Commerce Next: The rise of digital commerce risk

Technology Institute

At a glance

Emerging risks and market disruptors are stressing the limits of digital operating models, talent pools, and risk management practices

November 2015
The Commerce Next series provides PwC’s perspectives relative to the trends and challenges that businesses should consider to remain competitive in today’s evolving digital marketplace. PwC has identified a multi-phase customer lifecycle that is an important aspect of digital commerce. In this paper, we look at the dynamics of digital commerce which include a broad range of strategic, financial, regulatory, and operational risks that are stressing the limits of digital operating models. These dynamics may pose a risk to the brand and reputation of your company. Are you prepared?
Key considerations

- Your digital commerce strategy will be impacted by Megatrends and other market disruptors leading to unanticipated risks.
- “By 2017, 1/3 of large enterprises engaging in digital business will have a digital risk officer or equivalent.” It is important to understand the drivers behind this significant change and implications to your operating model.
- The landscape of digital commerce risks is expansive (strategic, financial, operational, regulatory) and requires a strong and proactive risk management culture.
- 59% of CEO’s see greater risk this year than three years ago. Is your company building the risk resilience capabilities needed to protect your brand and reputation?

What your company needs to know

- Your digital strategy will need to adjust for major market forces that will reshape how your company sells, delivers, and services its customer base. PwC’s Megatrends detail five major disruptors that are changing the landscape of the traditional digital business model. This article explores two of these disruptors and discusses how your risk management approach can turn these into a strategic advantage.
- The rise of mobile as a digital commerce channel adds new revenue streams and increased opportunities to engage your customers. However, this trend also introduces a variety of new risks. Mobile commerce is less secure, brings more technology and security risk, and adds a new channel to already-complex operating models.
- Security risks are the tip of the iceberg. Strategic, financial, regulatory, and operational risks may pose threats to your brand, reputation, and bottom line. Develop an understanding of your critical risks that span these dimensions and proactively develop appropriate mitigation strategies.
- Digital risk governance requires a new set of mandates that expand beyond the traditional scope of Chief Information Security Officer (CISO) and Chief Risk Officer (CRO). Digital operating models need to incorporate many corporate functions, including marketing, merchandising, technology, customer support, and finance. As the Internet of Things (IoT) magnifies increased dependencies and overlaps within your organization, your company may consider investing in developing a Digital Risk Officer (DRO).

---

2 PwC: 18th Annual Global CEO Survey, January 2015.
Digital disruptors – Megatrends

Risks and considerations

Strong growth in digital commerce

The digital commerce market is experiencing massive growth as the breadth of digital channels expands and the reach of traditional retail remains stagnant.

Industries from Hospitality to Financial Services to the Technology Sector are moving towards a digital strategy to engage, attract and retain new customers. Customer experiences and expectations across traditional ecommerce, mobile and social channels are evolving at an alarming pace.

Last year in the US, digital commerce grew 15.5% over 2013 vs. 3.7% for traditional retail. Internationally, the number is even higher with a 21% year over year growth rate. In 2014, there were 197 million digital shoppers making up a $304B market that will expand to $491B in 2018.

Adding complexity to this rapid growth are a few major market disruptors, known as “Megatrends.”

Megatrend #1: The shift in economic power and implications to international expansion through digital channels

We are seeing a significant realignment of global economic and business activity from the G7 Countries to E7 (China, Russia, Brazil, India, Indonesia, Mexico and Turkey). By 2050, the GDP of the E7 will nearly double that of the G7. So what does this mean for you?

Companies are now aggressively adopting digital strategies that help get their products and services into these new markets. International expansion through digital channels has a quantifiable upside (as does entry into these markets through traditional channels), but the risks and challenges are vast. Here are several considerations:

1. Your company will need to significantly scale Anti-bribery Anti-corruption (ABAC) controls and monitoring.

2. The more you engage and sell in emerging markets online, the more mature your third party risk management program should be. For example, partnerships overseas with ecommerce “white label” partners and marketplaces are common. They should be assessed with the same rigor as any other critical supplier.

3. As your digital business model becomes more complex and global, the emphasis on privacy and security for customer information and IP will significantly increase. Assess whether your security, anti-fraud, and crisis response programs are appropriately funded. Fraud is becoming more prevalent online resulting in financial losses. For every $1 of online fraud, a company spends over $3 in mitigation costs.

Megatrend #2: Technological breakthroughs and implications to your digital business model

Our clients are experiencing significant stress on their digital business models given several market disruptors. The “Internet of Things,” or IOT, is not a new market disruptor, but it is, perhaps, the most disruptive for one reason: Complexity. So what does this mean for you?

---

4 PwC: Five megatrends and their implications, April 2014.
5 LexisNexis Risk Solutions: True Cost of Fraud Study; Post Recession Revenue Growth Hampered by Fraud as all Merchants Face Higher Costs. August 2014.
The combination of the Internet, mobile devices, data analytics, and cloud computing will continue to transform how companies operate and compete. Many organizations across all sectors are grappling with how these developments will affect consumer expectations and interactions, as well as the supporting business model.

Consider the risk implications to your digital business model as it relates to big data, your operational technology infrastructure, and your monetization strategy. Simply put, your business model will need to scale to keep pace and manage the associated risks successfully.

Know your business model risks:

54% By 2018, 54% of digital commerce will be mobile vs. 19% today

The “rise of mobile” is another market disruptor that is forcing companies to invest in translating the online experience to the mobile phone and tablets. While many consider traditional enterprise commerce their primary digital channel, the reality is that mobile commerce is either supplementing or replacing the traditional approach altogether. So what does this mean for you?

Operating model risks persist; capabilities that were once offered online now need to be duplicated or altered to the mobile channel to deliver on these experiences.

In 2014, over 125 million people used mobile for research. Mobile also accounted for 19% of total online sales. By 2018, that figure will jump to 54%, a 184% increase. The mobile channel is less secure and comes with higher incidences of fraud that may cut into your bottom line.

Is your business model scalable to meet this trend? Do you have the engineering and skills needed to operate both channels together and handle their different risks?

---

Looking beyond just security

Drivers for a stronger risk management program

Strategic risks

The combination of rapid growth (especially internationally and in emerging markets) and market disruptors (e.g. the rise of mobile) creates a new set of strategic risks.

Invariably, your strategy will have a vision, mission, a set of critical objectives and an understanding of how to differentiate your products or services. Business model, macroeconomic, reputational, brand, and disruptive trends are strategic risks which need to be evaluated and incorporated into planning.

Consider this scenario: Your company has developed a strategy to expand your digital channels to reach new markets, invested in research and analytics, and you have the funding necessary to begin planning. Your team has analyzed revenue potential, assumptions and initial costs. The demographics and consumer segments for your products and services line up on paper.

What’s next?

Selecting the right business model for digital commerce is not a simple exercise and a careful understanding of the benefits and risks is warranted. For example, you can build your own set of capabilities or you could buy them by partnering with a third party or online marketplace. Each of these scenarios has a unique set of risks.

If you decide to build your own or scale your existing commerce engine, you will likely assume supply chain, tax, regulatory and human capital risks. These risks are compounded when entering foreign markets and navigating local laws and government regulations. While some organizations are equipped to manage these, many find that outsourcing the operations of digital commerce to a third party reduce many of these risks. On the other hand, choosing not to outsource offers greater control of your customer experience, support, pricing and branding.

Operational risks

Operational risks are by far the largest category and have major implications on your operating model. These include:

Online fraud and payment risk:
With online fraud continuing to rise, its implications are very real. Fraud in the mobile channel currently costs companies 3% of revenue. Strong anti-fraud, PII and PCI compliance programs are critical.

Operating model risks: Some risks span the lifecycle of your customer journey – from discovering your product to shopping to transacting and, eventually, fulfillment. Does IT have the agility to configure the social, mobile and enterprise commerce channels in parallel? Are your Standard Operating Procedures and handoff points between functions documented and understood? How effectively does the operating model support localization in terms of personalization and in identifying unique characteristics? We’ve seen clients enter markets with the wrong payment types, fail to address tax considerations, or not fully understand shipping requirements, including a plan for reverse logistics.

Social media risks: 65% of companies don’t have a policy in place that informs employees of acceptable social media use, or are unsure if one exists. 63% of organizations believe social media presents a significant security threat, yet only 29% have sufficient controls in place to manage this risk.

Governance around proper information distribution, employee accountability, and security safeguards for hacking and social malware can help limit reputational, regulatory, and legal risks.

---

8 Pymnts.com: Rising Mobile Commerce Fraud Costing Retailers, February 2015.
9 Ponemon Institute (sponsored by Websense): Global Survey on Social Media Risks, September 2011.
10 Of companies don’t have a social media policy that governs employee use, or are unaware of one exists.10

Know your social risks:

Technology and engineering risks: Technology challenges are daunting and make up the largest category of operational risks. System downtime can have a bottom line impact in terms of financial loss. Poor system performance can translate into lost sales and a negative customer experience.

In addition to downtime, companies are focusing on “responsive design” – the translation of the online experience to the mobile phone or tablet. The engineering and capabilities required for this initiative are not easy to source or build. Consider your talent and people gaps that this technology trend is driving.

Security risks: Security is top of mind for executives and is front and center of the digital risk agenda.

Breaches that compromise millions of users’ personal information are becoming regular news headlines. Moreover, these attacks are occurring at big-brand, reputable firms that invest heavily in security measures.

The financial losses to each affected company is in the millions (even after cyber liability insurance is deducted), and the reputational loss can be even more damaging. Further, the trend is getting worse, not better. Cyberattacks are increasing at a 66% year over year clip.11 This topic is not just a commercial entity issue; it is a national security concern as well.

The National Institute of Standards and Technology (NIST) recently issued a new framework for critical infrastructure to help manage and reduce cyber security risk as part of a Presidential Executive Order. We are seeing our clients aggressively incorporating this new voluntary framework, in an effort to adopt federal guidelines.

This article will not cover the breadth of our Security practice; however one critical area for immediate consideration is how your company is addressing cyber threats that surface via third parties. Your organization should have a strong supplier risk management program with strict policies and clear accountabilities that include your suppliers, vendors, and channel partners.

Regulatory and compliance risks

The regulatory and compliance requirement landscape is intimidating. Failing to comply can lead to hefty fines and increased security and financial risks. The challenge most companies face is how to manage this complexity and effectively prioritize resources to focus on the right set of activities.

Among the most common requirements are:

- Finance and Accounting (e.g., SOX, SSAE, IFRS)
- Tax (e.g., FACTA)
- Privacy/Information Security (e.g., NIST, ISO)
- Customs and Trade Requirements
- Export Regulations
- Anti-Corruption/Anti-Bribery (e.g., FCPA)

Navigating local laws and regulations (especially internationally) adds another layer of intricacy to a digital business. We recommend a very strong Compliance Management Office (CMO) for your digital store that works closely with a company’s Internal Audit function. Your CMO should be completely up to date with your strategy, growth objectives, and standard operating procedures. Moreover, it needs the resources (people, funding, and visibility) to be successful. Too often, this function is commonly viewed as a cost center and its importance is underestimated. Instead, it should be characterized as a value added cost avoidance center.

10 Ponemon Institute (sponsored by Websense): Global Survey on Social Media Risks, September 2011.

Financial risks

The majority of financial risks fall into three primary areas: data breach, fraud, and site performance. Consider these questions:

Do you know your company’s cost of online fraud as a percent of revenue?

Do you know how much your company spends mitigating fraud?

Do you know what financial losses you’ve incurred as a result of downtime?

Have you studied the potential loss of customers (and future revenue) that would result from a data breach?

The figures driving the questions above are alarming. For example, large ecommerce merchants’ fraud losses stand at 1.21% of revenue. Moreover, companies spend over $3 in mitigation costs for every $1 of fraud. These two statistics directly affect the bottom line and should be on the forefront of the CFO/CIO agenda.

Financial losses due to system outage and network downtime are a serious matter for organizations, but with a digital commerce business model, the urgency is magnified given the revenue impact. The average cost to a company of unplanned downtime is $5,600/minute. This includes containment costs, recovery costs, detection costs, etc. Compounding these costs is the lost revenue during the downtime. Strong IT controls with frequent testing can greatly support the prevention of unplanned outages.

Know the numbers on security and financial risks:

Year over year increase in cyber attacks

Cost to a company for every $1 of online fraud

Cost to a company for every minute of unplanned downtime

66%

66%

$3.08

$5,600

12 LexisNexis Risk Solutions: True Cost of Fraud Study; Post Recession Revenue Growth Hampered by Fraud as all Merchants Face Higher Costs, August 2014.


Re-think your digital commerce risk practices

What your company can start doing now

Invest in a Digital Risk Leader

Gartner predicts that “by 2017, one-third of large enterprises engaging in digital business will have a digital risk officer or equivalent.”

What’s driving this trend? Digital commerce risk is broader than just security. It requires a blend of both business and technical acumen. The ability to identify the financial risks of a digital business model requires sufficient knowledge in planning, budgeting and analytics. The same goes for digital marketing and customer risks.

How can this role be successful?

• **Your Digital Risk Leader should be accountable for risks within a digital operating model.** Too often, the management and governance of risks within a digital operating model fall within the jurisdiction of different groups, creating inconsistencies in approach, reporting, tools, etc. Assess your digital operating model and all functional areas that it touches to create the template for your Digital Risk Leader.

• **Understand and address responsibilities that overlap with the CISO.** Strong security and privacy processes are critical to your brand and reputation. While every organization is unique in terms of CISO reporting relationships, most tend to report to the CTO/CIO. Be cautious not to rush into a re-org or change processes. Instead, explore a gradual shift of reporting accountabilities to a Digital Risk Leader.

• **Empower your Digital Risk Leader with “tone at the top.”** We have seen many valuable reports that detail meaningful risk findings and mitigation strategies, only to be consumed and quickly forgotten. Risk leaders need the support at the top to drive accountability. Risk management is a strategic imperative and should be treated as such.

Drive stronger Enterprise Risk Management (ERM) for your online and mobile channels

All companies face uncertainties. Those that generate revenue through digital business models are no exception. Don’t understate the importance of a strong ERM program to help you navigate those risks.

If properly invested and supported, your ERM program should accomplish the following:

1. Align your risk appetite with your digital strategy
2. Enhance your risk response decisions
3. Reduce operational surprise and losses
4. Identify and manage multiple and cross-enterprise risks
5. Help you seize opportunities
6. Improve the deployment of capital

Support ERM at the highest levels of your organization and properly prioritize all communications and findings, rather than pushing ERM responsibilities and accountabilities to mid-level managers.

---


© Gartner Foundational September 2015 G00264735

© Enterprise Risk Management—Integrated Framework: Executive Summary, ©2004

Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.
Commit to stronger governance for compliance and reporting

Recognize the role governance plays in driving a culture of accountability and compliance. Many companies manage risk on an annual, semi-annual, or ad-hoc basis. However, benefits come with stronger governance:

1. Predictable management reporting
2. Stronger culture of accountability
3. Predictable and consistent messaging to business and process owners
4. Easier ability to drive compliance with controls testing
5. Better cross-functional coordination across your digital operating model

Recognize the need to change

Companies are beginning to recognize that risk management practices must innovate and evolve in parallel with technology. Start challenging traditional roles and traditional assumptions.

Many organizations are already taking the first step. We are seeing:

1. Chief Risk Officers (CRO’s) aggressively adding digital skills to their teams or sourcing externally
2. CEO’s creating a role for a Digital Risk Officer
3. More focus from Internal Audit on digital commerce risk compliance
4. Greater transparency and cooperation across siloes with executive mandates to drive accountability, especially with security and fraud in highly matrixed organizations.

84% of technology executives said they are either planning a change in the way they manage risks or have already started this change.17

33% of large enterprises will have a Digital Risk Officer by 2017.18

---

PwC can help
For a deeper discussion on digital commerce risk, please contact one of our leaders:

**Joseph Lamano**  
Principal, Digital Commerce Leader  
408 817 4427  
joseph.lamano@pwc.com

**Kevin J Keenan**  
Principal, US Risk Consulting  
310 848 5524  
kevin.j.keenan@pwc.com

Let’s talk
Please reach out to any of our technology leaders to discuss this or other challenges. We’re here to help.

**Pierre-Alain Sur**  
US Technology Industry Leader  
646 471 6973  
pierre-alain.sur@pwc.com

**Kayvan Shahabi**  
US Technology Advisory Leader  
408 817 5724  
kayvan.shahabi@pwc.com

**Kevin Healy**  
US Technology Assurance Leader  
408 817 3834  
kevin.healy@pwc.com

**Diane Baylor**  
US Technology Tax Leader  
408 817 5005  
diane.baylor@pwc.com

Acknowledgements
The following PwC professionals contributed their experience and knowledge to produce this paper.

**Jonathan Finch**  
Director, Digital Commerce Risk  
858 405 8792  
jonathan.t.finch@pwc.com

About PwC’s Technology Institute
The Technology Institute is PwC’s global research network that studies the business of technology and the technology of business with the purpose of creating thought leadership that offers both fact-based analysis and experience-based perspectives. Technology Institute insights and viewpoints originate from active collaboration between our professionals across the globe and their first-hand experiences working in and with the Technology industry. For more information please contact Pierre-Alain Sur, US Technology Industry Leader.