board of directors communicate with risk managers, and take an active role in assessing and overseeing the company's risk exposure to ensure it is in line with the company's strategic goals.

Evolution and Innovation in Risk Management

The study shows risks that are currently difficult to insure are emerging as major concerns for global organizations (the majority of the risks among the featured top 10 list are not insurable). This explains why financial services companies have indicated that they are less prepared for risks, despite more data and analytics and mitigation solutions available. In fact, risk readiness is at its lowest since Aon launched its survey in 2009. This means that the insurance industry will have to be more innovative and expand their products and programs to address some of the most complex and challenging risks.

While it is hard to predict which risk might emerge large and demand our immediate attention, we can be certain that successful companies will not be the ones taking a "wait and see" approach. Instead, they will be the ones who prepare themselves thoroughly and undertake the difficult process of finding solutions to address immediate needs while identifying opportunities for long-term growth. They will not just fix what is broken, but view their new circumstances as a portal to the next generation of business opportunity.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.