



**The future of risk**  
New game, new rules

The risk landscape is changing fast. Every day's headlines bring new reminders that the future is on its way, and sometimes it feels like new risks and response strategies are around every corner. The outlines of new opportunities and new challenges for risk leaders—indeed, all organizational leaders—are already visible.

***So what should leaders prepare for? This report profiles 10 trends that have the potential to significantly alter the risk landscape for companies around the world and change how they respond to and manage risk.***

What you'll see is that risk's onset and consequences, and the entire nature of the risk discipline, are evolving. The good news? The strategic conversation around risk is changing too. For leaders today, risk can be used as a tool to create value and achieve higher levels of performance. It's no longer something to only fear, minimize, and avoid.

Explore the drivers, opportunities, threats, and real-world examples for each trend. And ask yourself: will your organization be able to harness these trends to be even stronger, more resilient?

**Contact us** to discuss how you can better prepare for what's ahead. We can help you identify ways for your organization to manage risk, create value, and ultimately power your performance.

How are organizations' responses to risk changing?



**1 | Cognitive technologies augment human decision-making**

Driven by developments in artificial intelligence (AI) and easy access to huge amounts of data, smart systems will assist, and at times even replace, human-led risk management.



**2 | Controls become pervasive**

In a sensor-enabled, hyper-connected environment, organizations will deploy pervasive controls as part of their products, services, and business models to monitor and manage risk in real time.



**3 | Behavioral science informs risk insights**

Advances in behavioral sciences will fuel efforts to understand risk perceptions, influence risk behaviors, and improve risk-related decision-making.



**4 | Vigilance and resilience complement prevention as leading practices**

Organizations are realizing that 100 percent risk prevention is not feasible, so investment in vigilance (detecting risk events as they happen) and resilience (containing and reducing the impact of risk events) will increase.



**5 | Risk transfer broadens in scope and application**

Risk transfer instruments, such as insurance, contracts, and novel financial instruments, will increasingly be used by organizations to protect them from a wider range of risks – cyberattacks, climate change, geopolitical risks, terrorism, business disruptions, and more.

How are consequences of risk for organizations changing?



**6 | Innovation leads, regulation follows**

The marketplace will reward organizations that take on strategic, high-risk innovations—even if they fall outside the scope of existing regulations.



**7 | Risk becomes a performance enabler**

As risks become more measurable and tangible, organizations will be better able to determine an accurate upside value for risk—and encourage an appropriate level of risk-taking.

How is the onslaught of risk changing?



**8 | The networked economy demands collective risk management**

As businesses engage more deeply with a large number of external stakeholders, including “crowds,” they will rely more heavily on them to identify, manage, and reduce risks together.



**9 | Disruption dominates the executive agenda**

The constant threat of disruption resulting from emerging technologies, business model transformations, and ecosystem changes will force executives to make significant strategic choices to drive organizational success.







**10 | Reputation risks accelerate and amplify**

To survive in a hyper-connected world dominated by mobile devices, social media, and evolving expectations from society, leaders will proactively address accelerated, amplified risks to their organizations' reputations.

# Cognitive technologies augment human decision-making

Advancements in cognitive technologies, artificial intelligence, and data analytics are helping organizations go beyond traditional ways of managing risks by using smart machines to detect, predict, and prevent risks in high-risk situations. Autonomic computing combines automation and cognitive technologies to make systems self-managing—and potentially self-defending and self-healing against risks.

## What forces are driving this trend?

-  Massive growth in the volume of data available to organizations
-  Emergence of new and advanced AI-based algorithms
-  Expanding pool of data science talent
-  Adoption of behavioral analytics\* in risk management

\* Behavioral analytics is the tracking, collection, and assessment of user data and activities using monitoring systems to understand interactions and dynamics between different elements.

## What are the opportunities?

- Identify use cases that are well-suited for cognitive technology solutions: Where the risk area is critical, large amounts of data are available, and current solutions aren't effective
- Use visualization to analyze and communicate information in a human-friendly way to enable rational decision-making
- Upskill employees so that they are able to more effectively use cognitive technologies to extract insights from data

## What are potential threats and pitfalls?

- Difficulty in implementing complex cognitive tools
- Overhyped technologies unable to deliver on promises
- Lack of trust and assurance mechanisms for AI
- Inability to source the right data
- Human backlash against automated decision-making
- Unintended consequences of mistaken predictions

## Where is this trend already in play?

Warwick Analytics' early warning and prevention system looks hours, days, and months ahead to try to predict when and how products in the field (such as aircraft and vehicles) will require maintenance. Identifying the root causes of failure helps engineers take corrective action, such as remanufacturing and redesigning products. Economic benefits can include enhanced efficiency of plant or production line, reduced energy bills, and increased product life cycle.<sup>1</sup>

Hong Kong-based venture capital firm Deep Knowledge Ventures has appointed a software algorithm, "VITAL," to its Board of Directors. Just like other members of the board, VITAL gets to vote on whether the firm should make an investment in a specific company or not. It makes its decisions by scanning prospective companies' financing, clinical trials, intellectual property, and previous funding rounds.<sup>2</sup>







Nexgate is a provider of Deep Social Linguistic Analysis (DSL) technology and natural language processing (NLP) based social media risk management tools. Its major solutions scan social networks to try to discover and track an organization's accounts; detect fraudulent social media accounts, unauthorized changes, and anomalous behavior on social account profiles; reduce potential liability from inadvertent posting of sensitive data; and demonstrate compliance with more than 35 standards and industry regulations.<sup>3</sup>



# Controls become pervasive

Smart devices (also known as the Internet of Things) equipped with a variety of sensors, communications, and computing capabilities serve as risk monitoring and enforcement points. This presents an opportunity for organizations to detect risk events, derive crucial risk insights, and even take immediate actions in the environment. The result? Real-time, pervasive, dynamic risk management.

## What forces are driving this trend?

-  Declining cost, decreasing size, and increasing connectivity of sensors
-  Increasing investments in the Internet of Things
-  Growing adoption of workplace wearables
-  Advancements in sensor technology
-  Advancements in analytics
-  Businesses operating as networked ecosystems

## What are the opportunities?

- Enhance operations and improve risk-related decision-making by integrating pervasive risk controls in areas such as internal audit, supply chain management, finance, cybersecurity, and controls testing
- Reduce cyber security and fraud risk by using sensor-enabled devices to implement context-aware identity access capabilities
- Improve traceability across the supply chain, especially in security-sensitive industries such as food production and pharmaceuticals
- Automate compliance monitoring and reporting by embedding risk controls into business technologies
- Manage risks introduced by customers by analyzing customer behavior through real-time data feeds

## What are potential threats and pitfalls?

- Heightened exposure to cyber risks as business processes rely more heavily on the Internet of Things
- Greater availability of data revealing risks in areas that were formerly considered safe, resulting in new obligations to manage those risks or increased liability
- Rising privacy concerns from employees, customers, and business partners because of pervasive monitoring
- Increased difficulty of filtering relevant information from the noise, given the vast amount of data generated

## Where is this trend already in play?

Saia, a US-based freight company, has worked with Intel to deploy sensors into its truck fleet to track maintenance needs, driver safety, fuel usage, and other metrics in real time. Through real-time process intelligence, this initiative has led to a 6 percent increase in fuel efficiency, which translated to \$15 million in savings for Saia. In addition to achieving cost savings, Saia has been able to track maintenance needs, driver safety, and fuel usage, as well as other metrics, in real time.<sup>4</sup>

Fujitsu has developed wearable tags that can detect whether users have changed location or posture, have fallen down, or are experiencing high heat. With the help of these tags, employers can—in real time—monitor employees' working conditions or detect if they are carrying a heavy load or standing in a place where they might fall. The aim is to reduce the risks of injury at the workplace.<sup>5</sup>

Singapore-based TrustSphere, whose clients include financial services firms, specializes in trying to uncover the relationships that an employee has through digital interactions—attempting to reduce the risks of illegal collusion and internal fraud.<sup>6</sup>

# Behavioral science informs risk insights

Behavioral science is the study of human behavior through systematic research and scientific methods, drawing from psychology, neuroscience, cognitive science, and the social sciences. There is increasing demand for these skills in the business world—including risk organizations. What drives risky behavior? How do cognitive biases lead people to wrongly assess risk? How can risky behaviors be detected and modified? These are the types of questions leading organizations are looking to answer with behavioral science. In fact, some Fortune 500 companies today even have a Chief Behavioral Officer at the C-suite level.

## What forces are driving this trend?



Increasing interdisciplinary research across fields such as cognitive science, psychology, economics, and neuroscience



Renewed interest in making technology products intuitive for usage



Growing popularity of behavioral economics to inform decision-making



Early successes in commercializing gamification

## What are the opportunities?

- “Design interventions” to help executives overcome the influence of cognitive biases in decision-making
- Improved systems for monitoring high-risk individuals in sensitive roles
- More effective risk, forensics, and financial transaction-related business processes

## What are potential threats and pitfalls?

- Risk of regulatory action in case of perceived misuse of behavioral interventions
- Backlash from employees and executives who see behavioral interventions as an impingement of free will
- Slow (or no) return on investments in organizing complex behavioral interventions

## Where is this trend already in play?

Fujitsu has built a platform that uses psychological profiling to ramp up computer security in the workplace. This enterprise tool aims to identify workers who are most vulnerable to cyberattacks and also gives advice on how to sidestep them, based on their behavior while checking and sending emails, and browsing the web. This was developed after consulting social psychology experts and surveying more than 2,000 Japanese users, half of whom had experienced attacks, to determine which traits make some users more vulnerable to viruses, scams, and data leaks.<sup>7</sup>

Mi3 Security (formerly MetaIntell), a cloud-based mobile risk management company, recently brought onboard a behavioral science expert as a technical solutions and business advisor in the office of the CEO.<sup>8</sup>

Hand hygiene company DebMed offers an electronic hand hygiene compliance monitoring system that seeks to measure the compliance level of an entire unit instead of individual performance. It predicts expected hand hygiene opportunities by taking into account unique conditions of each hospital unit, such as census and nurse-to-patient ratio. This aims to promote a spirit of collaboration and accountability while also providing actionable feedback for the group without singling out individuals.<sup>9</sup>



# Vigilance and resilience complement prevention as leading practices

Risk prevention methods can never be foolproof, and increasing investment in preventative approaches often yields only marginal benefit along with unwelcome side effects such as slowing innovation. Organizations are expanding their approaches to focus on vigilance (detecting patterns that may indicate or even predict risk events) and resilience (the capacity to rapidly contain and reduce the impact of risk events) as well. We can expect activities like these to rise in importance: monitoring emerging threats, identifying anomalies in business processes, managing stoppages from third-party vendors, and preparing for risk-related workplace disruptions.

## What forces are driving this trend?

-  Growing recognition of inability to eliminate risks altogether
-  Rapid advancements in data analytics, machine learning, and AI capabilities
-  Greater sharing of information among organizations as a result of the networked economy
-  Rising threat of nation states investing significant resources into disruptive activities
-  Rise in macro risks such as climate change, natural disasters, political unrest, and more

## What are the opportunities?

- Assess and prioritize risks to determine where to invest in vigilance and resilience
- Identify and test cutting-edge, commercially available tools focused on vigilance and resilience

## What are potential threats and pitfalls?

- Inability to detect significant threats due to lack of data, tools, or expertise
- Ineffective resilience efforts due to complex interdependent operating structures or lack of agility

## Where is this trend already in play?

Cytora aims to provide real-time structured data on supply chain, operational, and geographic disruptions across multiple categories of risk, including factory fires and explosions, labor strikes, terrorism incidents, industrial accidents, and natural disasters for supply chain risk and corporate risk management. Alerts received within five minutes of an event breaking online seek to give organizations the opportunity to try to mitigate risks early and keep costs low.<sup>10</sup>

Verafin focuses on providing solutions in the fraud detection and anti-money laundering space based on AI-enabled algorithms and a more holistic view of banking transactions with diverse data points. Its latest product strives to enable cross-institutional analysis to detect suspicious activity across multiple institutions.<sup>11</sup>

Zeean, an open source project, taps the crowd to map the flow of materials across the world. Using this database, Zeean then attempts to help organizations analyze the economic impact of isolated events (for example, climatic catastrophes) on global supply chains through powerful visualizations, working to help organizations and governments achieve supply chain resilience in a cost-effective manner.<sup>12</sup>

# Risk transfer broadens in scope and application

Risk transfer instruments such as insurance and contracts aren't new, but expect them to play a bigger role in the face of "mega-impact" risk events like climate change, political unrest, terrorism, and cyberattacks. In the past, few considered hedging against such risks. Soon, it may become commonplace as commercial third-party insurance, risk-sharing agreements, captive in-house insurance, and other tools continue their ascent. Financial industry innovation is also generating novel financial instruments that transfer and monetize risk.

## What forces are driving this trend?



Growing instances of "mega-impact" events such as cyberattacks, political unrest, and climate change—and their growing financial and reputational impact



Increasing globalization and the rise of a networked economy leading to cascading risks



Persistent inability of organizations to completely eliminate risks through preventive controls



Rising cost pressure on organizations to look for cost-effective ways to transfer risks

## What are the opportunities?

- Evaluate risk transfer instruments as an option to achieve business continuity and more predictable performance
- Establish risk-sensing mechanisms to identify emerging risks and determine if instruments could be used effectively to transfer key risks
- Develop clear and stringent risk-sharing clauses in all partner contracts, and consider collective insurance with partners to address shared risks

## What are potential threats and pitfalls?

- Potential for conflict, litigation, and disputes with customers, partners, and suppliers over risk-sharing agreements
- Inability to determine the appropriate insurance premium for various risks
- Becoming "over-insured" or purchasing insurance in noncritical areas

## Where is this trend already in play?

Some of the largest medical device manufacturers like Boston Scientific, Medtronic, and St. Jude Medical are negotiating experimental deals with hospitals to take on performance-based financial risk for their implants. Such risk-sharing agreements are structured in a variety of ways. Some agreements may stipulate that the manufacturer return a percentage of the device's price if it does not meet certain performance goals or fails within a set period of time. Under other agreements, a hospital pays more for a device that fulfills a manufacturer's quality and economic claims.<sup>13</sup>

Willis SECURENET aims to assist organizations facing terrorism risks, and those that are penalized by exorbitant rates of terrorism insurance, with the development of captive insurance entities. It can help them in every stage of captive formation, including feasibility analysis, domicile selection, development of underwriting parameters, and maintaining communication with state insurance departments.<sup>14</sup>

BitSight Security Ratings seeks to provide objective, data-driven, daily ratings of an organization's security performance through continuous monitoring. It works to help insurers look at historical data, compare an organization against industry peers, and make informed underwriting decisions. It also helps identify and alert applicants of potential threats in their networks. This aims to enable insurers to get insight into past and current cybersecurity risk levels.<sup>15</sup>





# Innovation leads, regulation follows

As the pace of innovation quickens across diverse industry sectors, it is becoming more difficult for regulations to keep up. Meanwhile, many businesses and other organizations are taking on high-risk innovations as a strategy—even when they fall outside the scope of existing regulations—and reaping the rewards. Increasingly, the rapid pace of innovation is driving the regulatory agenda.

## What forces are driving this trend?

-  Rapid pace of proliferation of innovations
-  Growing adoption of new business models, such as sharing-based, freemium, and subscription-based, leading to increased diversity of competitors
-  Industry convergence and blurring of market boundaries
-  Deliberate restraint on the part of regulators in order to allow innovations to gain steam
-  Growing consumer activism and empowerment

## What are the opportunities?

- Reduce regulatory risks by educating regulators and harnessing customer and public support
- Work with the industry ecosystem to establish self-regulatory frameworks
- Clarify the organization's risk appetite when evaluating projects that lie outside the realm of current regulations

## What are potential threats and pitfalls?

- Losses due to investments in projects that operate in legal gray areas that subsequently become prohibited
- Fast-moving disruptive organizations can rapidly gain market share from incumbents before regulations are even put in place
- Negative publicity from lobbying efforts against disruptive startups

## Where is this trend already in play?

Companies such as Google are investing in building autonomous cars ahead of a regulatory framework, driving regulators to strategically balance their priorities around promoting innovation and ensuring public safety.<sup>16</sup>

Sharing economy-based businesses, such as Airbnb and Uber, are growing rapidly by breaking away from traditional industry norms and established assumptions built into regulations.<sup>17</sup>

Telemedicine, provided by companies such as Teladoc, enables doctors to offer primary care services over videoconference. While telemedicine has been heralded as a way to increase health care access, it has required the renegotiation of relationships between insurers, physicians, and regulators, with many states not allowing reimbursements for video visits despite a shortage of doctors.<sup>18</sup>

# Risk becomes a performance enabler

In the past, risk management was often an exercise in fear and avoidance, with organizations focused primarily on completing necessary, compliance-driven activities. But that's changing. Many leaders are now viewing risks in terms of their potential to drive performance and value. As risks become more measurable and tangible, organizations will be better able to determine an accurate upside value for risk—and encourage a desired level of risk-taking behavior in a bid to balance risks and rewards.

## What forces are driving this trend?



Focus on innovation and experimentation is creating a culture in which failure is being viewed as a necessary step to success rather than something to be avoided at all costs



Analytics capabilities are helping leaders link risk to performance



New workplace technologies such as wearables, image recognition, and AI are improving risk sensing and monitoring capabilities



Disruptive new business models are driving the need for increased risk-taking



Decentralization is creating flat organizations where employees are empowered and rewarded for taking on risks themselves

## What are the opportunities?

- Use risk dashboards, visualizations, and scenario analysis to empower leaders with data to make risk-informed decisions
- Recognize and reward intelligent risk-taking
- Foster a risk-intelligent culture and empower employees at every level to take on informed risks

## What are potential threats and pitfalls?

- Exposure to risks beyond desired risk appetite
- Potential reputation damage and regulatory actions as a result of taking on excessive risk
- Inability to correlate performance with risk due to lack of appropriate tools

## Where is this trend already in play?

Adobe's Kickbox Innovation Workshop encourages innovation and risk-taking by providing the participating employees with seed money (\$1,000 prepaid credit card), a step-by-step startup guide, and a 45-day period to experiment with and validate new ideas.<sup>19</sup>

Chief Financial Officers are using risk dashboards for driving strategic decision-making, such as weighing M&A possibilities, developing new product lines, planning market entry strategy, and deciding on capital allocation.<sup>20</sup>

Advertising agency Grey gives out the Heroic Failure Award that honors new, unproven ideas that were failures in the market, thus rewarding and encouraging risk-taking among employees.<sup>21</sup>



# The networked economy demands collective risk management

Businesses and other organizations are more connected to one another, and “crowds,” than ever before. They share data, technology, and much more. As a result, they also share more risks. Increasingly, they are managing risk in a manner that reflects this new reality—transforming their risk processes through more open, collaborative approaches that rise to the challenges of a networked economy and working to identify, manage, and reduce risk together.

## What forces are driving this trend?



Businesses operating as networked ecosystems are leading to more dependence on external stakeholders



Crowd-driven and sharing-based initiatives are gaining more acceptance among stakeholders such as customers, employees, business partners, vendors, and suppliers—leading to new collaborative business models



Governments and organizations alike are moving toward radical transparency



The increasingly ratings-driven culture means that sellers, customers, and products are all reviewed with increasing frequency—supplying businesses with data for risk analysis



Globally distributed business models leave brands more vulnerable to physical and virtual risks around the world

## What are the opportunities?

- Use collaborative practices like gamified crowdsourcing to reduce the cost of risk management and improve its effectiveness
- Form alliances with risk experts, researchers, and academia to stay abreast of the latest threats and mitigation approaches
- Adopt an ecosystem-led approach for risk management by forming industrywide partnerships and consortiums

## What are potential threats and pitfalls?

- Potential for incurring legal costs, regulatory action, and reputation damage if sensitive information is leaked through partners or data-sharing portals
- Results may be manipulated if bad actors deliberately feed inaccurate data to skew the models

## Where is this trend already in play?

United Airlines is seeking to harness the power of the crowd to improve security of its software through a “bug bounty” program that will award miles to people for finding vulnerabilities. With this program, the company is following the steps of technology corporations like Google, Facebook, and Microsoft, which have their own bug bounty programs. These programs engage independent researchers, experts, and hackers to find potentially dangerous security flaws for a reward.<sup>22</sup>

ThreatExchange, a social data exchange platform by Facebook, is being used by security professionals and researchers across the world to share cyber threat information.<sup>23</sup>

Wikistrat, the crowdsourced consulting organization, uses interactive role-playing games that leverage a crowd of experts from all over the world for strategic forecasting. Wikistrat’s open source platform provides access to vetted crowdsourced expertise to address complex client issues and risks and to develop effective action plans.<sup>24</sup>

# Disruption dominates the executive agenda

Business leaders are increasingly focusing on risks that threaten to disrupt the fundamental assumptions of their organization's strategies. Prioritizing such risks has become increasingly crucial—these risks cannot be handled in typical organizational silos, and they can destroy sources of value creation for the business. Yet, they also have the potential to form the basis of game-changing moves for an organization, if handled well. Disruptions in the forms of emerging technologies, business model transformations, and ecosystem changes will force executives to make significant strategic choices to drive organizational success.

## What forces are driving this trend?



Globally distributed business models are increasing dependencies on stakeholders across geographies, making brands more vulnerable to geopolitical risks



Growing connections between businesses are expanding the sources of potential disruption



Advancements in social, mobile, analytics, and cloud-enabled emerging technologies are creating opportunities for startups to disrupt incumbents



Traditional industries are converging to create new markets



Business model innovation (such as sharing-based, freemium, and subscription-based) is driving organizations to constantly reinvent themselves



Customers are increasingly expecting more personalized products and services

## What are the opportunities?

- Continuously monitor the changes in the environment to determine which could be truly disruptive
- Revisit the approach to corporate strategy development to introduce more agility, adaptability, and responsiveness to emerging threats
- Identify organizational blind spots, built-in institutional challenges, and personal biases of senior management that can get in the way of action
- Employ tools and techniques such as real-time monitoring, scenario planning, stress testing, war-gaming, and simulations to drive higher levels of sophistication in managing risk

## What are potential threats and pitfalls?

- New startups and cross-industry players can catch organizations off-guard if they don't have strategic threat monitoring and identification mechanisms in place
- Senior management can become overwhelmed by the sheer volume of complex, real-time data, leading to ambiguity and indecision
- Innovation can be stifled by the organization's core business assumptions or structural limitations

## Where is this trend already in play?

Media companies such as HBO that were under the threat of disruption by online streaming players have now reinvented their strategies by adapting to the fast-changing business environment. They have embraced online streaming and have introduced a host of related offerings, thus posing competition to existing streaming content providers.<sup>25</sup>

3D printing is transforming the health care sector, with many incumbents adopting 3D printing for manufacturing medical implants, dental products, and bio-printed tissues.






To counter the growing threat of car sharing companies like Zipcar, German automaker Daimler has launched its own car sharing service called car2go. Through car2go, Daimler aims to disrupt the disruptors like Zipcar not by copying their business models but by creating its own unique value proposition – a “roving” model in which its cars have no fixed spaces and can be parked anywhere to end a trip.<sup>26</sup>



# Reputation risks accelerate and amplify

In today's hyper-connected world dominated by mobile devices, social media, and evolving expectations from society, information can spread like wildfire. This convergence of mobile and social media is intensifying the impact of reputation risks for organizations and is driving them to fundamentally rethink their approaches to risk management and proactively address these accelerated, amplified risks.

## What forces are driving this trend?

-  Social media is creating a more connected, networked world where information is rapidly amplified
-  Disruptive mobile technologies are ushering in a new era of hyper-availability in which people are always available and connected
-  An upsurge of socially conscious consumers, and growing consumer activism, is putting pressure on businesses to be socially responsible and transparent
-  New multichannel marketing strategies built on social platforms allow for greater interactivity for consumers and less control for brands
-  Globally distributed business models are increasingly dependent on third parties and other stakeholders

## What are the opportunities?

- Develop new capabilities for proactive brand-related crisis management
- Continually scan media sources with technology-enabled intelligence capabilities to monitor reputation risk
- Initiate targeted campaigns and develop an external ambassador program to nurture external brand advocates
- Foster a more risk-intelligent culture with tools, resources, and training opportunities to help employees see the reputation implications of their actions

## What are potential threats and pitfalls?

- Personal online activity of employees can cause reputational damage to the organization
- Organizations may be forced to respond to risk events in haste without fully investigating the situation

## Where is this trend already in play?

A media conglomerate fired its head of communications for an offensive personal social media post—which went viral in a matter of hours—in an effort to prevent further damage to its reputation.

Websites like Ripoff Report and Scambook offer online platforms for consumers to post complaints. Ripoff Report receives more than a million visits a week and generates several million dollars of revenues a year from firms that pay to resolve customer complaints.<sup>27</sup>

Food safety incidents can cause significant reputation loss and revenue impact for food and beverage companies. The impact on a company's reputation is often intensified due to the negative attention received through social media channels. Brands that are not prepared to respond to crisis face further scrutiny for moving too slowly when incidents occur.

## Contact the authors



**Nancy Albinson**  
**Managing Director**  
**Deloitte & Touche LLP**  
nalbinson@deloitte.com  
+1 973 602 4523

Nancy is a managing director at Deloitte & Touche LLP and leads Deloitte Advisory's Innovation Program. She guides the business in establishing innovation strategies, identifying emerging client needs, overseeing a portfolio of strategic investments from validation to commercialization, and building a culture of innovation.



**Andrew Blau**  
**Managing Director**  
**Deloitte & Touche LLP**  
ablau@deloitte.com  
+1 415 932 5416

Andrew Blau is a Deloitte Advisory managing director at Deloitte & Touche LLP. He leads Strategic Risk Solutions, which helps clients spot, assess, and manage critical long-term risks.



**Yang Chu**  
**Senior Manager**  
**Deloitte & Touche LLP**  
yangchu@deloitte.com  
+1 415 783 4060

Yang Chu is a senior manager at Deloitte & Touche LLP. She is a specialist in strategic, financial, operational, technological, and regulatory risk and focuses on exploring emerging trends for opportunities and threats for clients and for Deloitte.

## Contributors

**Meghna Panwar**  
**Manager**  
**Deloitte & Touche LLP**  
mpanwar@deloitte.com

**Priyanka Priyadarshini**  
**Senior Consultant**  
**Deloitte & Touche LLP**  
ppriyadarshini@deloitte.com

**Tanmay Tapase**  
**Senior Consultant**  
**Deloitte & Touche LLP**  
ttapase@deloitte.com

# Footnotes

1. Warwick Analytics, "Industries – Manufacturing," <https://warwickanalytics.com/industry/manufacturing>.
2. Rob Wile, "A venture capital firm just named an algorithm to its board of directors – here's what it actually does," Business Insider, May 13, 2014, <http://www.businessinsider.in/A-Venture-Capital-Firm-Just-Named-An-Algorithm-To-Its-Board-Of-Directors-Heres-What-It-Actually-Does/articleshow/35075291.cms>.
3. Nexgate, "Nexgate – Overview," <http://nexgate.com/solutions/overview/>; "LinkedIn selects Proofpoint's Nexgate division for Certified Compliance Partner Program," Nexgate, January 14, 2015, <http://nexgate.com/blog/page/4/>.
4. Erica E. Philips, "Internet of Things reaches into the trucking business," The Wall Street Journal, April 29, 2015, <http://www.wsj.com/articles/internet-of-things-reaches-into-the-trucking-business-1430342965>; "How IoT is transforming the logistics industry," Mubaloo Innovation Lab, May 15, 2015, <http://innovation.mubaloo.com/news/iot-logistics/>.
5. Tim Hornyak, "Fujitsu pushes wearable IoT tags that detect falls, heat stress," PC World, May 13, 2015, <http://www.pcmag.com/article/2921972/fujitsu-pushes-wearable-iot-tags-that-detect-falls-heat-stress.html>.
6. Vidya Ranganathan, "Banks chase trading cheats with 'fuzzy' surveillance," Reuters, November 18, 2014, <http://www.reuters.com/article/markets-surveillance-idUSL3N0T23N220141118>.
7. Tim Hornyak, "Fujitsu psychology tool profiles users for risk of cyberattacks," Computerworld, January 21, 2015, <http://www.computerworld.com/article/2873638/fujitsu-psychology-tool-profiles-users-for-risk-of-cyberattacks.html>; Mike Wheatley, "Fujitsu uses psychological profiling to defend against cyberattacks," SiliconANGLE, January 26, 2015, <http://siliconangle.com/blog/2015/01/26/fujitsu-uses-psychological-profiling-to-defend-against-cyberattacks/>; "Fighting back against the threat of new cyber-attacks with the power of ICT," Fujitsu Journal, May 29, 2015, <http://journal.jp.fujitsu.com/en/2015/05/29/01/>.
8. "Renowned cyber intelligence and behavioral science expert Dr. Terry Gudaitis joins MetalIntell," Business Wire, May 06, 2014, <http://www.businesswire.com/news/home/20140506005752/en/Renowned-Cyber-Intelligence-Behavioral-Science-Expert-Dr.#VVQqPmqpBc>.
9. Debmed, "About us," <http://debmed.com/about/>.
10. Cytora, "Cytora data products," <http://www.cytora.com/products.html>.
11. Verafin, "Verafin – Home," <http://verafin.com/?nabt=1>.
12. "Zeean, "Zeean – Home," <https://zeean.net/>.
13. Jaime Lee, "Devicemakers explore risk contracts with hospitals," Modern Healthcare, December 06, 2014, <http://www.modernhealthcare.com/article/20141206/MAGAZINE/312069964>.
14. "Using captives for terrorism solutions," Willis SecureNet, April 19, 2011, [http://www.willis.com/documents/publications/Services/Political\\_Risk/48701\\_UsingCaptivesForTerrorismInsurance.pdf](http://www.willis.com/documents/publications/Services/Political_Risk/48701_UsingCaptivesForTerrorismInsurance.pdf).
15. BitSight, "Security ratings for cyber insurance," <https://www.bitsighttech.com/security-ratings-cyber-insurance>.
16. "California isn't ready for driverless cars," Los Angeles Times, December 28, 2014, <http://www.latimes.com/opinion/editorials/la-ed-driverless-cars-20141228-story.html>; Rob Toews, "The federal government must act to ensure that the autonomous vehicle revolution takes place in the U.S.," Tech Crunch, January 17, 2016, <https://techcrunch.com/2016/01/17/the-federal-government-must-act-to-ensure-that-the-autonomous-vehicle-revolution-takes-place-in-the-u-s/>; Quentin Plummer, "Google asks feds to fast track regulations for self-driving cars," Tech Times, March 20, 2016, <http://www.techtimes.com/articles/142482/20160320/google-asks-feds-to-fast-track-regulations-for-self-driving-cars.htm>.
17. Joe Harpaz, "Airbnb disrupts hotel economy, sends regulators scrambling," Forbes, May 07, 2014, <http://www.forbes.com/sites/joeharpaz/2014/05/07/airbnb-disrupts-hotel-economy-sends-regulators-scrumbling/#4c5c71da726d>; Bruce Chew, Don Derosby, Eamonn Kelly, Bill Miracky, "Regulating ecosystems", Deloitte University Press, April 15, 2015, <http://dupress.com/articles/regulatory-framework-business-ecosystems-business-trends/>; Finn Poschmann, "Taxation and regulation in the era of Uber and Airbnb present new hurdles for government," Financial Post, April 01, 2015, <http://business.financialpost.com/fp-comment/taxation-and-regulation-in-the-era-of-uber-and-airbnb-present-new-hurdles-for-government>.
18. Jayne O' Donnell, "Video visits blocked despite doctor shortage," USA Today, December 07, 2014, <http://www.usatoday.com/story/news/nation/2014/12/07/telemedicine-state-laws-rural-hospitals-specialists/70094828/>; Lauren Silverman, "Texas puts brakes on telemedicine – and Teladoc cries foul," NPR, June 02, 2015, <http://www.npr.org/sections/health-shots/2015/06/02/408513139/texas-put-brakes-on-telemedicine-and-teladoc-cries-foul>.
19. Maggie Zhang, "Adobe Kickbox gives employees \$1000 credit cards and freedom to pursue ideas," Forbes, August 19, 2015, <http://www.forbes.com/sites/mzhang/2015/08/19/adobe-kickbox-gives-employees-1000-credit-cards-and-freedom-to-pursue-ideas/#292d4ebc3c39>.
20. Frank Friedman, Chuck Saia, "How dashboards can help CFOs manage risk," Deloitte Insights (The Wall Street Journal), April 28, 2015, <http://deloitte.wsj.com/cfo/2015/04/28/how-dashboards-can-help-cfos-manage-risk/>.
21. Gwen Moran, "Fostering greater creativity by celebrating failure," Fast Company, April 04, 2014, <http://www.fastcompany.com/3028594/bottom-line/a-real-life-mad-man-on-fighting-fear-for-greater-creativity>.
22. Rob Price, "United Airlines will let you fly free if you find bugs in its software," Business Insider, May 15, 2015, <http://www.businessinsider.com/united-airlines-bug-bounty-free-air-miles-flight-security-vulnerability-2015-5>; "The bounty programs of Google, Facebook, Microsoft... Which tech giant offers the juiciest rewards to hackers," Panda Security, June 23, 2014, <http://www.pandasecurity.com/mediacenter/security/bounty-programs-google-facebook-microsoft/>.
23. Rex Santus, "Facebook's ThreatExchange is a social platform for sharing cybersecurity threats," Mashable, February 11, 2015, <http://mashable.com/2015/02/11/threatexchange-facebook/#.gadARfymq5>.
24. "Wikistrat launches analytics wargame harnessing the power of crowdsourced forecasts," Wikistrat, July 07, 2015, <http://www.wikistrat.com/wikistrat-launches-analytical-wargame-harnessing-the-power-of-crowdsourced-forecasts/>.
25. Emily Steel, "Netflix, Amazon and Hulu no longer find themselves upstarts in online streaming," The New York Times, March 24, 2015, [http://www.nytimes.com/2015/03/25/business/media/netflix-amazon-and-hulu-no-longer-find-themselves-tvs-upstarts.html?\\_r=2](http://www.nytimes.com/2015/03/25/business/media/netflix-amazon-and-hulu-no-longer-find-themselves-tvs-upstarts.html?_r=2).
26. Thomas Bartman, "Confronting a new-market disruption Part 3 – Car2Go," The Forum at Harvard Business School, November 19, 2015, <https://medium.com/bsse-gets-social-media/confronting-a-new-market-disruption-part-3-car2go-7e01398fb458#.d552kxhxb>.
27. Adam Tanner, "Love it or hate it, Ripoff report is in expansion mode," Forbes, May 09, 2013, <http://www.forbes.com/sites/adamtanner/2013/05/09/love-it-or-hate-it-ripoffreport-is-in-expansion-mode/#722e789f33dd>.



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication 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 publication.

#### **About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of DTTL and its member firms. Please see [www.deloitte.com/us/about](http://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.