Deloitte.

Gaps in the digital net

How retailers can close the risk holes

In the new digital era, do organizations have a false sense of security, perhaps even complacency, resulting from their investments in non-agile risk management tools and processes they have relied on for years?

Digital is redefining relationships in retail. The forces of social media, omni-channel shopping[1] and a spate of emerging technologies are transforming the retail industry, compelling companies to rethink almost every aspect of their operations and pushing them to come up with novel, innovative ways to accommodate customers. But as they wade deeper into the digital waters, retailers will need to contemplate an entirely new set of risks. It will not be enough to consider these risks piecemeal. Only by looking at the larger picture and determining how these risks are interconnected will retailers be able to develop approaches to anticipate and manage them and capitalize on the opportunities they may bring.

Figure 1. Consumers are using multiple channels to research and purchase

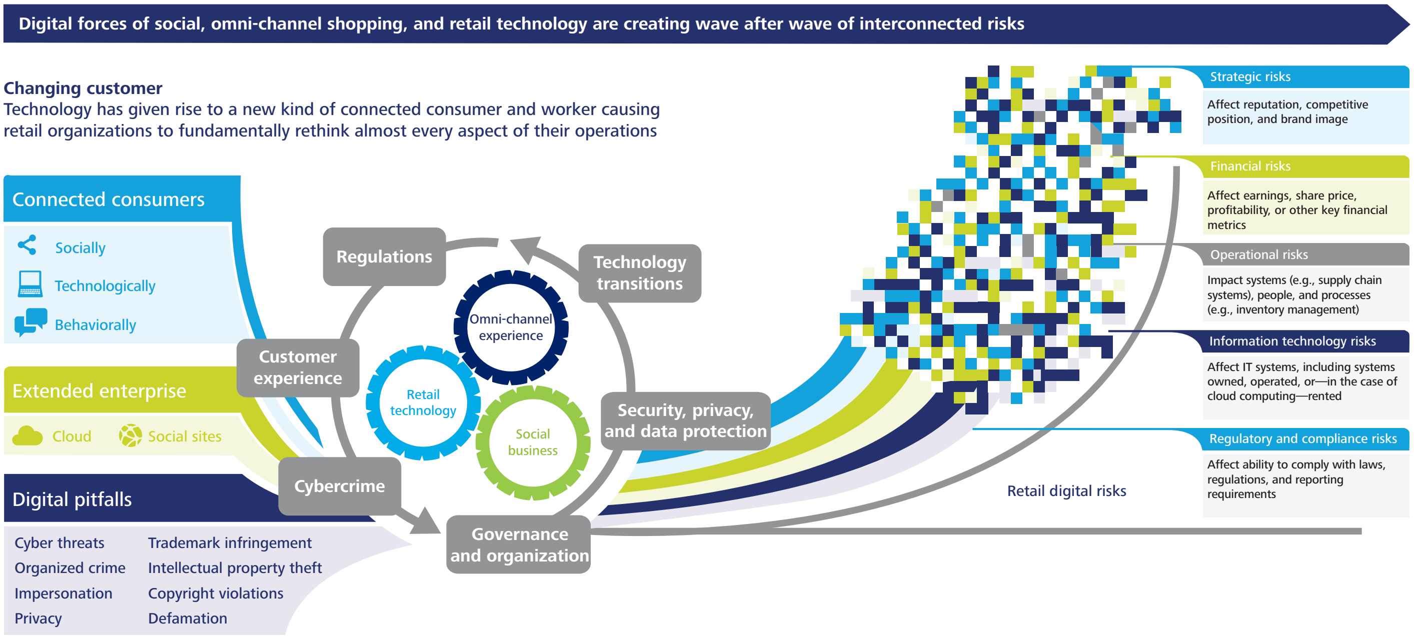
58% **of Omni-channel consumers** are not loyal: in-store price comparisons lead to delayed purchases elsewhere when lower prices are found[2]

78% **of Shoppers use two or more** channels to research and purchase an item[3]

41% **of Smartphone users** are interested in using their mobile phone to pay for an item in-store, rather than using a cashier[4]

66% **of Tablet owners** use their tablets for shopping purposes[5]

Figure 2. Retail digital landscape



Digital forces of social, omni-channel shopping, and retail technology are creating wave after wave of interconnected risks

Changing customer
Technology has given rise to a new kind of connected consumer and worker causing retail organizations to fundamentally rethink almost every aspect of their operations

Connected consumers
- Socially
- Technologically
- Behaviorally

Extended enterprise
- Cloud
- Social sites

Digital pitfalls
- Cyber threats
- Organized crime
- Impersonation
- Privacy
- Trademark infringement
- Intellectual property theft
- Copyright violations
- Defamation

Strategic risks
Affect reputation, competitive position, and brand image

Financial risks
Affect earnings, share price, profitability, or other key financial metrics

Operational risks
Impact systems (e.g., supply chain systems), people, and processes (e.g., inventory management)

Information technology risks
Affect IT systems, including systems owned, operated, or—in the case of cloud computing—rented

Regulatory and compliance risks
Affect ability to comply with laws, regulations, and reporting requirements

[1] A customer-centric experience that seamlessly connects a company's digital and physical stores and allows buyers to sample and purchase merchandise via a variety of mediums, including in-store, online, and mobile.
[2] "Winning the Mobile Consumer Showdown," McKinsey, March 2012.
[3] "Cross-Channel Commerce: A Consumer Research Study," Oracle, March 2011.
[4] "Mobile Trends: Consumer Views of Mobile Shopping and Mobile Service Providers," Oracle 2011.
[5] "How US Smartphone and Tablet Owners Use Their Devices for Shopping," Nielsen, March 2012.

Approach to digital risk management should begin with an understanding of the organization's digital footprint and what digital risks impact the "heart of the business"

Casting a new net – Strategic certainty in the digital age

The declining cost of technology has allowed a growing number of people to participate in a lifestyle of constant connectivity. Today's typical consumer is now able to access the Internet 24/7 via a panoply of smart, portable, and highly usable devices. For many, these devices are critical to the shopping experience — from real-time research and price comparisons to completing the actual purchase.

To win over the new digital shopper, retailers will have to expand upon their efforts to create a unified customer experience across in-store, online, mobile, and other retail channels, while at the same time juggling the risks that accompany this transition.

Social media has given rise to another phenomenon: an increased willingness on the part of consumers to share personal information, including birth dates, individual likes and dislikes, purchase histories, and biometric details (height, weight, health status, etc.). It is a trend that is not lost on retailers: they are finding ways to capitalize on a host of customer data and past behaviors, creating individualized customer experiences that promote brand loyalty. In fact, consumers often engage more readily with retailers that create tools (social, incentive, loyalty, etc.) which offer not only an exceptional customer experience but that cater to their unique purchasing criteria.

Clearly consumers benefit from better tailored shopping experiences — from exclusive offers, discounts, recommendations from social circles and advance notice of new products — and often spend more, according to *Deloitte's Holiday Mood Survey*.[6] Consequently this data proliferation requires the consumer to be vigilant about monitoring who, how and why their information is being accessed. For retailers, loyalties can be won or lost based on how well they protect this sensitive data as well as how efficiently they use it.

As the digital revolution unfolds, retailers have hardly been asleep at the wheel. They have responded by embracing a range of technologies that allows them to transform the shopping experience and connect with customers in new and often highly personal ways.

There are certain "table stakes" for succeeding as a retailer in a digitally driven world. Since the early to mid-1990s, when retailer websites were little more than glorified online catalogs, most companies have not only developed sophisticated sites with e-commerce capabilities, they have also set up Facebook pages to connect with customers, and often offer mobile apps that provide a range of services. But many retailers have gone considerably beyond these "must-have" tools, to embrace more creative and future-leaning technologies. Such technologies can help drive consumers back to brick-and-motor stores by putting a new spin on the shopping experience. These are technologies that leading retailers are using now.

For example: One big box retailer has developed an app that gives consumers personalized offers based on past purchases. Mobile bar codes promote items and allow consumers to purchase them in-store using a mobile device. Shoppers at an office supplies store can "check in" using a mobile app that then issues special in-store coupons.

In short, digital technology has unleashed a wave of innovation that continues to flourish in the retail space. Yet as each new initiative hits the market, consumers are clamoring for the next great thing, pushing companies to experiment and roll out more conveniences, more customized experiences, and more ways to interact with their brands. The road to digital leadership can certainly garner happy customers, but it can also become a slippery slope. Because the digital arena is so new, it is also relatively untested. Not every concept succeeds, and most retailers can point to ideas that have gone up in flames or died on the vine. Initiatives often backfire because companies fail to consider each of the risks involved. As retailers try to incubate new solutions, business models, etc., it is essential they understand how to execute these initiatives without an overbearing risk and security infrastructure that might stifle innovation.

[6] Deloitte Holiday Mood Survey, 2012.

Amid the rush of excitement that can accompany the launch of a new digital initiative, it's not uncommon for companies to assign risk management a seat at the very back of the bus.

The phishing and fishing line — Digital risk pitfalls

The changing retail landscape is introducing digital risks that are both unprecedented and revolutionary in nature. These are not risks that operate on the sidelines: they impact the very heart of a company's business—its strategy, brand reputation, and the loyalty of its customers. There are myriad cautionary tales of the damage that can be caused when these risks come home to roost.

Emerging customer experiences bring new digital risks

Customer loyalty and digital rewards can be instrumental in promoting customer loyalty and retention.

Vibrant digital displays and creative use of quick response (QR) marketing codes produce an interactive shopping experience.

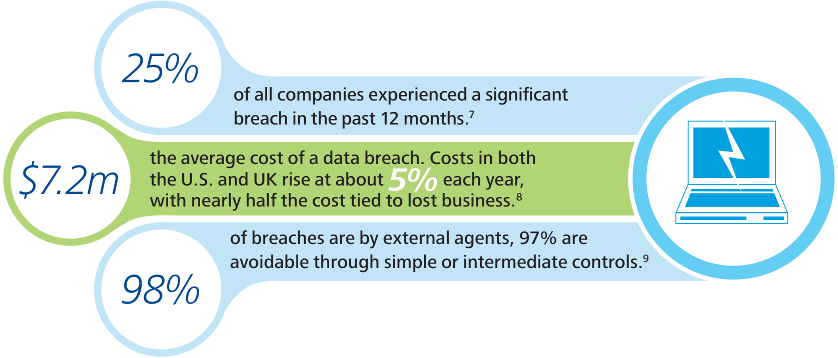
Mobile payments solutions allow customers to pay for merchandise using their smart phones and other mobile devices, reduce costs, and accelerate the checkout process.

Shoppable media provide special deals for customers willing to make an immediate purchase of products using various technologies such as videos or electronic ads.

Geofencing / IP recognition and location-based services allow retailers to use personal data their customers share with them to send targeted deals and advertisements to phones when consumers walk into a predefined virtual space inside or near stores.

Intelligent video monitoring allows retailers to capture consumer demographics and shopping behavior so that the retailer can make adjustments to their offerings and services.

Take for example, a recent case of cyber theft at a large supermarket chain. The company's payment system was compromised, but the breach was not discovered until three months later, after customers began reporting fraudulent claims on their credit cards. During those three months, the numbers and expiration dates for more than two million credit and debit cards had been exposed to hackers. While the problem was corrected within days of its discovery, the company was forced to divert considerable resources to damage control. Despite its efforts, the chain faced several class action lawsuits charging lax security and failure to inform its customers of the breach in a timely manner, as well as incalculable damage to its brand.



25% of all companies experienced a significant breach in the past 12 months.[7]

$7.2m the average cost of a data breach. Costs in both the U.S. and UK rise at about 5% each year, with nearly half the cost tied to lost business.[8]

98% of breaches are by external agents, 97% are avoidable through simple or intermediate controls.[9]

The recent 'Dexter' point of sale ("POS") malware attack is another example of the increasing risks within the stores (e.g., POS self-checkout attacks). However, not all digital disasters are attributable to data breaches. The rise in social media presents numerous opportunities for companies to create campaigns that miscarry. Witness the fast food chain that invited customers to share what were meant to be warm and fuzzy stories at a specially created social media site, only to experience a barrage of vitriol that forced it to pull it down. Or the company that announced a limited-time offer for free downloads via its mobile apps and web store: the move resulted in such an enthusiastic response that it brought down the company's servers, leading to angry fans and much criticism on various social media sites for poor planning.

Companies also find themselves at risk when they fail to maintain pace with new and emerging technologies. Perhaps there is no better example than a large online retailer's price checker app, which allows consumers to scan barcodes in actual stores and compare prices with those offered on the company's site. The app has forced retailers to pay particular attention to how they price items in their stores. And it has certainly led to some lost sales. The online retailer, still not subject to collecting local sales tax from customers and oftentimes offering free or nominally priced subscription-based flat shipping charge, can continue to offer lower prices than brick-and-mortar sellers on many items.

[7] "Navigate the Future of the Security Organization," Forrester, February 2012.

[8] "Cost of a Data Breach," Ponemon Institute, 2011.

[9] "Data Breach Investigations Report," Verizon, 2011.

Digital risk can surface in the external environment as well as within the confines of the organization, making it imperative for executives and managers to adopt both "outside-in" and "inside-out" views of the company's strategy and risk profile. Understanding where risks are coming from can help companies identify what is under their control, so they can manage it, and what is outside of their control, so they can monitor, plan for, and mitigate it.

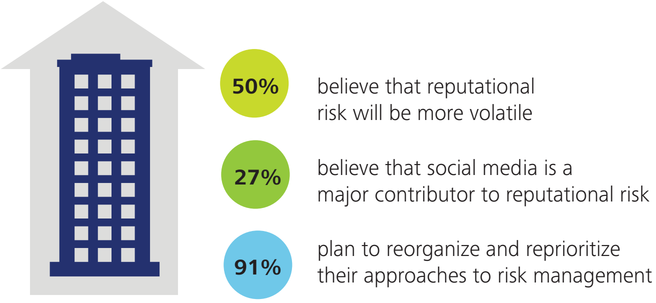
To get a handle on the risks that can surface as a company pursues its business objectives, it is helpful to categorize them into various risk types. These broad risk types are not specific to the digital world, but digital activities will give rise to different risks within each category. Quite often, a particular activity will generate risks in multiple categories. The primary digital forces shaping the retail industry — social media, omni-channel shopping, and emerging retail technologies — have implications for each of these major risk types.

The depth of the sea — A retailer's view of risk

Retail executives clearly appreciate the significance of the digital forces at play in their industry and, like many other executives, are beginning to turn their attention to the inherent risks these forces present. Indeed, in a recent survey conducted by Deloitte and *Forbes Insights*,[9] when executives were asked what risk sources would be most important over the next three years, more than a quarter (27 percent) identified social media. It was the fourth-most frequently identified risk source,[10] coming after such stalwarts as global economic environment, regulatory changes, and government spending.

The volatility that has characterized the business landscape in recent years has placed risk management at the top of the executive agenda. When it comes to digital risk in general, most retail executives view its management both narrowly and incompletely, relegating "ownership" of different types of risk to the departments that seem the most logical fit or allowing individual business units to create their own risk management plans. The problem with such an approach is that it ignores the interconnectedness of digital risks, creates process and resource inefficiencies, potentially allows certain risks to slip through the cracks, and serves to strengthen the law of unintended consequences. Regulatory compliance issues can also arise when different groups fail to adequately communicate their risk management policies to others that may be affected by them.

Figure 3. Risk sources of greatest importance over the next three years



Source: "Afterschock: Adjusting to the new world of risk management," www.deloitte.com/us/afterschock

It is also important to recognize that risk management is not just about protecting the organization or even mitigating risk. It's an approach to value creation: value is rarely created without taking on some level of risk, and this is especially true in a space as new and relatively untested as digital. Redundancies and lack of formalized risk management processes can create obstacles to the intelligent risk-taking required to outpace the competition.

To understand and leverage this risk-reward balance — and to develop strategies that protect and create value for their organizations — retail leaders should be able to "see around the corner" and anticipate both emerging risks and digital disruptors.

Connecting the anchors — Getting digital risk management right

An effective approach to digital risk management comprises an ongoing "sense and respond" process that crosses silos and touches any stakeholders. The building blocks for such an approach are not radically new, but together they add up to an end-to-end lifecycle process that can help organizations achieve maximum protection with the greatest competitive benefits. There are four key phases of the digital risk management lifecycle, as outlined in figure 4.

Laying the foundation for a solid digital risk management process requires a firm grasp of the company's current state, including its digital footprint, what digital risks might be strategic game changers today, where additional risks might arise tomorrow, and the organization's existing risk management capabilities.

[9] "Aftershock: Adjusting to the new world of risk management," Deloitte and *Forbes Insights*, 2012.

[10] Consumer and industrial products executives actually put social media in second place as a risk source, after the global economic environment.

Weaving your net — Defining the digital footprint and evaluating risks

Every company maintains multiple digital assets, across a different set of digital channels. Some of these are directly owned by the organization, and therefore controlled by it, and others are outside the organization's direct control. Together these assets make up the company's "digital footprint":

- **Owned/controlled digital assets:** Examples include e-commerce web sites, mobile apps, information technology infrastructure, data, corporate/employee-owned smartphones, etc.
- **Non-controlled digital assets:** Examples include how people use your brands and digital assets, what people say about your organization in the digital space (posting opinions; media coverage; regulators' perception), or what they say about your digital assets.

Knowing what belongs to the organization, and what it is responsible for, is fundamental to understanding a company's digital risk. Even when assets are outside the organization's direct control, they are often affected by its activities. For instance, when a retailer receives a customer complaint, the way it handles that complaint could well find its way into a number of digital venues in the form of either an angry rant or effusive praise. It is therefore important to understand the nature of these uncontrolled digital assets and how they can affect the company's overall risk profile.

Identifying digital assets is only one aspect of understanding an organization's digital footprint. It is also essential to ask which internal stakeholders control which digital assets. This is one way to surface the enormous duplication that exists in many retail organizations when it comes to digital initiatives. In the world of digital, things are evolving so fast that many initiatives are "bottom up," hatched within specific business units or functional areas that don't always see across the entire organization. The digital development landscape is the Wild West, with small development teams pushing new digital programs to market — oftentimes done by breaking the rules — which is behavior that is rewarded and celebrated. Retailers are loath to squash this type of innovation; rather, they wish to enable it by having specific processes that allow the business to respond quickly to risk.

Figure 4. The digital risk management lifecycle

Identify	Develop	Implement	Monitor
Frame and benchmark the current risk management strategy and inventory the supporting policies, process, controls, and metrics, especially as they apply to digital.	Create a digital governance structure and risk mitigation and response plans. Create policies and procedures that are relevant to the new digital age and put in place supporting risk management processes.	Roll out the integrated risk management program — including assurance programs, frameworks, and activities- to business units and enabling areas (i.e., Internal Audit, IT, Marketing, HR, etc.).	Execute business and digital risk management strategy: test risk process/controls, including escalation and response scenario testing; and implement reporting and performance management.
Digital risk management strategy	Digital governance structure	Integrated approach to strategy and risk management	Risk management oversight
Risk management policies, processes, controls	Risk management policies, processes, controls	Integrated risk management within key business activities	Business and risk management strategy execution
Risk scenarios, measurement, vulnerability	Risk mitigation and response plans	Enhanced risk management infrastructure	Risk processes/ controls escalation and response
Capability maturity	Technology infrastructure to manage risks	Assurance program, frameworks, and activities	Board and executive management performance

One way an organization can get its arms around defining the digital risk environment is to look at its major digital initiatives and the technologies it is employing and then identify what risks might arise with respect to those initiatives in each of the major risk categories (strategic, financial, operational, IT, and regulatory and compliance). Take, for example, a campaign that cuts across various social media platforms and that allows customers to purchase and receive a particular product in the manner they would like. The company may encounter operational risks as part of the fulfillment process, which involves engaging with the third-party shipper to determine what can be shipped where and confirming that shipping costs are pre-calculated. If the campaign specifies that customers who recommend the product can receive a discount or gift card on a future purchase, the company should consider various financial risks (for carrying the liability) as well as regulatory risks (for confirming the right language is included in the offer/ redemption). Overall response to the campaign involves a strategic risk: If the campaign is well-received it enhances the brand. But if the response is negative, it could have an adverse impact. If the company is able to document and anticipate these risks, it can develop standardized procedures for mitigating them.

Evaluate digital risk readiness by asking questions based on these dimensions

Ownership: Do you know what digital activity you own and how others use your brand online?

Alignment: Is your digital activity aligned with your business objectives?

Operations: Have you set the rules of engagement with digital through appropriate policies and procedures?

Assurance: Do you regularly monitor the performance and compliance aspects of your digital footprint?

Tightening the holes — Developing a framework and understanding risk management capabilities

Because digital risks are still relatively new and unfamiliar to retailers, leaders may find it useful to establish a framework that presents a big-picture view of the risk landscape. A digital risk framework can also help executives understand what capabilities they need to have in place to manage digital risk and what areas they need to focus on when they think of building those capabilities. The framework should organize risk management activities based on the core components of a comprehensive risk management program. It is a starting point for evaluating the organization's ability to sense and respond to digital risk. Effective management of digital risk calls for capabilities in a number of areas, some of which are familiar as part of traditional risk management, and others that are relatively new organizational skills.

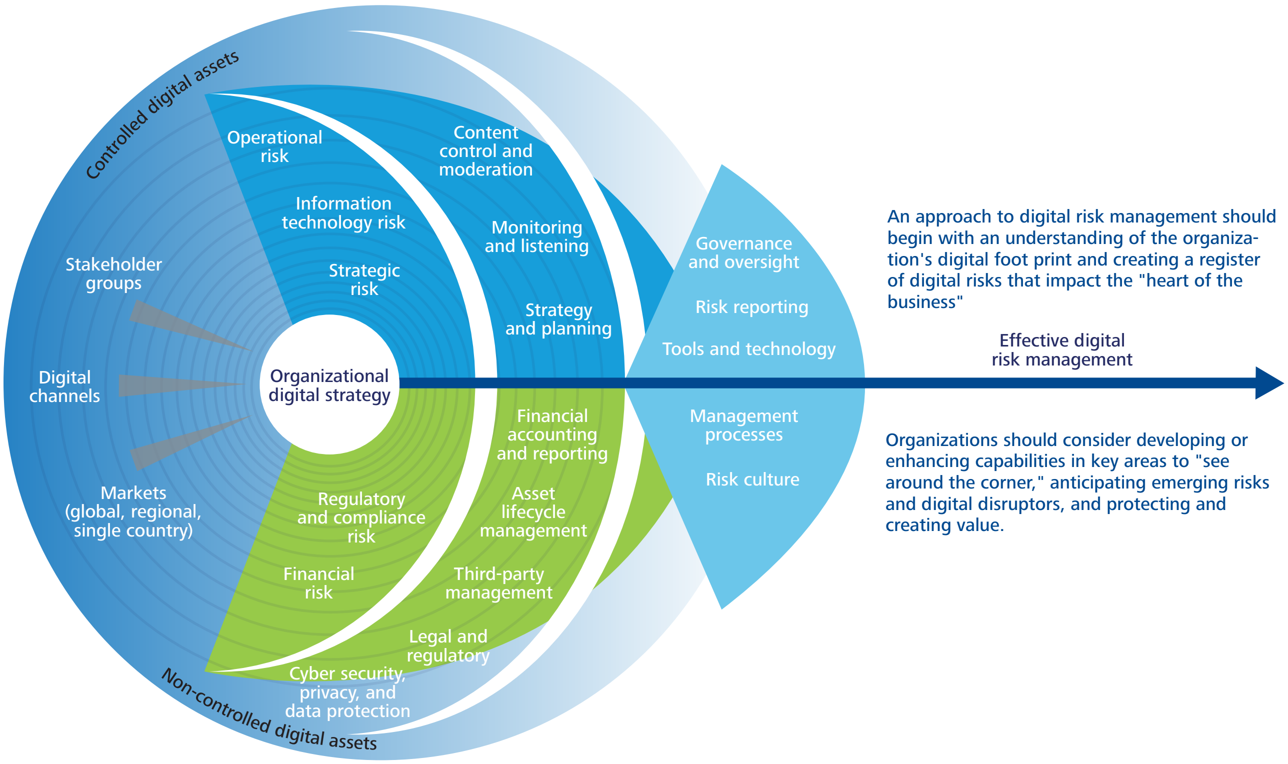
Conducting a formal assessment of the company's digital risk management capabilities can help pinpoint deficiencies so that corrective action can be taken. In some cases management may also discover there are overlapping or redundant capabilities that can be consolidated or reassigned. It may be helpful to use a set of probing questions as a starting point for evaluating the company's digital risk readiness.

Digital risk management is the product of multiple layers of risk defense, each linked via a cascading set of roles and responsibilities. However, setting the vision and assigning and coordinating these lines of defense is the responsibility of senior leaders. It is also up to leadership to establish a culture that values the importance of digital risk management.

Because the business units are closest to the customer, they are almost always the first line of defense in digital risk situations. Working hand-in-hand with IT, they should incorporate risk-informed decision-making into their day-to-day operations. They should also seek to determine the level of risk they are willing to accept so they can take steps to mitigate risks as appropriate and then escalate issues when a risk extends outside their zone of tolerance.

The second line of defense lies in the risk management function itself, which provides oversight and consultation to the business and establishes checks and balances and enterprise-level policies and standards.

The third line of defense is the audit function. Audit is responsible for independently verifying the effectiveness of the digital risk management process and for providing assurance to management and the board of directors that this process is working properly.


Controlled digital assets
Operational risk
Information technology risk
Strategic risk
Content control and moderation
Monitoring and listening
Strategy and planning
Stakeholder groups
Digital channels
Markets (global, regional, single country)
Organizational digital strategy
Regulatory and compliance risk
Financial risk
Financial accounting and reporting
Asset lifecycle management
Third-party management
Legal and regulatory
Cyber security, privacy, and data protection
Non-controlled digital assets
Governance and oversight
Risk reporting
Tools and technology
Management processes
Risk culture
Effective digital risk management

An approach to digital risk management should begin with an understanding of the organization's digital foot print and creating a register of digital risks that impact the "heart of the business"

Organizations should consider developing or enhancing capabilities in key areas to "see around the corner," anticipating emerging risks and digital disruptors, and protecting and creating value.

It is important to recognize that if internal audit is consistently the first to identify and flag digital risks, that may be a signal that the first two lines of defense are not operating properly or that there are new risks that haven't yet been addressed in the digital risk program. What's more, if an organization relies on internal audit as the first line of defense, it may find itself in the position of continual damage control and never addressing the underlying cause.

Groups within the organization should understand their role in managing digital risks and how they should work together. Most importantly, the lines of defense should be working in tandem and continuously learning from one another. Senior leadership should have a clear understanding of where the risks lie, as well as how, and by who, those risks are being addressed. Then when opportunities arise, they can be leveraged for competitive advantage.

Charting the course — Realizing digital opportunities

As digital elbows its way into the center of the shopping experience, retailers will need to stay one step ahead in order to deliver on their customers' ever-escalating demands and sidestep unforeseen risks that may crop up along the way. A solid risk management framework drags potential risks out into the open so that organizations can develop controls and repeatable processes and streamline their risk responses.

The benefits of such an approach are significant. It creates efficiencies because systems and resource redundancies are eliminated. When there is a single set of policies and standards — rather than one per department, business unit, or even campaign — the company does not need to waste time resolving different approaches, or even worse, developing ad hoc responses to risk events. Some key actions for retail executives include:

- Frame and benchmark the current risk management strategy and inventory the supporting policies, processes, controls and metrics, especially as they apply to digital.
- Create a digital governance structure and risk mitigation and response plans. Create policies and procedures that are relevant to the new digital age and put in place supporting risk management processes.
- Roll out the integrated risk management program — including assurance programs, frameworks, and activities — to business units and enabling areas, such Internal Audit and IT.
- Execute business and digital risk management strategy; test risk process and controls, including escalation and response scenario testing; and implement reporting and performance management.

When companies establish organization-wide, well-coordinated risk management processes, they can be more secure, vigilant, and resilient.

A detailed risk framework enables leadership to consider the level of risk it is willing to take on in the pursuit of innovation and potentially lucrative new ideas. When risk management coordination is effective, the result is a seamless interplay of sense-and-respond activities that free up the organization to focus on the significant opportunities presented by the unfolding digital landscape.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.