Gartner

Fi.r.st.

The Gartner Journal of
Finance. Risk. Strategy.

In This Issue

Second Quarter 2020

Fi.r.st.
The Gartner Journal of
Finance. Risk. Strategy.

Group Vice Presidents
Assurance Scott Christofferson
Finance Mark Wiedemer

Practice Vice Presidents
Assurance Christina Hertzler, Matthew Shinkman
Finance Alexander Bant, Bryan Kurey, Johanna Robinson

Distinguished Vice President, Research
Doug Eckstein

Editor in Chief Judy Pasternak

Contributors
Sam Abrams
Stephen Adams
Chris Audet
Alexandra Bellis
Sam Berndt
Pritika Bhattacharjee
Brent Cassell
Laura Cohn
Caroline Conroy
Doug Eckstein
Blakeley Hartfelder
Jessica Kranish
Eliza Krigman
Oana Lupu
Malcolm Murray
Timothy Raiswell
Laura Reul
Daniel Ryntjes
Steve Shapiro
Peter Young
Dian Zhang

Project Manager Cindy Zhang

R&A Creative

Art Director Mike Jurka
Senior Designers Divya Malkani, Brittany Fritz
Editor Ian Whiteley

A World Remade

Letter From the Editor

Remember when cautious optimism ruled the day about avoiding a recession in 2020? Not so long ago, headlines read like this: "With U.S. Help, Global Growth in 2020 May Recover a Bit from a Dismal 2019."[1] Pundits hedged their bets, noting risks like trade wars and debt could cause a downturn. No one mentioned a pandemic.

Yet here we are, battling a health disaster on six continents, a worldwide economic earthquake and a sudden mass shift to remote work — for how long, no one knows.

In this issue, you'll learn how functions can pull together even in the time of COVID-19 to prepare for recovery while staying afloat, be both nimble and efficient, and respond to complex, fast-changing risks.

Among the articles inside:

- A special "Cutting Edge" section is devoted this quarter to what thousands have told us in conference calls and polls about their coronavirus plans, tactics and tough calls.
- "A New Phase of the Virus Crisis" offers lessons from the 2008 financial crisis, past pandemics and the early months of this one.
- "Ethical Sales During a Crisis — What to Do Now and Later" shows how to shore up integrity for commercial teams as pressure ratchets up.
- "When Employees and Suppliers Work Remotely: Privacy and Security Risks" explains how to protect sensitive data when employees, third parties — and their families and roommates — are all working from home.
- "Governance of Third-Party Risk Is Less Complicated Than You Think" gives you an effective oversight model for an area of critical concern, amplified now.

Fi.r.st. stands for the intersection of **Finance, Risk and Strategy** — how companies expand, how they can be both bold and principled and how they persuade employees and investors to join them for the ride. The journal addresses challenges that cut across the C-suite and executive teams.

Recent issues also offer relevant advice. See the 3Q19 Fi.r.st., "Winning in the Turns" for outpacing peers across economic cycles, and the 4Q19 edition, "Paradigm Shifts," for redesigning structure and mindsets to thrive during long-term uncertainty.

— Judy Pasternak

[1] "With U.S. Help, Global Growth in 2020 May Recover a But From a Dismal 2019," Bloomberg Businessweek. (Paid subscription required.)

Table of Contents

Departments

Top Story

Table of Contents

Feature Articles

The Cutting Edge: 2Q20

A Fi.r.st. Look at New Research

Compiled by Oana Lupu

COVID-19 Executive Pulse

This special edition of our quarterly research snapshot is devoted to pandemic plans, tactics, tough calls and opportunities shared by thousands of functional leaders in our conference calls and polls.

4 Pandemic Shifts That Could Last

Sales

1 **Virtual sales-client meetings.** Chief sales officers have used this period of remote work to test lower-cost sales models. The proportion of CSOs considering a permanent change to virtual sellers jumped from 5% in the last week of March to 25% in the first week of April.

2 **Digital marketing spend replaces some sales employees.** CSOs have been forced to prioritize digital marketing spend over traditional sales capacity. It may be difficult to justify adding salespeople back to the team after the downturn.

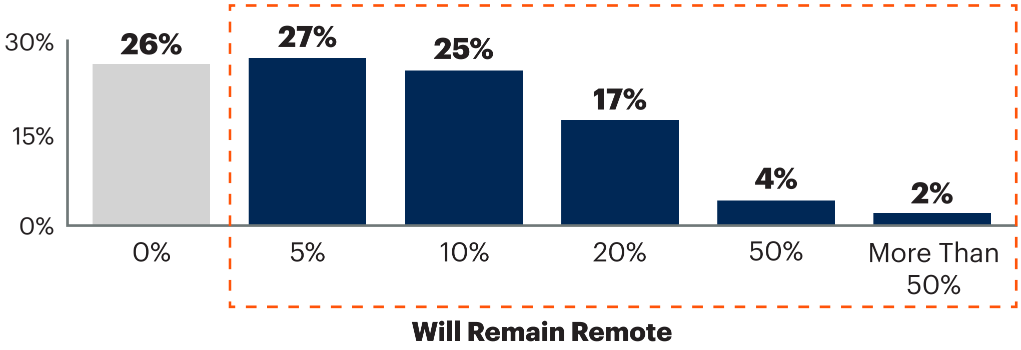
Supply Chain

3 **Improved risk-sensing capabilities.** Companies are monitoring suppliers' financial health and actively searching for a technology solution that can provide real-time visibility into supply chain risks. To better predict future disruptions, it's likely that they will continue the quest for more information about first-, second- and third-tier suppliers.

Working From Home

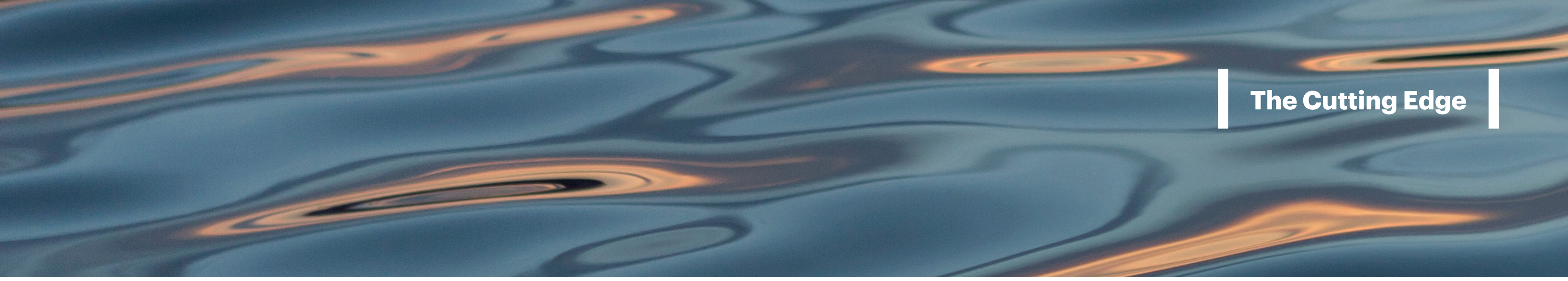
4 **More remote workers.** Some employees will likely shift to long-term arrangements to do their jobs from home after the crisis.

Proportion of Workforce to Remain Permanently Remote Post COVID-19
Percentage of Respondents



Three-quarters of companies plan to permanently shift to more remote work post-COVID.

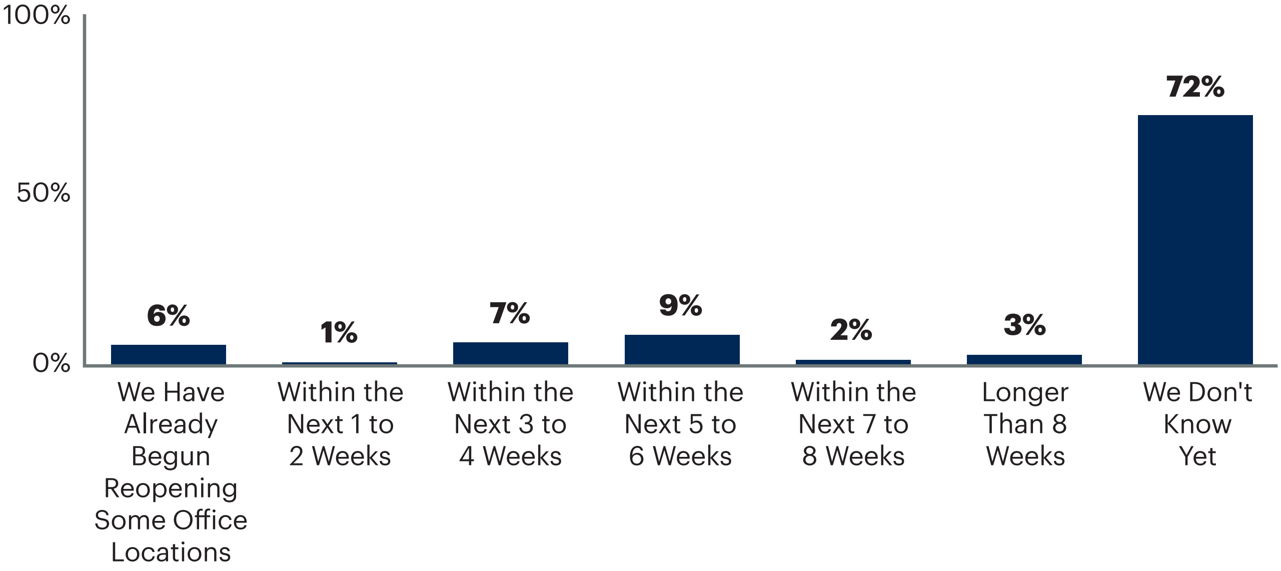
n = 317
Source: 2020 Gartner Finance Leaders Poll
Note: Percentages don't add up to 100% due to rounding.



Reopening Workplaces: A Complex Decision

Most executives don’t know yet when non-essential employees will be able to return to work. But the decision to reopen facilities will be made as a group.

Q: When Do You Expect to Be Able to Reopen Closed Facilities and Start Bringing Employees Back?
Percent Selecting



n = 162

Source: Gartner Managing Through Disruption Benchmarking Against Your Peers Webinar Poll (21 April 2020)

Q: Who Will Be Involved in Making the Decision to Return to the Workplace?
Percent Selecting; Multiple Responses Allowed

1. CEO (94%)
2. Head of HR (82%)
3. General Counsel (53%)
4. CFO (48%)
5. Business Unit Leaders (44%)
6. The Board (29%)

n = 165

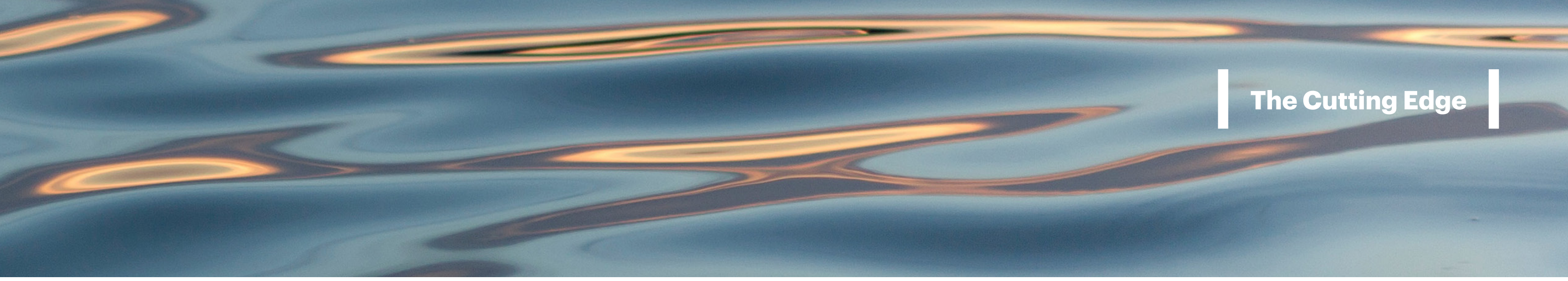
Source: Gartner Managing Through Disruption Benchmarking Against Your Peers Webinar Poll (21 April 2020)

Factors That Will Determine When to Reopen Offices
Percentage of HR Leaders; Multiple Responses Allowed

□ Government Policies/Orders (93%)
□ Guidance From Public Health Officials (85%)
□ Judgement of Leadership (57%)
□ Virus Case Counts/Statistics (28%)
□ School Closures (18%)
□ Local Competitor Actions (18%)
□ Employee Opinions (2%)
□ Other (2%)
□ Not Sure Yet (3%)

n = 165

Source: Gartner Managing Through Disruption Benchmarking Against Your Peers Webinar Poll (21 April 2020)



The Return to the Office: It Won’t Be the Same

Offices will likely reopen before COVID-19 is eradicated, corporate real estate (CRE) leaders tell us. But social distancing, one predicted, could last for another two years. So the office will be different than it was the day it closed:

81% of CRE leaders anticipate staggered remote working days to reduce the number of employees in the building at any given time.

The same percentage say they’ll continue with frequent cleaning.

Employees can expect to have their temperature taken when they enter the building.

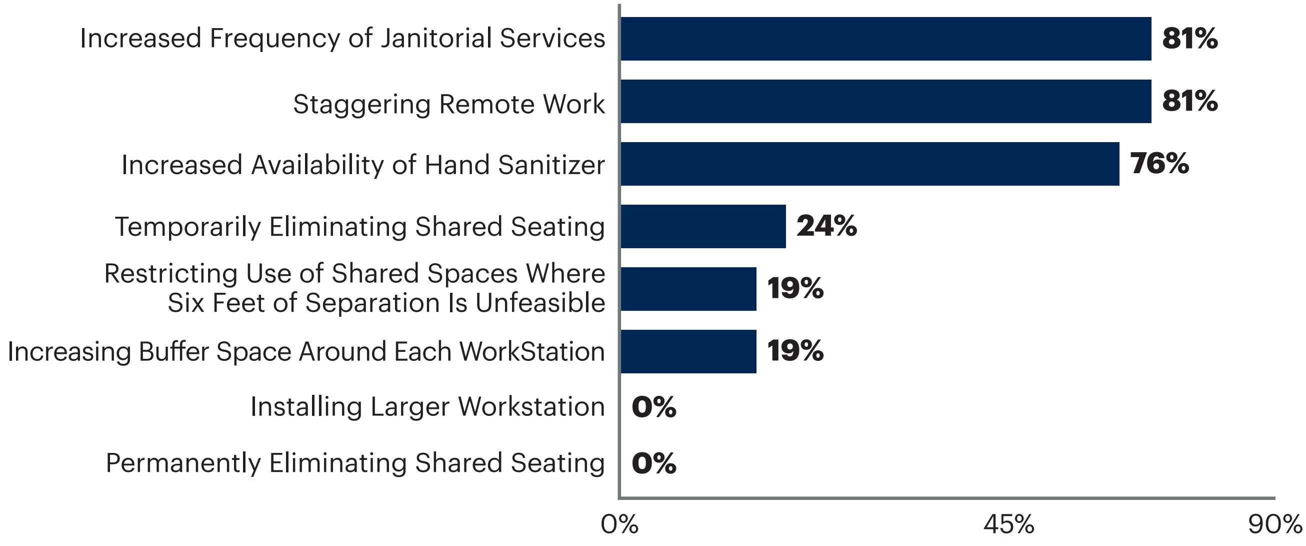
Chairs and monitors may be removed from some desks to create buffer space between colleagues (none said they plan to install larger workstations).

They may restrict the number of employees who can ride in an elevator at a time — that could mean lines — and flex work hours may be required to avoid a morning and evening rush.

CRE executives have not yet determined protocols for deciding when nonessential employees who commute via public transit can safely return to the office.

Q: Which Tactics Do You Expect to Implement Once Employees Return to the Office?

Percentage of CRE Leaders Who Agree



n = 21

Source: Gartner CRE COVID-19 Cohort

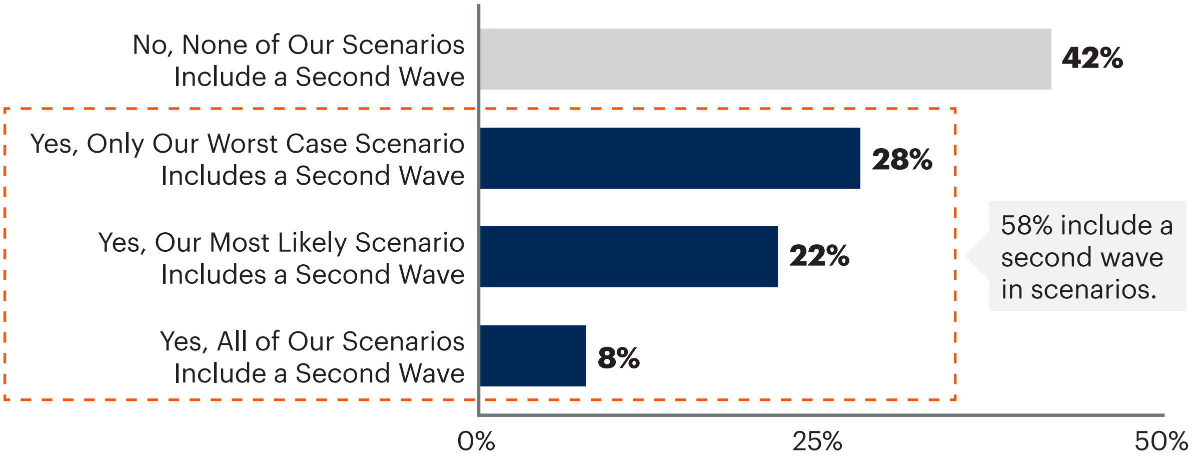
Will A Second Wave of COVID-19 Crush Recovery Hopes?

Six in 10 CFOs are preparing for the possibility of a W-shaped recovery, in which many sectors snap back on pent-up demand and then decline again, especially if there's a new surge in novel coronavirus cases. The same proportion also expect a reduction in earnings (EBITDA) of at least 10% in 2020.

Many finance leaders are:

- Factoring a new outbreak into their scenario planning
- Assessing the revenue impact of a double-dip recession scenario
- Lengthening the timing of worst-case scenarios from 2Q and 3Q of this year to early 2021

Do Your Scenario Plans Include a Second Wave of Disease Outbreak?
All Industries



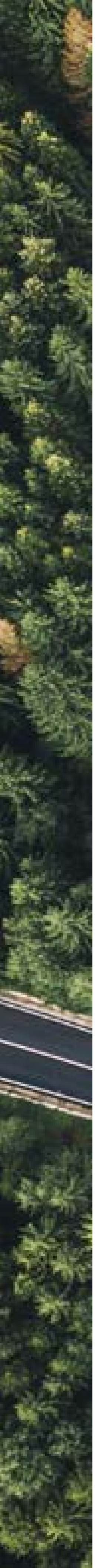
n = 97

Source: Gartner COVID-19 Finance Quick Poll (15-19 April 2002)

Tradeoffs and Priorities

Amidst budget cuts, functions are revisiting their priorities:

Executives	Tradeoff
Sales	Cautiously shifting sales capacity to **healthier business segments** and emphasizing **existing accounts** over new business.
Finance	Ratcheting up collections pressure **on small or infrequent customers,** while limiting such pressure on clients whose market share could increase post-crisis.
Procurement	Extending help to critical **suppliers most likely to survive** the downturn (e.g., shorter payment terms, pulling forward orders) when feasible.
Shared Services	If using more than one business process outsourcing provider (BPO), shared services leaders took note of **which one adapted the fastest** and will choose to do more business with that BPO in the future.



A New Phase of the Virus Crisis

by Dian Zhang

with contributors Stephen Adams, Chris Audet, Sam Berndt, Oana Lupu, Timothy Raiswell, Laura Reul and Steve Shapiro

Now that the COVID-19 crisis has moved from an acute to a chronic stage, senior corporate executives must lead their employees, their investors and their customers through an extended period of fear and uncertainty while planning for recovery.

For a while longer — no one knows how much longer — it will still be true that "the virus does not allow normal life," as a health ministry official in devastated Italy put it to the New York Times.[1] For top management, that means addressing workforce needs and the impact on business operations, knowing that new waves of disease or financial distress could send the company right back to an emergency footing. CFOs have told us they're planning for shutdowns through August, though one noted that with all the volatility, one-week planning is the new "long-term."

Here's some help and some hope, drawn from an analysis of surveys and conversations with thousands of executives across functions, and lessons from the financial crisis of 2008, past pandemics and the early months of this one.

This is a time for all parts of the company to pull together; to practice proactive transparency with employees, investors and the board about efforts to protect the workforce and the business for the long haul. It's time to put capabilities to full use, even outside of traditional boundaries, and to reevaluate the future while assessing cost cuts strategically. Assurance functions can save resources by monitoring third-party risk in a manner both more effective and less time-consuming than conventional methods. Along the way, don't forget to document your lessons learned and put them to future use.

Practice Transparency With Employees, Investors and Boards

Clarity is essential for bringing stakeholders along during prolonged upheaval and to protect the business over the long haul.

Employees

As enforced remote work, fear of illness and worries about job security become a way of life — not just a change of pace — top leaders and managers must help employees handle the ongoing impact on their personal and professional lives. The feelings of anxiety, frustration and burnout common during uncertainty are compounded now by isolation from colleagues and blurred work-life boundaries.

Leaving these emotions unattended can affect staff productivity and engagement, leading to errors, poorer quality and eventually influencing an organization's ability to survive in these difficult times. Those who address these feelings directly can see a 5% improvement in employee ability to focus. Those who don't can see as much as a 21% decline.[2] Take these steps right away if you haven't already:

- Don't "sell" organizational changes; instead engage in two-way dialogue. Staff understanding is more important than employees "liking" the shift.
- Set very clear objectives connecting employee efforts to corporate priorities.
- Be clear about technology use; it's essential for running any dispersed enterprise. Every end user should confirm their understanding by signing a policy that explains access and parameters in simple local language. IT should draft the document and HR, legal, compliance and executive leadership should approve it. Don't forget to include backup communications systems.
- Continually reinforce the importance of a respectful workplace, even when interactions are virtual, as xenophobia and racism have erupted periodically throughout the pandemic. Run your messaging past a diverse group of colleagues to make sure you haven't unwittingly included offensive or tone-deaf language.

Prepare employees for a phased return to work once offices eventually reopen, as it's unlikely their first day back will feel much like "business as usual." Local and national jurisdictions may continue to impose requirements for face masks, disinfection and social distancing. And some employees may remain remote workers for a while.

In China, where the virus hit first and eased first, workers at state-owned companies and key sectors including the finance industry were the first to come back. At Ping An Insurance, a Chinese holding conglomerate, employees in IT, trading and operations went back on site in split shifts as early as 3 February, while everybody else continued to work from home.[3]

Investors and Boards

If your organization needs to revise earnings guidance:

- Avoid unnecessary fluff. Acknowledge the headwind, clarify how it's impacting your business and provide the updated guidance numbers. Investors appreciate brevity.
- Company leaders should highlight successes that preceded restrictions in response to the outbreak. When responding to analyst questions related to COVID-19, address them directly but also underscore business opportunities beyond the time frame of the pandemic.
- Be sure to update all your guidance metrics. If you guide on both revenue and earnings per share, then explain how both will change.
- Immediately following the announcement, speak with your sell-side analysts and top shareholders to explain the impacts in greater detail.

The same is true of communication with the board of directors. Boards require more frequent updates on financial performance during periods of instability. Stay focused on the elements of business economics that matter, to help the board understand performance and relay better advice to management. If board members fulfill the same roles at other companies, what are they seeing in those industries? What was their experience in previous crises and recessions? Board members may have valuable experience the current management team does not.

Redeploy Capabilities That Would Otherwise Go Underutilized

When Italy abruptly shut down restaurants and bars as a COVID-19 containment measure, Campari's commercial team needed to assess the impact quickly; bars alone represent 50% of the company's business in its home country. Antonio Zucchetti, senior director of internal audit, told us his team had been investing heavily in data analytics, so it was well-positioned to help. Audit extracted data and packaged reports for sales in a matter of minutes. At a different Italy-based multinational, compliance is working with audit to test controls in North America and China.

Creative redeployment extends to the front line. In China, cosmetics company Lin Qingxuan closed 40% of its shops but shifted more than 100 in-store beauty advisors to digital platforms like WeChat, where these employees could continue to interact with customers and serve as influencers to boost online sales. The company's sales in Wuhan, where the outbreak first emerged, grew 200% year-over-year.[4]

More than 40 Chinese restaurants, hotels and movie theater chains with plunging revenues also shared a significant portion of their workforce with a supermarket chain that badly needed delivery help because of a boom in online grocery purchases.[4] And in the U.S., hotel chains helped their furloughed workers find temporary jobs at drugstore and grocery chains where demand was surging.[5]

Facilities that would otherwise be idle are also being put to good use. Globally, for instance, auto and other manufacturers announced plans to make ventilators and face masks to help address shortages in medical equipment.[6] In France, perfume production lines were repurposed for hand sanitizers and delivered to hospitals for free.[7] Decisions like these could prove strategic once the economy rebounds, as they help instill public trust in your brand. Nearly seven in 10 consumers are concerned about a brand's impact on society, and 81% say trust is key to their buying decisions.[8]

Meanwhile, executives across functions have told us they are helping employees ready the company for the future in other ways too, assigning those with more downtime than usual to start planning for recovery and take virtual training to sharpen their analytics skills.

Reevaluate the Future While Assessing Spend and Investment

Finance chiefs tell us they are using this time to reevaluate which customers are most likely to survive the downturn and which businesses they want to be in now and after the pandemic fades. Another important area to consider is your current long-term plan, including where to cut and where to invest.

Negotiate better contracts in priority areas rather than abandoning them altogether. It makes little sense to cut budgets on data security, cloud storage or VPN server capacity in a virtual-enterprise world.

For example, functional leaders and procurement can work together to make thoughtful indirect spending decisions. Here are some sample questions to consider (see Figure 1).

Figure 1: Questions for Business Partners

Indirect Spend Category	Questions for Business Partners
Human Resources	• Does your benefits provider have a virus transmission resource center and is it available to staff?
Information Technology	• Is each outsourced help desk prepared and available to assist with a surge of requests from staff working remotely?
Assurance	• Can service contracts with legal, audit or risk management services be renegotiated (e.g., with clearer and better-enforced billing and staffing guidelines)? • Can the scope be expanded at no additional cost? • Are there any duplicate software and tools among assurance functions?
Real Estate and Facilities Management	• Are heating, ventilation and air conditioning (HVAC) systems and building maintenance vendors optimized to prevent virus transmission? • Do contracts include sufficient terms, conditions and requirements to indemnify the buyer and limit virus transmission?
Office and Logistics	• Will critical staff or teams need access to purchasing cards or policies to facilitate at-home or out-of-office supply purchases?

Source: Gartner

Answering these questions will help procurement retain stakeholders' support and inform its conversations with critical indirect suppliers. Ultimately, it can help you find mutually agreeable terms to maintain or expand services without increasing costs.

It also puts the firm at a competitive advantage by avoiding cuts to services, helping the business maintain its edge.

Monitor Third-Party Risk With More Effective, Less Resource-Intensive Methods

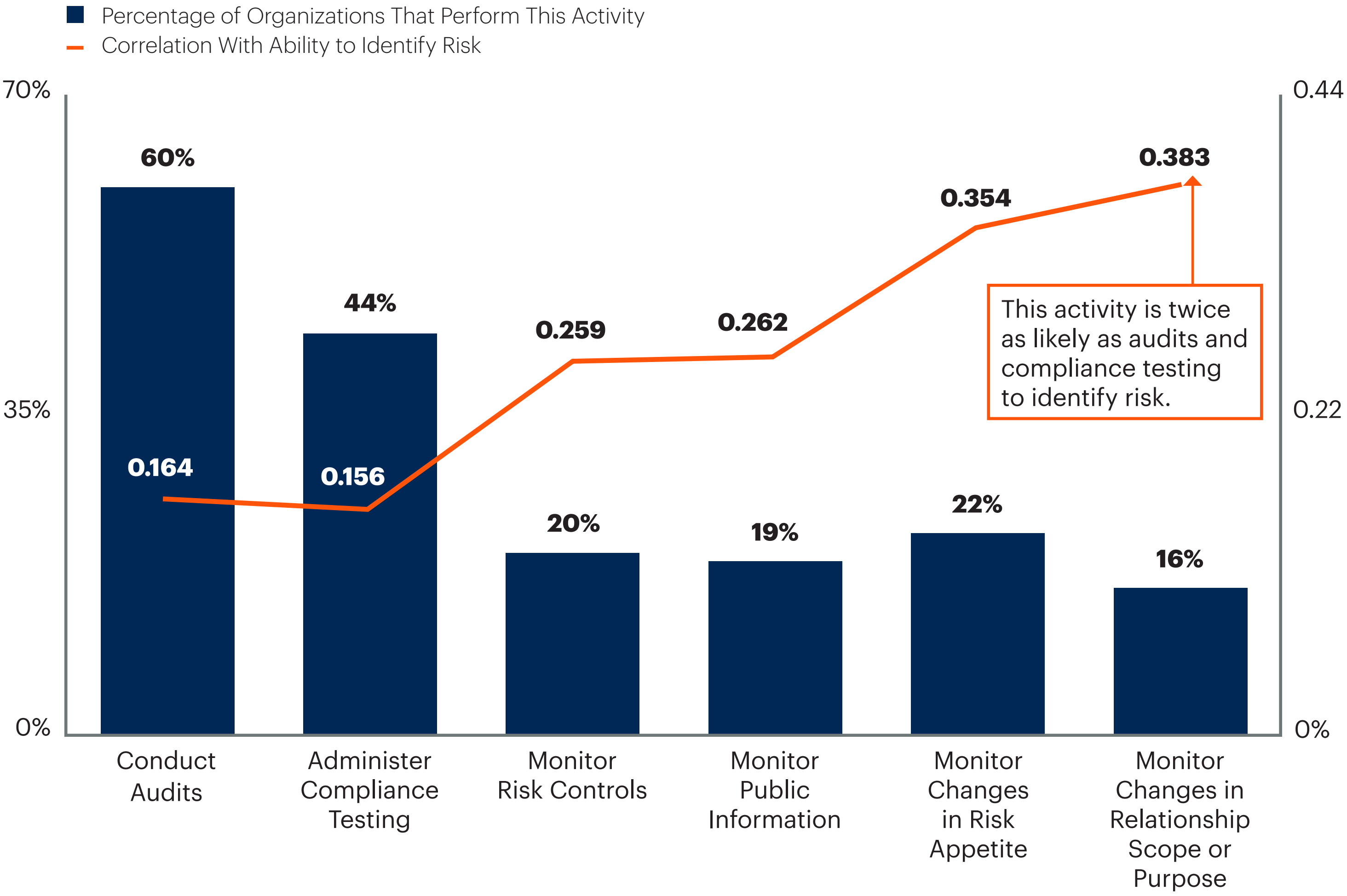
When events move as swiftly as they do now, it's especially critical to monitor third-party risk during the life of a contract, not just during upfront due diligence or when it's time to renew.

Assurance, finance, procurement and supply chain executives at hundreds of organizations told us their most common tactics are regular audits of high-risk third parties and tests to ensure they meet relevant compliance standards. Those activities are resource-intensive and don't sufficiently improve risk outcomes.

Increasing the business's role has about twice the impact of those conventional methods of identifying risks — and it's a lighter lift (see Figure 2).

These findings are critical for organizations that might think monitoring is out of reach. They also suggest the most important support organizations can receive is from those closest to the third-party relationships — business partners.

Figure 2: Relationship Between Monitoring Activities and Risk Outcomes



n = 953

Source: 2019 Gartner Cross-Functional Third-Party Risk Management Model

To help the business play a more meaningful role in monitoring third party risks, you should:

- Create a clear role for business partners and relationship managers. Equip them with risk triggers that will alert them during performance reviews or invoicing to changes in risk appetite or relationship scope — for instance, when the third party names a new fourth-party supplier or merges into a new geographic location.
- Rethink audits and other monitoring activities that take more effort but are less effective.

Document Lessons Learned and Feed Them Into Risk Models for the Future

Crisis response teams should discuss at each meeting what went well since the last one, what didn't and how they may need to adjust current response plans for the future. Ask, "What would we do differently if we were doing this again? Who would we have worked with to better prepare before and during the outbreak?" Keep a list as you go.

Use the lessons to develop or update prebuilt risk models for future pandemics, the same way companies have done with previous outbreaks such as SARS from 2002 to 2003, H1N1 from 2009 to 2010 and MERS from 2012 to 2019.

For instance, one company worked out business areas' priorities in advance to keep response efforts focused on what matters most (see Figure 3).

Figure 3: Example Pandemic Preparedness Framework

Recovery Timeline

Tier	Class	RTO[a]	RPO[b]	Description	Business/IT Function
0	🟥 Critical IT Infrastructure	0-15 mins	0 mins	Base infrastructure and common services to be restored prior to business functions.	Network, VPN servers, OS, software/DB DNS, Active Directory
1	⬜ Mission-Critical/ Platinum	<1 hour	8 hours	Business functions with the greatest impact on the company's continued operations — require immediate recovery.	Client-facing, revenue production, email
2	🟧 Business-Critical/ Gold	<24 hours	24 hours	May not meet mission-critical criteria but will need to be recovered soon after that class.	Less critical revenue-producing functions
3	◼ Important/ Silver	3-10 days	1 week	Important business processes that will require recovery but only after mission-business-critical classes.	Administrative functions
4	🟫 Deferrable/ Bronze	10+ days	Last backup	Business processes not immediately required to support critical business processes. They may be functions needed in the long term but not in the first weeks of a disaster.	Budgeting, training/LMS, low-impact activities

Source: Gartner

[a] Recovery time objective

[b] Recovery point objective

To prepare for an avian flu outbreak in 2006, Goodyear outlined three steps to make sure it would have the right personnel available to continue operating (see Figure 4).

With new inputs from the world's searing experience with COVID-19, companies will be better equipped to navigate the next pandemic — if the past is prologue, more outbreaks will occur.

[1] "Italy, Pandemic's New Epicenter, Has Lessons for the World," The New York Times.

[2] 2013 Gartner Quality Leadership Council Employee Survey

[3] "Here Comes the First Wave of Returning Workers After the Coronavirus Outbreak," ChinaNews.com.

[4] "How Chinese Companies Have Responded to Coronavirus," Harvard Business Review.

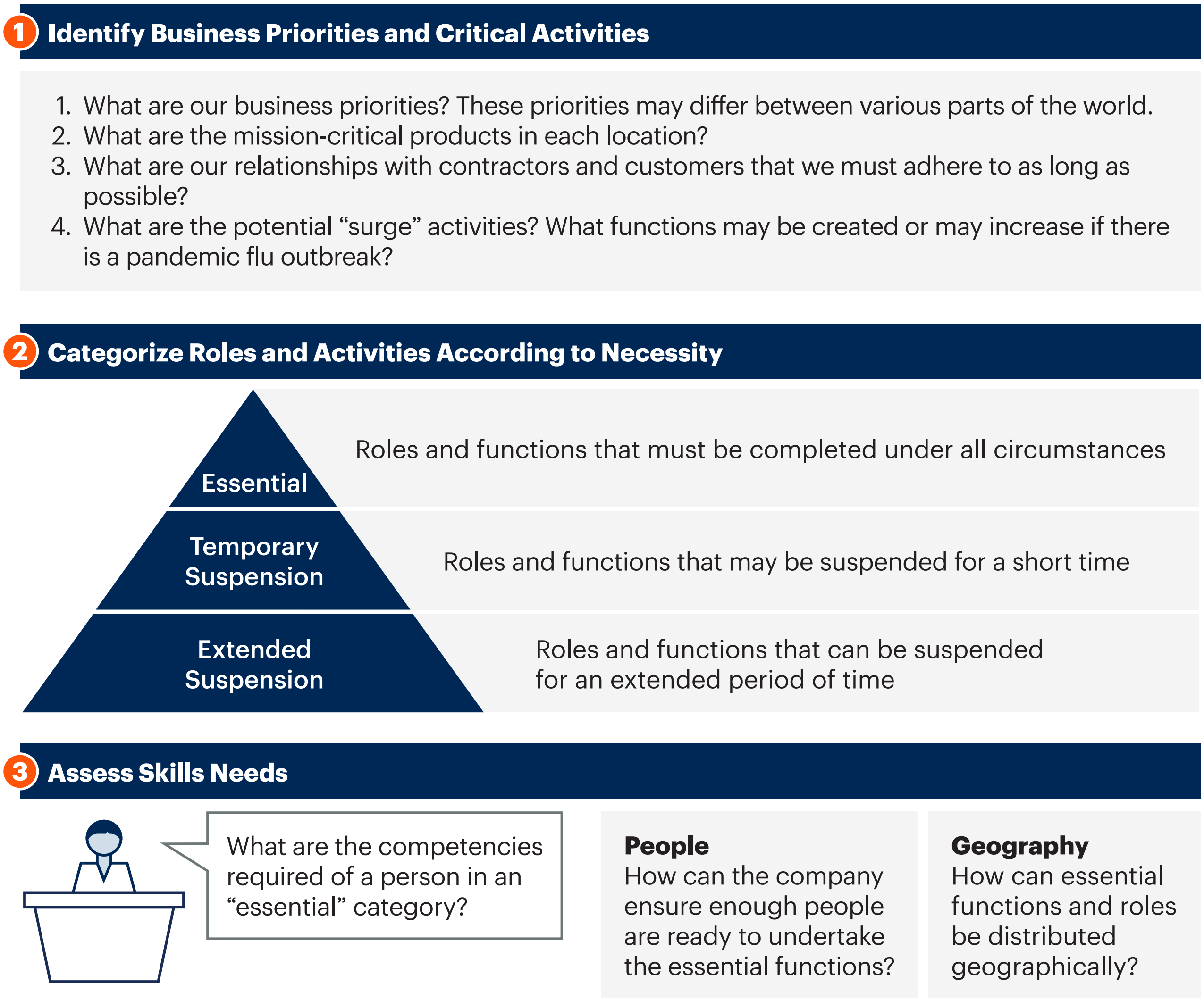
[5] "Furloughed Hilton Workers Offered Access to Other Jobs During Coronavirus Pandemic," USA Today.

[6] "Automakers Step Up to Challenge of Helping in Coronavirus Pandemic," Car and Driver.

[7] "LVMH, Which Owns Luxury Brands Like Louis Vuitton and Christian Dior, Will Use Perfume Production Lines to Make Hand Sanitizer," CBS News.

[8] "In Brands We Trust?: 2019 Edelman Trust Barometer Special Report," Edelman.

Figure 4: How Goodyear Planned for Absenteeism
Goodyear's Process for Identifying Critical Roles



1 **Identify Business Priorities and Critical Activities**

1. What are our business priorities? These priorities may differ between various parts of the world.
2. What are the mission-critical products in each location?
3. What are our relationships with contractors and customers that we must adhere to as long as possible?
4. What are the potential "surge" activities? What functions may be created or may increase if there is a pandemic flu outbreak?

2 **Categorize Roles and Activities According to Necessity**

Essential — Roles and functions that must be completed under all circumstances

Temporary Suspension — Roles and functions that may be suspended for a short time

Extended Suspension — Roles and functions that can be suspended for an extended period of time

3 **Assess Skills Needs**

What are the competencies required of a person in an "essential" category?

People
How can the company ensure enough people are ready to undertake the essential functions?

Geography
How can essential functions and roles be distributed geographically?

Source: Gartner

When Employees and Third Parties Work Remotely: Privacy and Security Risks

by Laura Cohn
with contributor Steve Shapiro

The sudden and massive work-from-home arrangement now underway around the world presents companies with enhanced risks surrounding remote work. What was once a background concern over privacy, cybersecurity and disengagement is now front and center in the face of COVID-19.

Most employers have neglected to convey the rules staff should follow while working outside the office. A Gartner poll of 500 U.S. employees taken in the first week of March showed just 22% of companies communicated a plan of action in response to the virus.

With data breaches at record highs in 2019, organizations were vulnerable even before the global pandemic hit, but effective communication about behaviors is critical now more than ever.[1] These aren't your normal remote work concerns because this is not a normal situation. It's not just your employees and potentially your third parties staying at home, but also their spouses, roommates, parents and children. They're also working at a time when people are most vulnerable to malicious actors seeking to take advantage of misinformation and uncertainty.

Sensitive company data, and that of employees themselves, is vulnerable. To protect such information, assurance leaders should help their organizations communicate remote working rules that include clear guidance on how to safeguard data while working outside the office.

"Policies don't mean much if they are not properly communicated," Daniel Marvin, a partner and co-leader of the cybersecurity, privacy and data protection team at Morrison Mahoney, told us. "An informed workforce is key. Employees are both the weakest link and often the last line of defense."

> Even overhearing a work call held by a spouse or roommate could make a person privy to nonpublic material information.

Most security failures originate from an organization's own employees, according to our data privacy research. In the work-from-home environment, assurance leaders must:

- Work with the CISO and IT to communicate cybersecurity guidance.
- Remind employees that rules regarding proper email protocols must be followed outside the office.
- Check that remote work policies include measures to safeguard company data — and then distribute (or redistribute) the policies.
- Guard against an increase in phishing and malware attacks exploiting virus-related anxiety.
- Confirm that vendors also have adequate work-from-home policies and strong privacy and cybersecurity standards.

At a time when even overhearing a work call held by a spouse or roommate could make a person privy to nonpublic material information, it's critical to be careful about sharing confidential corporate information. Let's take each step one by one.

Work With the CISO/IT

Coordinate with your cross-functional partners to make clear to employees that the security practices required in the office also apply at home. In fact, one company's general counsel told us their legal team has already started providing guidance on remote working arrangements to the organization's information security team.

Heightened risks have also led data protection authorities and cybersecurity agencies to release recommendations. The U.S. Cybersecurity and Infrastructure Security Agency, for instance, published an alert on 13 March 2020 on the security of VPNs.[2]

Remind Employees About Email Protocols

It's also crucial to tell employees that rules regarding proper email and cybersecurity protocols must be followed.

"Public Wi-Fi is an 'absolute no,'" Morrison Mahoney's Marvin warned. "Companies could invest in virtual VPNs to offset privacy issues relating to Wi-Fi outside of the home. It is also important that home Wi-Fi systems that are used to access company resources are Wi-Fi protected and secure."

While it may seem unnecessary to remind workers to secure their home Wi-Fi systems, which is as simple as making it password protected, the Pew Research Center has found that Americans struggle with cybersecurity.[3]

Sending sensitive data to a personal email account or computer is also an unnecessary risk, since such accounts and devices tend to be less secure. Instead, staff should always use a work-issued computer or connect to the secure work network (VPN), to work with personal information.

Check Remote Work Policies

Assurance leaders should also check that remote work policies include measures to safeguard company data — and then distribute (or redistribute) the policies to get the word out. Coordinate with the CISO and human resources to send an email blast, with bullet point reminders and links to relevant policies, including confidentiality policies. Employees are not likely to read long policy documents when they're glued to the news and trying to get work done.

If you need help setting up such a policy, our "Toolkit: Remote Work Policies" provides guidance.

For instance, the toolkit notes it's critical to "take precautions to ensure that monitor screens and/or printed materials with sensitive data (such as health records, customer personal information or financial data) are not visible to others." More specifically, where appropriate employees at home should lock doors and windows "to ensure that family or house members do not have access to confidential materials."

Guard Against Heightened Employee Vulnerability

Cybercriminals generally exploit people's hopes and fears, and with a lot of fear around COVID-19 they've already found ways to cash in. Behaviors and emotions that cyberattacks exploit include an inclination to respond to authority, a desire for rewards, ignorance and fear, an impulse to be helpful — and a tendency to trust (see Figure 1).

Awareness about these scams is often the best protection, but you should also consider why employees are vulnerable to these threats and target your training resources accordingly (see Figure 2).

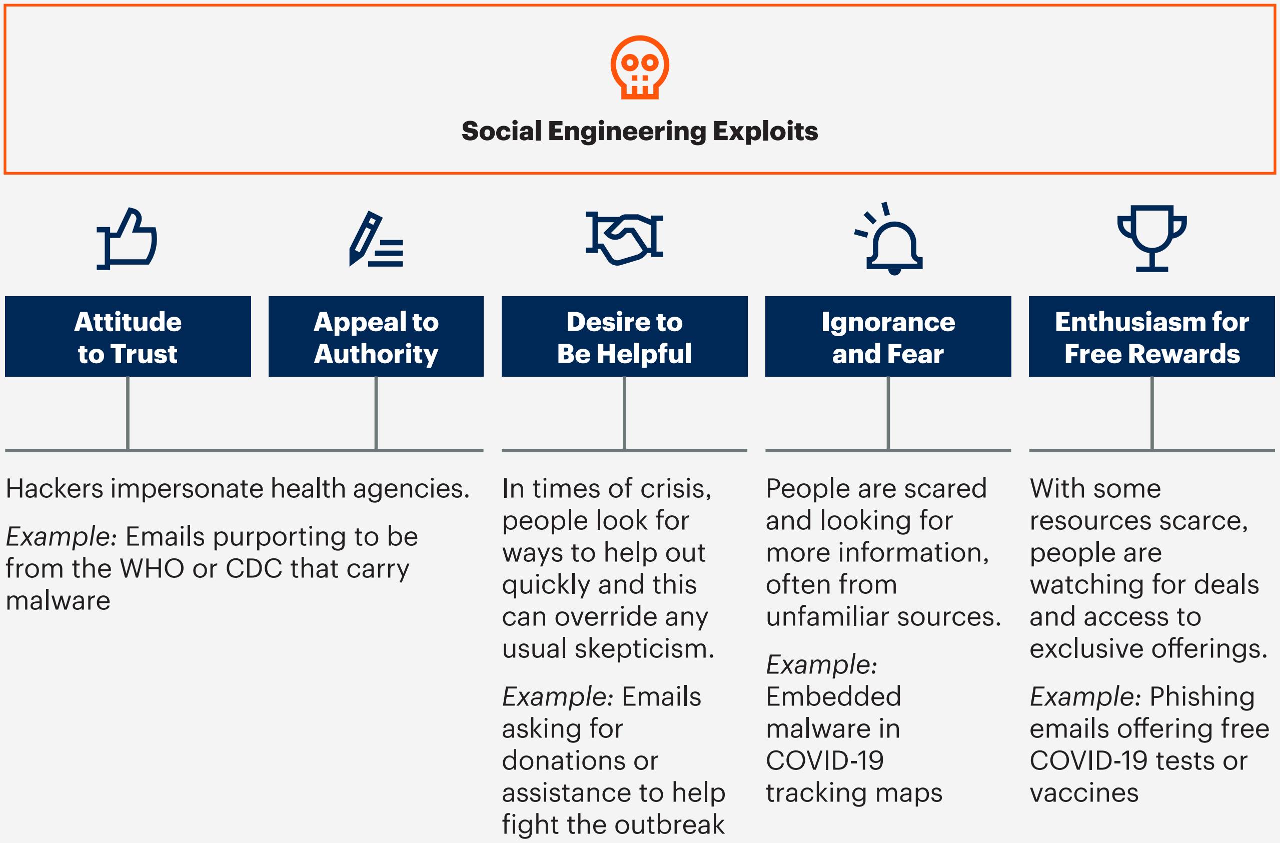
Note that cybercriminals have even used a legitimate interactive coronavirus map to spread malware, so collaboration between assurance partners at this moment is crucial.[4]

Third-Party Employees Are Working From Home Too

A new challenge that emerged in the wake of the COVID-19 crisis: third parties with remote workforces might put sensitive company data at risk.

For organizations, managing third-party privacy risk is tough even in the best of times, since an increased dependency on outside parties has expanded the risk universe into an extensive fourth and "nth" party network.[5] Just as organizations must make sure their employees maintain strong privacy practices when working from home, they also need to check whether their outside vendors are taking steps to secure sensitive company data. This could fall to in-house legal and privacy leaders in collaboration with compliance or procurement. It may also involve business executives or IT managers.

Figure 1. Behaviors That Social Engineering Attacks Exploit: Amplified by COVID-19



Social Engineering Exploits

Attitude to Trust / **Appeal to Authority**

Hackers impersonate health agencies.

Example: Emails purporting to be from the WHO or CDC that carry malware

Desire to Be Helpful

In times of crisis, people look for ways to help out quickly and this can override any usual skepticism.

Example: Emails asking for donations or assistance to help fight the outbreak

Ignorance and Fear

People are scared and looking for more information, often from unfamiliar sources.

Example: Embedded malware in COVID-19 tracking maps

Enthusiasm for Free Rewards

With some resources scarce, people are watching for deals and access to exclusive offerings.

Example: Phishing emails offering free COVID-19 tests or vaccines

Source: Ashish Thappar, "Social Engineering: An Attack Vector Most Intricate to Tackle!" 3 August 2018; Gartner

Organizations should ask about the home-working, bring-your-own-device and cybersecurity policies of their vendors, Marta Dunphy-Moriel, partner and interim head of the data protection and privacy team at the London law firm Kemp Little, told us.

More specifically, she suggests confirming the staff of third parties have had privacy and security training recently. In addition, she says companies should make sure they have clauses in their contracts that cover data loss and breaches to an extent they're satisfied with. Finally, she said it's crucial to be clear about which vendors an organization's third parties use and how those organizations deal with privacy and security issues.

Engaging in open dialogue about privacy and security commitments is critical. "Now more than ever, it is important that we work with providers to have a good communication flow, so that companies in the processing chain work together to fix any issues that happen instead of dealing with them internally and keeping quiet about them," she said.

Dunphy-Moriel also offered a note of caution. "Don't engage vendors in a rush – even if we are working on tight deadlines, make sure you know who you're entrusting your data to," she said. "The urgency is unlikely to be a sufficient excuse if something goes wrong."

[1] "Number of Records Exposed in 2019 Hits 15.1 Billion," Risk Based Security.

[2] "Enterprise VPN Security," U.S. Department of Homeland Security.

[3] "Americans and Digital Knowledge," Pew Research Center.

[4] "Live Coronavirus Map Used to Spread Malware," Krebs on Security.

[5] 2019 Gartner Cross-Functional Third-Party Risk Management Survey.

Figure 2: Reasons for Insecure Behavior and What to Do About It

Reason for Insecure Behavior	Why It Leads to Bad Behavior	How to Target Training Resources
Burden of Compliance	Employees perceive that maintaining cybersecurity is time-consuming and difficult to achieve as it requires extra steps from their daily routine.	• Create short and crisp content. • Use employee-friendly language. • Help employees see that behaving securely is easier than they think.
Policy Knowledge	Employees aren't aware of the security policy and what they should do to be secure.	• Link training back to organizational policies. • Align all awareness tools (e.g., posters, wallet cards) to the same key policy points.
Risk Perception	Employees do not perceive their actions to be risky.	• Share examples of actual cyberattacks on similar organizations. • Quote industry experts, academic professors and quantitative studies for credibility.
Emotional Commitment	Employees don't consider behaving securely as the "right thing to do," regardless of self-interest. They think no one complies with security guidelines.	• Engage senior leaders and role models for training (e.g., video segments). • Conduct group discussions about company values and the mission statement and security's role in enabling them.
Self-Interest in Security	Employees feel they will not be impacted by a cybersecurity attack.	• Share examples of actual cyberattacks and their impact on individuals. • Create incentives for secure behavior and penalties for nonsecure behavior.

Source: Gartner

Ethical Sales During a Crisis — What to Do Now and Later

by Dian Zhang

Now is the time to remind commercial teams, which are particularly vulnerable in high-pressure environments, to maintain integrity and corporate guidelines.

With COVID-19 weighing down the global economy in ways potentially greater than previous recessions, sales employees are more likely to make poor decisions, such as circumventing appropriate procedures, making false promises and opening accounts without customer consent.[1,2,3,4,5] These mistakes, which may show up in the news, can hurt the company's reputation, attract heavy regulatory penalties and damage long-term financial results.

And while keeping employees on the right side of company policy is an important step to take today, compliance leaders should also think about how to, as a longer-term project, revamp training for the commercial team so ethical sales is part of their DNA.

Here are some tactics on ways to engage with sales about maintaining ethics now and a primer on how to upgrade training in the long term. For example, we show how Dell, from planning to execution, baked compliance guidance into the broader commercial curriculum.

Now: Share Timely Reminders and Specific Guidelines

Start by candidly acknowledging the pressure — at this point, sales employees will be reeling from shock at the virus's spread and its impact on their personal and professional lives. Then reiterate the importance of heeding your company's ethical principles, especially in difficult times.

Instead of repeating the code of conduct for all employees, make your message specific to the day-to-day work of this group. You could:

- **Translate your company's core values into expected behaviors.** For instance, "Do the right thing" in the sales context can mean, "Clarify what the product/service can do for customers and what it can't."

- **Answer frequently asked questions related to sales practices,** such as gifts and entertainment, fair competition and anti-corruption.
- **Remind sales employees of all the different channels available for asking questions or reporting issues.** Allay concerns by clarifying how compliance handles their claims. For instance, if a person claims through the helpline that a sales target is unreasonably high, say his or her identity will not be shared with the supervisor.

Additionally, offer managers tools and resources to engage their teams in regular conversations, especially while working remotely, about what's good, what's unacceptable, and creative ways to achieve good results without breaking corporate rules.

In the Long Run: Better Training That Fits Into Sales Workflows

To make compliance teachings last, you'll also need a longer-term plan to transform how your salespeople learn.

One way is to integrate compliance training into the broader sales curriculum. This can release employees from other stand-alone requirements, and help compliance better tailor its offering to salespeople's needs.

This was the idea behind technology company Dell's compliance training for the sales team. As a result, the course became the highest-rated module, receiving a Net Promoter Score of 93%. It also helped with sales performance. It "gave me trust in our ethical model facing the customer," said one participant.

To make the content relevant to the target audience, Dell's compliance team collaborated with sales leaders to:

- Feature language familiar to salespeople.
- Structure training around core sales activities.
- Link concepts and actions to outcomes that matter to sales.
- Invite tenured members from sales to co-facilitate workshops and answer specific questions (see Figure 1).

Figure 1: How Dell Allocates Training Content Delivery Responsibilities by Strength

	Pre-workshop	Live Training Workshop	Post-workshop
Compliance facilitators contribute expertise on how risk and company policies impact sales workflows and ensure technical questions are answered appropriately.	Use compliance subject matter expertise to help create the training content.	Co-facilitate a four-hour training session of sales employees by answering their questions.	Host optional monthly calls to answer any lingering employee questions.
Sales facilitators have strong relationships with sales staff, increasing the credibility of the training and presenting content in a way that is more relevant and easily understood by employees.	• Lead an ongoing "train the trainer" process for new facilitators. • Inform content creators on sales topics.	Co-facilitate a four-hour training session of sales employees by leading the discussion.	Manage ongoing training operations in coordination with sales learning and development.

Source: Adapted from Dell

Borrowing this tactic requires buy-in from your sales counterparts. See how Dell's compliance leaders addressed and overcame common concerns about the project (see Figure 2).

Revamping training is not a short-term project. It took Dell's compliance team six months to design the content and another three to plan for implementation. But the effort was worth it; after the integrated training, compliance was able to discover and respond to red flags faster.

Figure 2: Overcoming Stakeholder Pushback

I am worried this will distract from the key messages we must get across in our training.	Sales Leader	Compliance	**The training is designed to make salespeople sell more effectively while being compliant.**
How long is this going to take? I don't have time to take my employees off the floor.	Sales Manager	Compliance	**It will actually be less disruptive as staff will be released from all other existing compliance training requirements.**
How will this be better than current training?	Sales Leader	Compliance	**This training teaches sales staff how to use ethics and compliance as a competitive differentiator, while providing clarity on specific behaviors that achieve compliance rather than high-level guidance.**
Changing the way we train on compliance is a lot of work.	Compliance Staff	Compliance Leadership	**The training will be very valuable for salespeople and will have a big impact on compliance outcomes.**

Source: Adapted From Dell

[1] "More Severe Than the Great Recession," The New York Times (free registration required).

[2] "The U.S. Economy Can't Withstand the Coronavirus by Itself," The New York Times (free registration required).

[3] "CFPB Says Fifth Third Employees Opened Accounts Without Customer Consent," Wall Street Journal (free registration required).

[4] "AT&T Might Be the Next Wells Fargo (and Doesn't Seem to Be Doing Anything About It)," Compliance Week (free registration required).

[5] "The Price of Wells Fargo's Fake Account Scandal Grows by $3 Billion," The New York Times (free registration required).

Organizations with a strong culture see 9x fewer instances of misconduct

Research shows that employee misconduct spikes during times of economic uncertainty.

But less than a third of compliance executives are confident in their ability to improve their organization's culture.

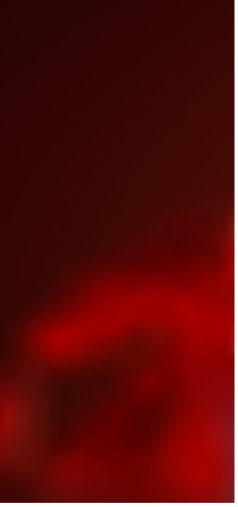
Use our RiskClarity survey to assess your organization's culture and identify hidden risks:

- Target specific areas of employee risk quickly.
- Perform an enterprisewide cultural assessment.
- Uncover root causes of employee misconduct and manage them proactively.

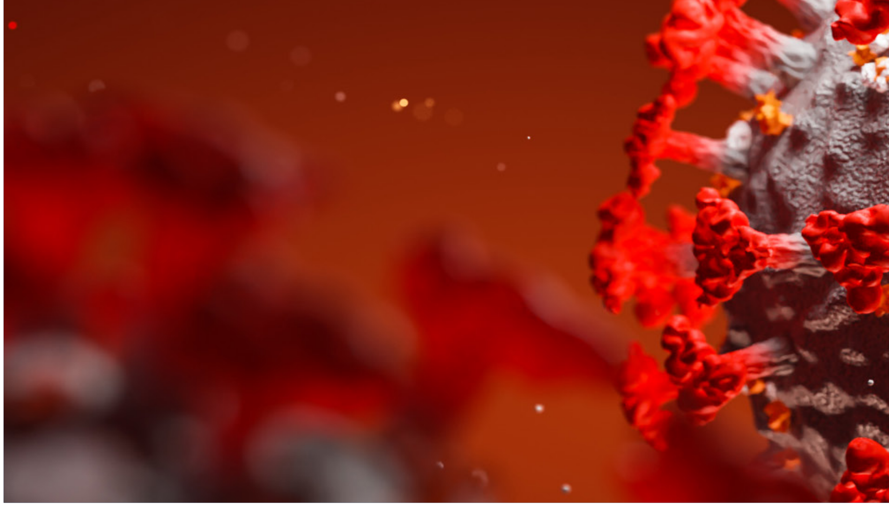
Learn more about RiskClarity: A Corporate Integrity Service™

gartner.com/en/legal-compliance/trends/risk-clarity-survey

Gartner®



Pandemic Briefing



Virtual Development Conversations and Mid-Year Reviews

by Brent Cassell

While almost 90% of organizations are promoting social distancing with remote work, HR leaders tell us managers are concerned about employee productivity and engagement. Fortunately, manager-led employee development will help even if conversations take place online.

You may be tempted to postpone, or even cancel, performance conversations due to the tremendous personal and professional impact of the coronavirus. Don't.

1. When employees feel isolated from friends, co-workers and family, make conversations continuous and ongoing. Forty percent of organizations added more virtual check-ins between employees and managers since the start of the pandemic, and 32% introduced new tools for virtual meetings.
2. When employees are anxious about the present, focus on the future: skills to learn, possible career paths and network connections to drive performance. This is effective any time and may also be a welcome "release valve" for employees.
3. When employees are inundated with dire news, focus on the positive while preparing for negative reactions — you may see more denial, shock, anger (and even open hostility) from direct reports during performance management now. The best course, as always, is to stay calm and unbiased: support feedback with examples, seek reasons for resistance and candidly discuss the consequences of failing to address issues.

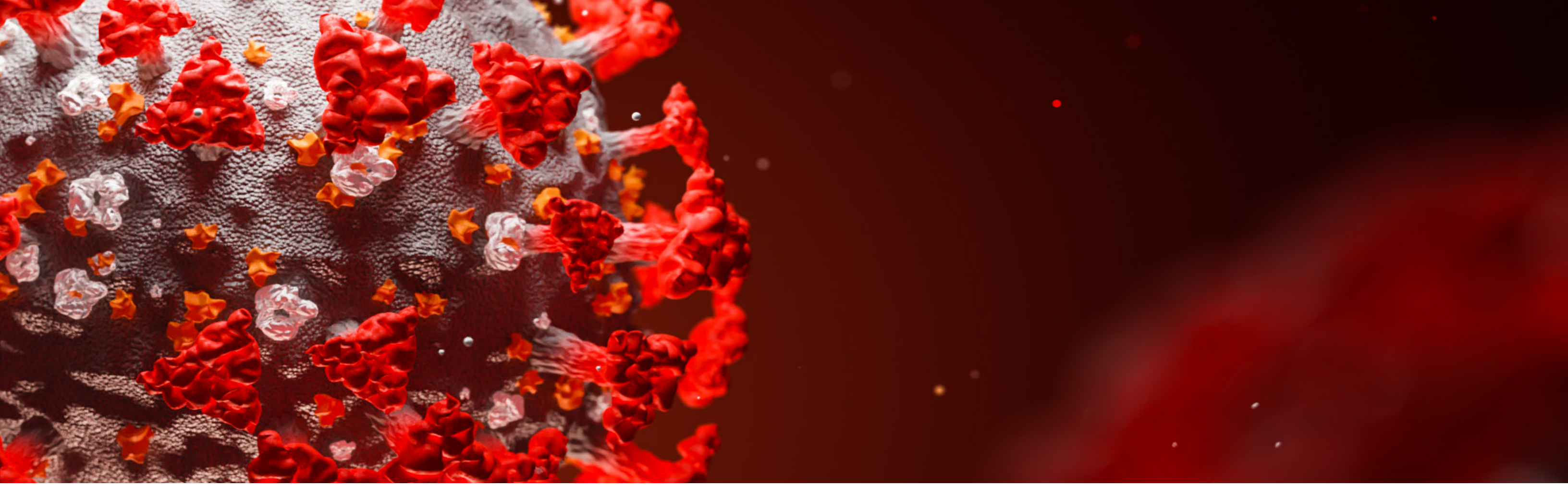
Protecting Those Who Work On-site

by Dian Zhang

Staying on-site is scary. In grocery stores, hospitals, manufacturing plants and shipping services, personal interactions are integral to the work, raising the odds of exposure to SARS-CoV-2.

Among ways to keep the frontline and essential staff healthy and feeling protected:

1. Allow protective gear "if it makes your employees feel safer and does not create a problem," Katherine Dudley Helms, an expert in employment matters at Ogletree Deakins, told us. Some supermarkets opposed this step at first but came around. Walmart announced plans to deliver non-N95 masks to all staff.
2. Get creative with social distancing. Safeway put markers on the floor and limited the number of customers in stores. Louws Truss Inc. staggered shifts at factories and closed doors between departments. Corporate real estate executives also cite reconfigured assembly lines with each person handling more steps.
3. To prevent discrimination against those returning from self-isolation or medical leave required by authorities, clarify to all that nobody sick — either staff or third parties — is allowed on site. Explain criteria employees must meet to come back from quarantine. "When they see someone in the workplace, they should know [that person] has come through that [standard]," Carol Miaskoff, associate legal counsel at the U.S. Equal Employment Opportunity Commission, said.



Performance Targets for the Pandemic Year

by Pritika Bhattacharjee

FP&A leaders should think differently about internal targets in COVID-19's wake or risk demotivating staff just when motivation is crucial. Yet adjusting too soon may require more change as the impact unfolds, piling undue pressure on the business.

Consider:

1. Metrics crucial to effective response and recovery instead of traditional financial metrics.
2. Monthly, quarterly or semi-annual targets for certain metrics or KPIs. Keep staff focused on what matters most in the near term. Allow "early wins." Leave room for change if needed.
3. Relative rather than absolute targets to hold business leaders to a fair standard. Use familiar metrics like revenue, profit, and cost but as percentages or growth rates; measure performance against counterparts (e.g., beat 50% of peer group on cost).
4. Ranges rather than point targets; keep the business focused on goal without expecting leaders to hit a falsely precise number. Set the bottom of the range as the minimum expectation and anything above that as overperformance; you'll inspire efforts to overperform.
5. Targets that must remain ambitious. An example: units that make products currently in higher demand, such as medical devices. Similarly, determine if businesses across the portfolio need more aggressive strategic objectives to keep long-term value creation in sight (even if short-term financial targets are downgraded).

Privacy and Health Checks Should Go Hand-in-Hand

by Laura Cohn

Legal leaders have an obligation to maintain sound privacy practices while keeping the workplace safe.

A case in point: The temperature check. About a quarter (26%) of legal, compliance and privacy leaders told us during an April snap poll their companies were already doing this; these tests could become common at entrances as offices reopen.

1. Notify staff and visitors of this new policy. Consider posting a sign visible to all approaching your building so no one is surprised. If your organization falls under the California Consumer Privacy Act, tell people what information you're collecting, what you're going to do with it and who has access to it.
2. A healthcare professional or someone authorized to make decisions about sending people home and handling data should conduct these tests in an area away from others.
3. Carefully weigh whether you need to hang onto readings you collect. Store such data securely and only retain it as long as you need it.
4. Communicate privacy practices. Legal leaders tell us they are releasing messages through HR since employees view it as a familiar source of information.

Dynamic Risk Governance Works Better Than the 3 Lines of Defense Model

by Malcolm Murray

The chaotic corporate response to the COVID-19 pandemic spotlights the flaws of the "three lines of defense" risk governance model widely adopted in the wake of the 2008 financial crisis — the model 87% of organizations still rely on.[1] It's time to upgrade to a next-generation model we call dynamic risk governance (DRG) that boosts the effectiveness of risk management significantly.

Supply chains falling into disarray as the outbreak started to spread and the hasty adoption of untested business contingency plans illustrate that traditional governance mechanisms fail when confronted with fast-moving and interconnected risks. Senior management and the board of directors have only a fragmented view of risk, the risk and assurance functions have trouble collaborating and business units are tired of thinking about risk, if they consider it at all.

The classic three lines of defense (3LOD) model — with the business as first line, risk monitoring functions as second and audit as third — is one-size-fits-all, role-based and analog. DRG, by contrast, is activity-based, risk-tailored and digital-first (see Figure 1).

The shift may sound daunting, especially to C-level executives who must get more involved, but DRG brings much-needed clarity and efficiency — matching responsibility to the right owner and risk management to the right level of intensity. As a result, investments of time and energy flow where they are needed most and response is faster.

The Building Blocks of DRG

Activity-based means dispensing with the idea that only the first line owns all risk activities and assigning accountability without regard for the borders between first-, second- and third-line risk management. Senior management — not assurance functions — should determine who will decide the task owners for a particular risk.

Figure 1: Differences Between Traditional Risk Governance and DRG

Traditional Risk Governance (Risk Governance 1.0)	**DRG** (Risk Governance 2.0)
Role-Based Risk Governance: Accountability for risk activities is assigned based on the broad roles of the 3LOD: ownership, monitoring and independent review.	**Activity-Based Risk Governance:** Accountability for risk activities is assigned based on key activities, such as risk reporting, risk tolerance setting and risk identification.
One-Size-Fits-All Risk Governance: The same governance models are used for different industries, organizations and risks.	**Risk-Tailored Risk Governance:** The governance model is tailored to the risk based on three specific factors — the risk's speed, the risk tolerance and organizational constraints.
Analog Risk Governance: Technology solutions are applied as an afterthought if deemed applicable.	**Digital-First Risk Governance:** Risk management prioritizes automating controls and KRIs, sharing data analytics and using common technology platforms.

Source: Gartner

For some risks, it will not even matter which function is accountable for each activity, as long as specific accountability is assigned (see "Governance of Third-Party Risk Is Less Complicated Than You Think," on p. 30).

Risk-tailored means the governance model should depend on the risk's speed, the organization's risk tolerance and internal constraints rather than relying on a one-size-fits-all level of scrutiny (such as the centralized oversight of all risks or models based on industry norms). Again, corporate leaders should have the final say here, because the governance model should be determined based on the company strategy. A benefit of placing this authority with senior management rather than the board and the assurance functions is it enables a more rapid response. These top executives can take faster action.

Digital-first means considering digital solutions as you create the governance framework for the risk, not as an afterthought. For instance, if large parts of risk management can be automated, fewer functions need to be involved. Risk and assurance executives we interviewed at a large company put the need for a joint governance, risk and compliance system above the requirements of individual functions that could have delayed or canceled the whole project.

DRG is rare, but some companies practice at least some of its principles. For instance, risk and assurance leaders at one multinational corporation told us they create a different framework for each risk based on its characteristics and make executive management the overall owners of the risk management approach.

DRG Also Improves on Aligned Assurance

DRG also moves beyond and rejuvenates the "aligned assurance" movement for functions like compliance, legal, ERM and quality. Aligned assurance has been touted as a panacea since the growth of new risk and assurance functions (such as privacy) in response to a faster and more complex risk landscape. Because companies established these new teams without a holistic view, the business complained duplicated effort was slowing down its work. The various players recognized the problem and started to focus on how to collaborate. But, as no one was ultimately responsible for pushing those efforts, they have been stuck for a decade.

Increased coordination between those teams is not the right goal, anyway. Improving risk management of the company should be the main objective.

At that, DRG succeeds. We surveyed over 200 organizations and used the results to assess whether traditional or dynamic approaches to risk governance led to better risk management behaviors and better risk outcomes. The presence of each DRG pillar increased the occurrence of high-quality risk management behaviors by 18% to 22% (see Figure 2).

Putting DRG to Work on Pandemic-Driven Risk

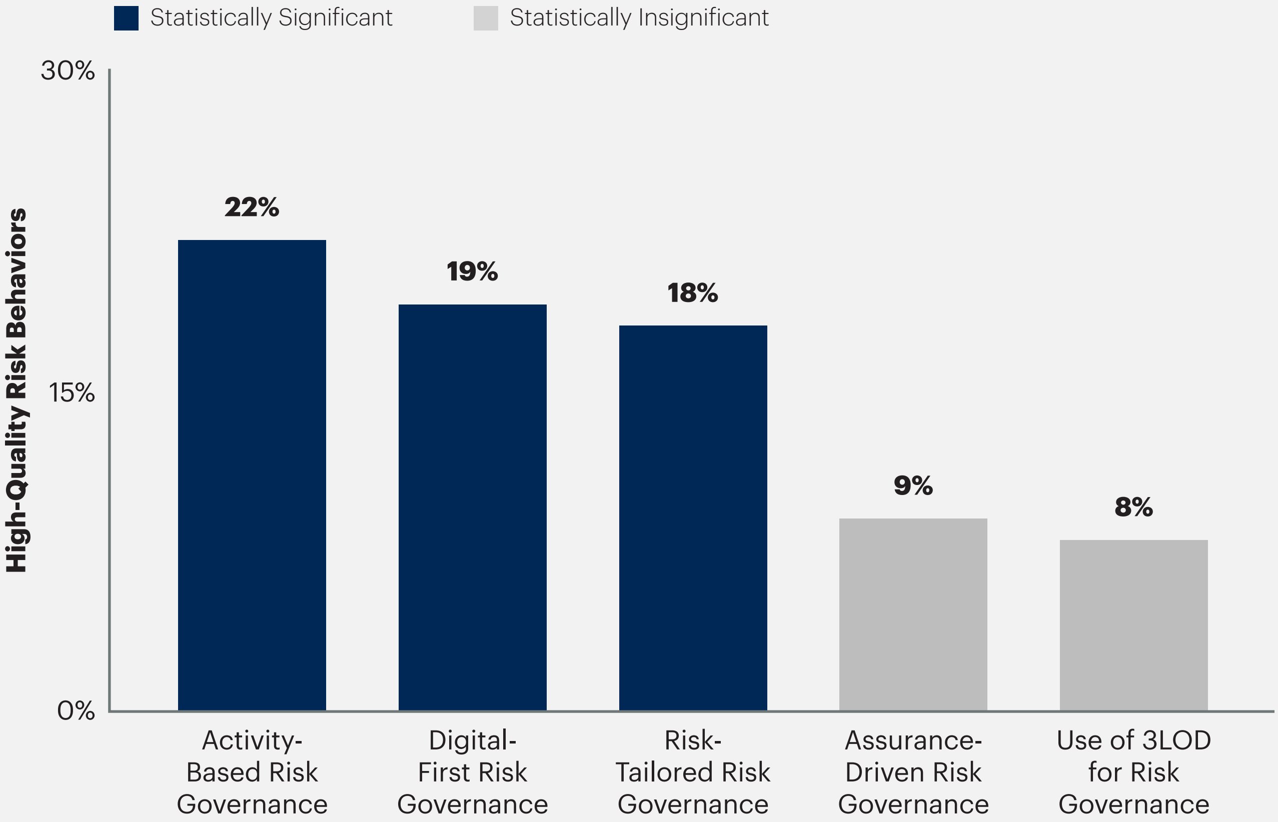
The next step is to learn from the haphazard response to the virus. If the company hasn't already identified one overall senior management owner, it should do so now. That person should define the risk management activities that need to happen immediately and deprioritize those that can wait.

As attention shifts toward recovery and restoration, applying DRG means regularly revisiting whether the risk is governed correctly. Once there is more visibility of the risk path, add more activities (such as a focus on monitoring the risk and assessing its longer-term impact).

Finally, pick a few additional important risks to create a more dynamic framework and prepare for the next crisis, such as another pandemic or climate change. If the board or senior management aren't doing this, suggest they look at the overall level of dynamism in the company's risk governance in relation to its strategy and see how fast they feel comfortable with increasing it.

[1] 2019 Gartner Audit Budget and Headcount

Figure 2: Maximum Impact of Drivers on High-Quality Risk Management Behaviors



n = 217

Source: 2020 Gartner Dynamic Risk Governance Statistical Model (R2=0.275)

Are you confident in your risk assessment?

Gartner's risk assessment tools provide a complete, bottom-up risk identification and prioritization exercise.

Available risk assessment tools include:

- Legal and compliance risk assessment
- Privacy risk assessment
- Fraud risk assessment
- Enterprise risk assessment

Use the risk assessment tools to:

- Get a custom report that can be segmented by BU, geography and employee level
- Identify critical gaps in your risk coverage and strengthen your overall risk management program
- Create actionable guidance for leadership and the board on where to prioritize risk response

Learn More

Contact your account executive or email GartnerBusinessLeaders@gartner.com to get started.

Gartner®

Governance of Third-Party Risk Is Less Complicated Than You Think

by Chris Audet

Third-party risk management is a jerry-rigged affair at the typical corporation. Decentralized and often duplicative processes have grown organically and the resulting gaps in coverage stand out during periods of crisis like the COVID-19 outbreak.

It's only natural to worry; while the corporation races against the virus's impacts, how can functions possibly coordinate efficiently to address interrelated threats? Consider businesses that relied heavily on factories in China for parts and materials. Mounting pressure to maintain output while reducing supply chain costs motivated companies to quickly pursue new strategies in new geographies, with implications far beyond the supply chain function's focus on operational risk. In this circumstance, finance executives must also pivot to a different set of concerns, including the financial health of the new supplier and implementing new payment terms. Legal and compliance teams must concentrate on the risks of bribery and corruption, as well as the environment, health and safety record of the new vendor.

But finding the right path to third-party oversight is less complex than it may appear. The most important step is to name a function — any function — to take primary responsibility for third-party risk management. Only half of organizations have done this, but the other half should.

As long as one function is accountable, we observe a 32% increase in the ability to identify and remediate third-party risk exposure. Leaders often ask us which function is best positioned to take the lead, but they shouldn't worry about that, according to our survey results from more than 11 corporate functions and nearly 1,000 organizations.

No single functional owner improves risk management outcomes in identifying or remediating third-party risk over any other function — not even procurement, supply chain or dedicated third-party risk management teams.

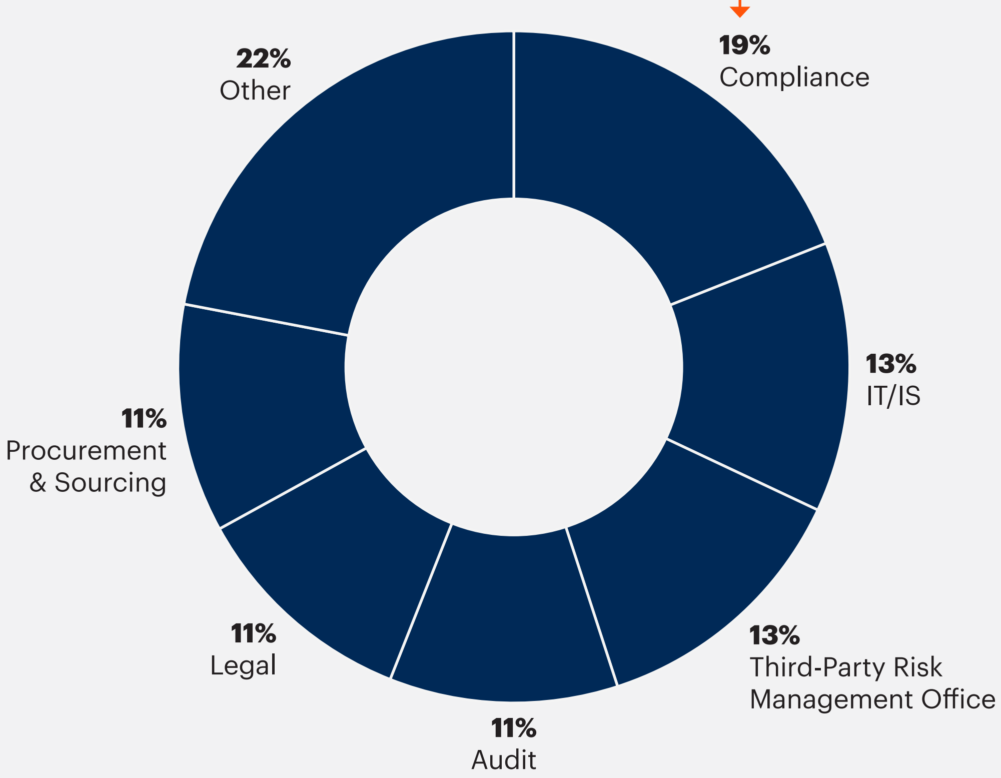
Who Owns Third-Party Risk Management?

Perhaps of greater concern than the 50% who have no named primary owner is the almost one-third of organizations who aren't sure which function plays that role.

The picture is certainly muddy. Compliance is most often the primary owner of third-party risk management activities — at just 19% of organizations, with IT/IS close behind at 13% (see Figure 1). Generally, primary ownership for the management of third-party risk remains spread across functions, including legal, compliance and IT and IS partners.

Figure 1: Primary Owners of Third-Party Risk Management
Percentage of Agreement

Compliance is the most frequently reported primary owner of third-party risk management, owning the process at 19% of organizations.



n = 644
Source: 2019 Gartner Cross-Functional Third-Party Risk Management Survey

Who Conducts Third-Party Risk Activities?

A closer look at specific activities illustrates most companies' fragmentation. No function owns more than one task or process (such as contracting, remediating risk, or recertifying) (see Figure 2). At a plurality of organizations, multiple different functions own discrete activities. This can lead to trouble.

For example, while 29% of IT and IS leaders are involved in sending and collecting third-party questionnaires, only 17% are involved in monitoring and auditing. This suggests those risks attended to by IT and IS leaders at due diligence may not be consistently attended to throughout the third-party relationship.

Don't Spend Time and Effort on Shifting Your Governance Model

In recent months, many executives have told us they're considering the advantages of a central model, which is becoming common in the heavily regulated financial services and pharmaceutical industries. Yet upending governance models may make less difference than once thought. This is good news for organizations looking to improve their third-party risk programs without significant disruption.

We examined four primary risk management governance models, each with varying degrees of functional ownership and centralized oversight:

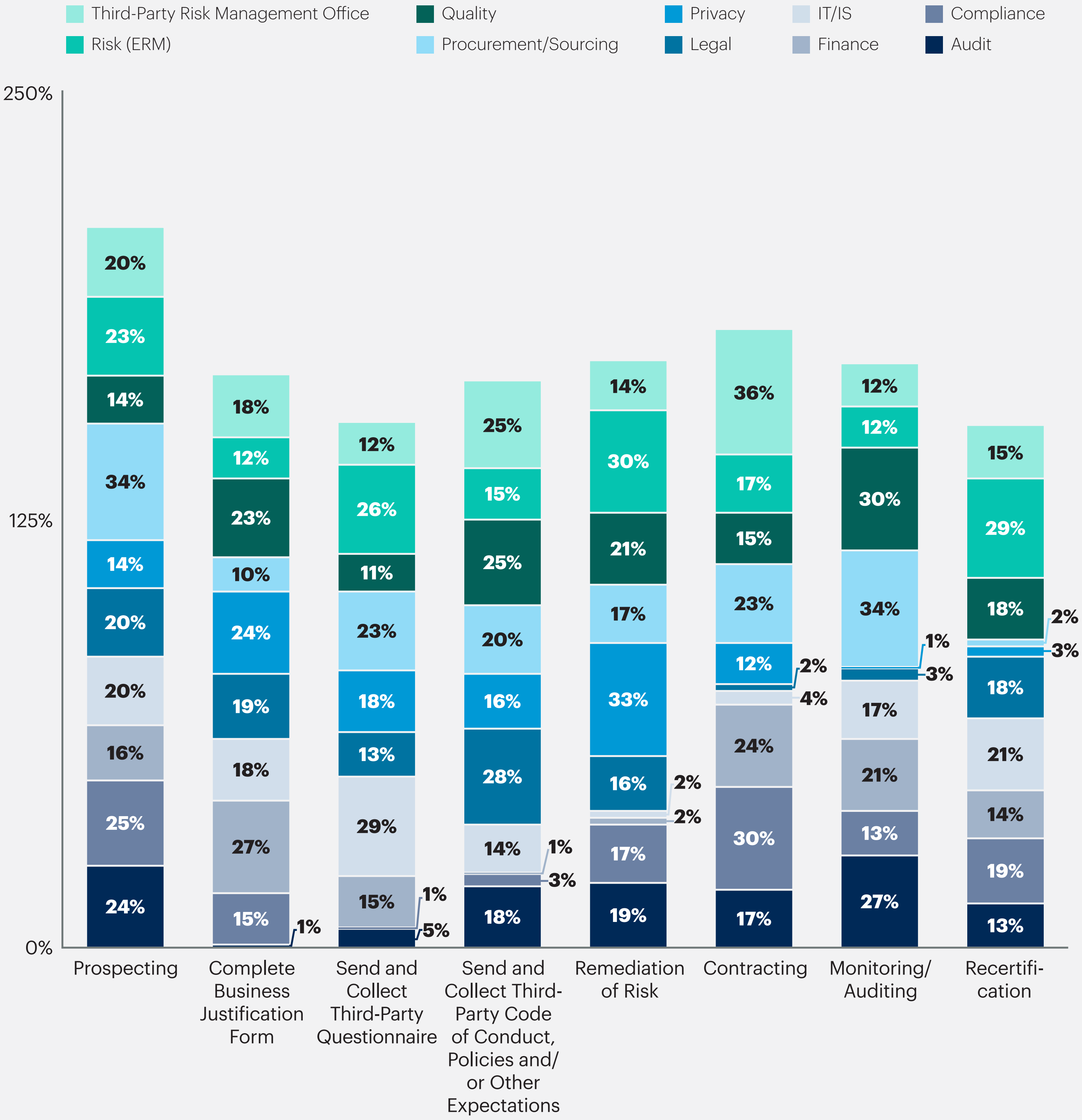
- **Functional model —** In a functional model, individual functions are responsible for specific risk identification. There is some visibility between functions, but little central, enterprisewide visibility. Just over 40% of organizations use this model.
- **Federated model —** In a federated model, there is centralized oversight of third-party risk management activities, with distributed or functional risk identification. Approximately 20% of organizations use this model.
- **Distributed model —** In a distributed model, business lines are responsible for specific risk identification, with little enterprisewide visibility. Just under 20% of organizations use this model.
- **Centralized model —** In a centralized model, there is centralized oversight of third-party risks and centralized risk identification. There is little regular involvement from functions for business units. A little over 15% of organizations use this model.

No single third-party risk management governance model has an outsized impact on risk outcomes. The most important step is to concentrate on naming the primary owner, which is a lighter lift than restructuring the model.

Coming Together to Identify the Best Fit for the Lead Role

Functional leaders can collaborate to identify which of them would be a best fit for the business in the lead coordination role. The named leader would depend upon the kind of work most third parties are completing — for example, are they distributors, agents or simply suppliers? Ultimately, the designation is a CEO-level decision.

Figure 2: Third-Party Activity Ownership



n = 684

Source: 2019 Gartner Cross-Functional Third-Party Risk Management Survey

The Right Way to Engage Customers for Profitable Growth

by Alexandra Bellis

Even before the coronavirus outbreak kept tens of millions inside their homes and forced shoppers online, consumers were happily taking advantage of a disruptive landscape. New competitors, new technology and lower switching costs offer consumers countless brands to discover and limitless opportunities to sift through options. This threat to the era of long-term customer loyalty is a risk for any corporate leader tasked with driving revenue growth. Because customer acquisition costs have risen 50% over the past five years for B2C companies, retention and a greater wallet share are crucial.[1]

The change in habits is well-documented. Sixty-one percent in our recent survey of more than 2,000 consumers stated they enjoyed the process of researching new products and services, while 58% said they loved to seek out new products and services to try. Similarly, nearly half of global consumers told Nielsen they were more likely to try new brands than five years ago and as few as 8% described themselves as firmly committed.[2]

To win out over rivals, companies tend to try three tactics. One is prioritizing frequent contact with customers through ongoing conversations and interactions. This can backfire. Another is improving the customer experience to build satisfaction, which has surprisingly little impact. The third is boosting brand affinity. This can be beneficial but is quite difficult to achieve.

Here's the missing piece. When customers feel in control of their purchase experience and confident in their ability to make good decisions for themselves, they are 42% more likely to purchase additional goods or services. This is true regardless of whether the purchases are cross-sell or upsell, for big-ticket items or low-consideration goods. To build this sense of control, the best companies help them explore options but at the same time keep them within the company's ecosystem. Against the backdrop of a global pandemic and economic shock, seizing any opportunity for repeat business and upsell is even more critical.

Let's walk through the pitfalls of the three conventional efforts. Then we'll explain the more effective method we call bounded exploration and show you how M.M. LaFleur, Hilton and Burt's Bees apply this concept.

Always-On Communication: A Non-Starter

Customers who reported having more contact via email, social media or mobile apps from a company they had previously purchased from were 12% less likely to complete another purchase (see Figure 1). The results here are very clear — increasing the volume of interactions is likely to annoy or overwhelm customers and hurt efforts to increase revenue from them.

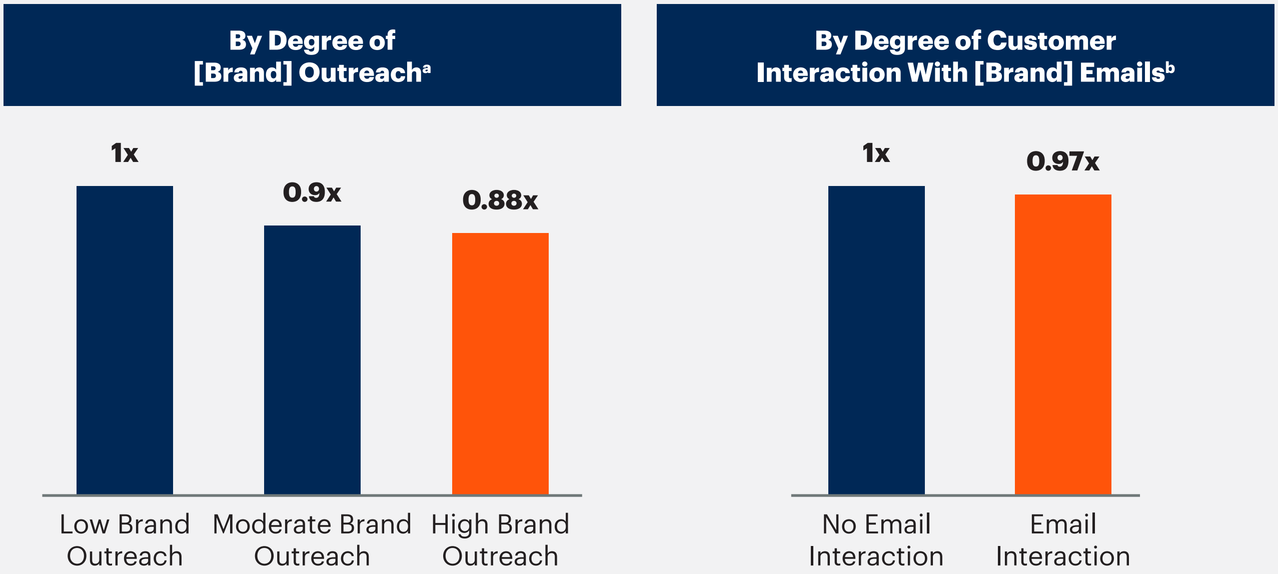
Customer Satisfaction: Taken for Granted

How satisfied a customer is with their overall brand experience — including the products/services, interactions and ease of buying — has no significant impact on their likelihood of completing an additional purchase. Our 2019 survey of B2B customers also showed satisfaction with an existing supplier had no significant effect on incremental account growth.[3]

Why? Because it's not a differentiator. Companies have spent fortunes to improve their Net Promoter scores and drive up customer satisfaction with apparent success. Reported customer satisfaction among our 2020 survey respondents was very high. Only 5% of consumers reported any degree of dissatisfaction with the brand. Therefore, it's time to rethink overinvesting in this area.

Companies still need to work toward achieving a baseline level of customer satisfaction, but once that has been achieved your company is more likely to see a greater return on investment through other engagement tactics.

Figure 1: Impact of Quantity and Quality of Interactions on Purchase Likelihood
Customer Likelihood of Completing a Purchase



n = 2,093 consumers

Source: 2020 Gartner B2C Customer Buying Survey

[a] Multipliers indexed to percentage reporting low brand outreach; [brand] outreach is a summation of the number of reported ways [brand] reached out or interacted with respondents. Sum of outreach is split into three groups — Low: 0-33rd percentile, Moderate: 34th-66th percentile, High: 67th-100th percentile.

[b] Multipliers indexed to percentage reporting no email interaction; email interaction is a summation of the reported types of responses respondents give when they receive an email from [brand]. If a respondent selects one or more response types, they are placed in the "email interaction" group.

Brand Affinity: Limited Opportunity

If higher customer satisfaction is not the answer, then what else? Brand affinity represents the sum of experiences a customer has with your company over time and can be a powerful sentiment with a moderate effect (13%) on additional purchases.

However, brand affinity is an inefficient strategy for driving revenue growth, given the considerable cost, effort and time involved. Success depends on your organization's ability to coordinate effectively across multiple departments and functions to ensure a consistent and positive customer experience throughout a customer's lifetime. This is an incredibly high bar to achieve.

If this does not sound daunting enough, only 21% of customers who currently do not feel a personal connection to the brand they purchased from believe it is important to have one at all.

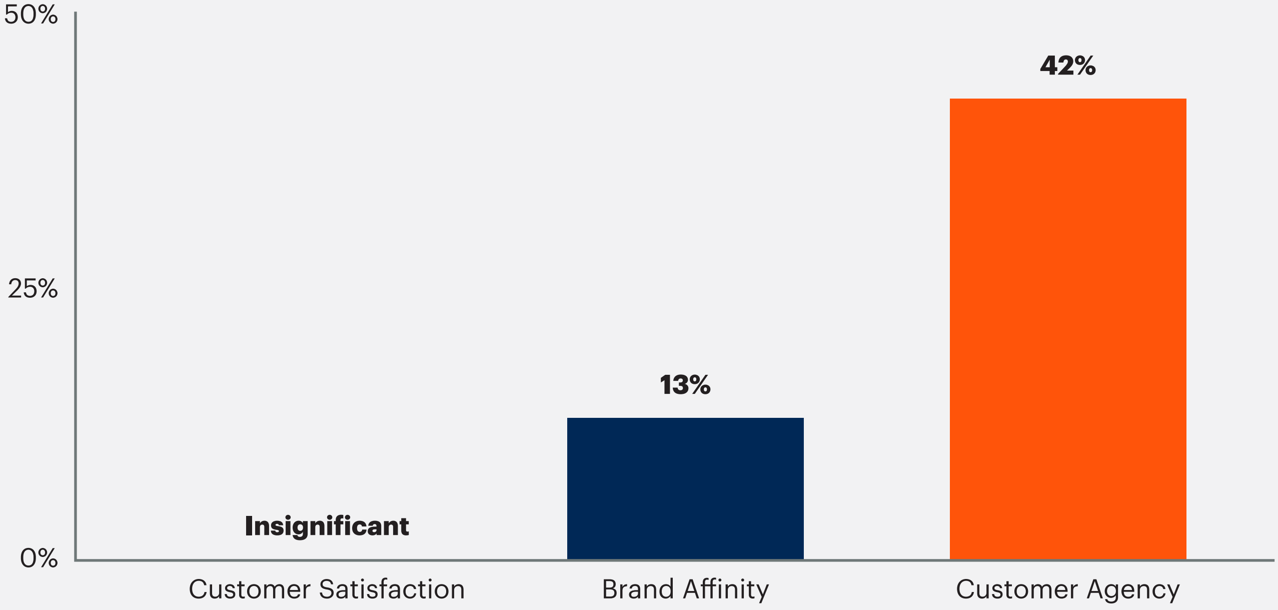
Feeling in Control: High Impact

The most consistent and predictable driver of a customer's likelihood to complete a purchase is their sense of agency — the degree to which they feel equipped to plan, evaluate and manage purchase outcomes (see Figure 2).

If customers want to feel in control, then companies that want to win the battle for customers' pockets must find ways to enable feelings of agency. To do this, corporate leaders must embrace and support customers' current exploration efforts. Engagement efforts should center on building an experience with these two components:

- Create the perception for customers that they have the freedom to explore and have fully examined all possible solutions.
- Keep customers relatively contained within the company's ecosystem to reduce the risk that they will buy from a competitor or abandon the purchase because they feel overwhelmed by too many choices.

Figure 2: Impact of Customer Agency, Brand Affinity and Customer Satisfaction on Purchase Likelihood



n = 2,093 consumers

Source: 2020 Gartner B2C Customer Buying Survey

Note: Model controls for respondent age, gender, nation of residence, education, employment status, category of product/service considered, degree of anxiety, top of mind, customer confidence in decision making (insignificant), income. Classification accuracy = 74.1%.

> Exploration should let customers feel they've arrived at their own decision without being overwhelmed by too much information.

Invest in Tools for Customers to Explore Without Letting Them Stray

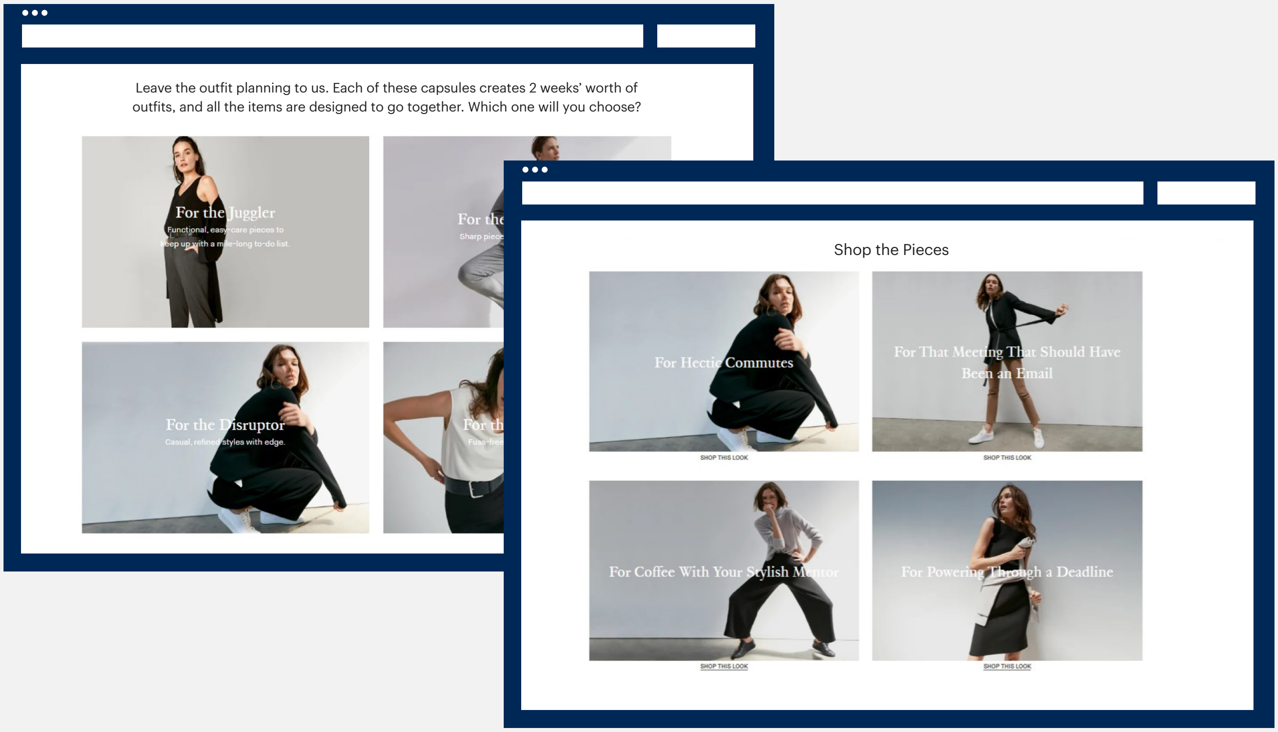
Corporate leaders responsible for customer-facing functions should lead the charge in designing customer experiences that enable exploration on their website, via mobile apps or on social media. Specifically, exploration should let customers feel they've arrived at their own decision without being overwhelmed by too much information.

Offer customers a series of logical and manageable choices as they move toward a relevant goal. Along the way, diverse viewpoints and reassuring messages help customers feel capable and confident. Ensure all of these milestones are set within logical boundaries that keep the customer within the brand's digital universe. Some companies are already doing this and there is a lot you can learn by following these examples.

M.M. LaFleur gives customers the opportunity to explore "capsule wardrobes" on its website. These are curated looks that customers can select based on their mood. Whether customers want to be "disruptive" or "power players," they can explore outfits and options within a contained experience — giving them control while keeping them on the brand's website (see Figure 3).

Similarly, Hilton's website and mobile app experience enables customers' vacation planning. Hilton customers can explore

Figure 3: M.M. LaFleur's Omakase Capsule Wardrobe



Leave the outfit planning to us. Each of these capsules creates 2 weeks' worth of outfits, and all the items are designed to go together. Which one will you choose?

For the Juggler
Functional, easy-care pieces to keep up with a mile-long to-do list.
For the
Sharp piece
For the Disruptor
Casual, refined styles with edge.
For th
Fuss-free
Shop the Pieces
For Hectic Commutes
SHOP THIS LOOK
For That Meeting That Should Have Been an Email
SHOP THIS LOOK
For Coffee With Your Stylish Mentor
SHOP THIS LOOK
For Powering Through a Deadline
SHOP THIS LOOK

Source: M.M. LaFleur

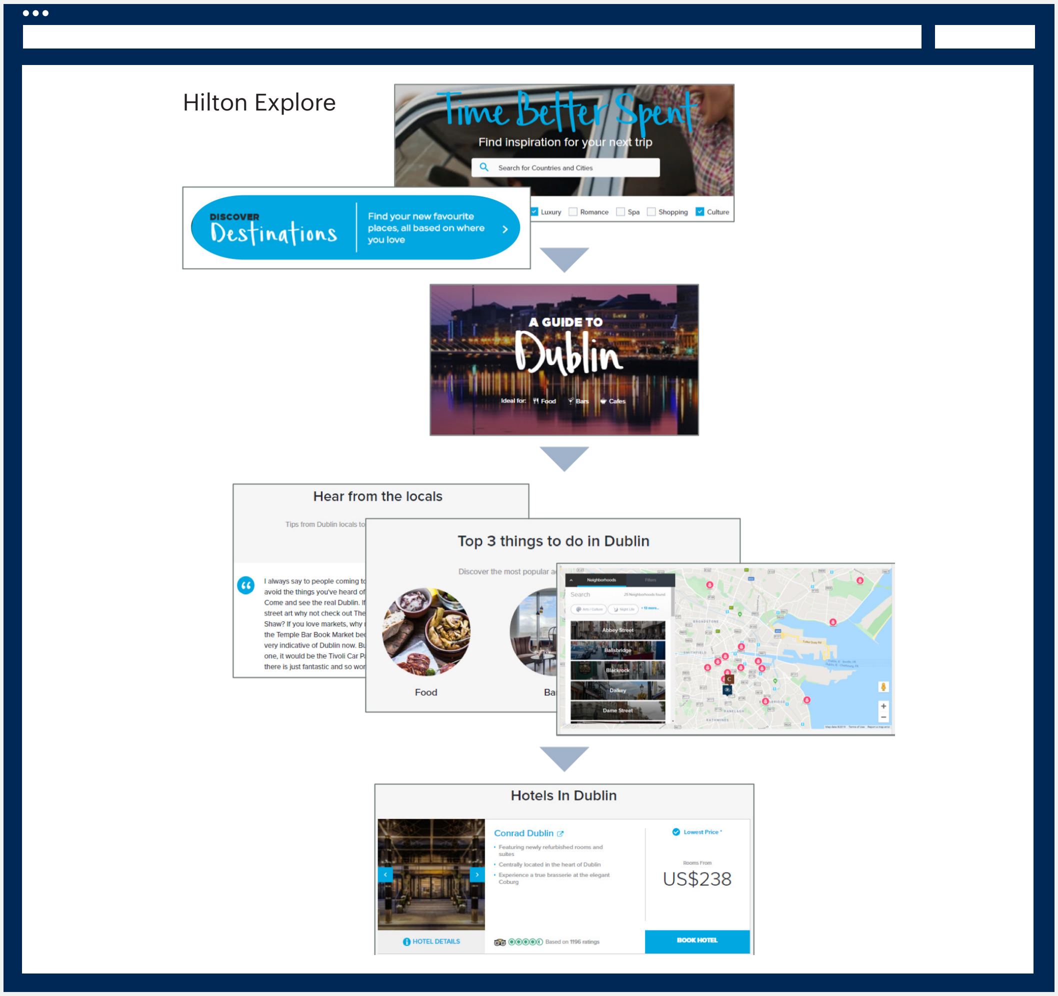
destinations, activities and hotels on their own but do so within the brand's ecosystem while being guided toward a hotel. Hilton even includes information from third parties to help customers make better decisions and keep them from straying (see Figure 4).

Finally, Burt's Bees uses its social media and website experiences to help customers explore makeup and skin care products. Starting on social media, customers can find examples of others who look like them to find choices that might fit their needs. Customers can then use tools on the brand's website to get recommendations to complete their desired makeup look (see Figure 5).

To get your organization ready, corporate leaders need to understand their customers' needs and concerns and recognize these efforts must be a company priority. Finance leaders should start by funding projects to enhance understanding of how a customer seeks choices and information. Look for projects that involve gathering data directly from your customers about their experiences and decision-making processes. This will allow your organization to identify typical customer goals and questions and map them onto customers' purchase journeys.

Then, finance leaders should support retention efforts. Business cases from marketing leaders should clearly denote how much projected

Figure 4: Hilton's Explore Experience



I always say to people coming to
avoid the things you've heard of
Come and see the real Dublin. If
street art why not check out The
Shaw? If you love markets, why
the Temple Bar Book Market be
very indicative of Dublin now. Bu
one, it would be the Tivoli Car P
there is just fantastic and so wo

- Featuring newly refurbished rooms and suites
- Centrally located in the heart of Dublin
- Experience a true brasserie at the elegant Coburg

Based on 1196 ratings

Source: Hilton

growth derives from repeat customers versus new customers. Pay particular attention to projects that target improvements in the digital customer experience and ask whether these efforts will improve the productivity of customer exploration and streamline the buying experience.

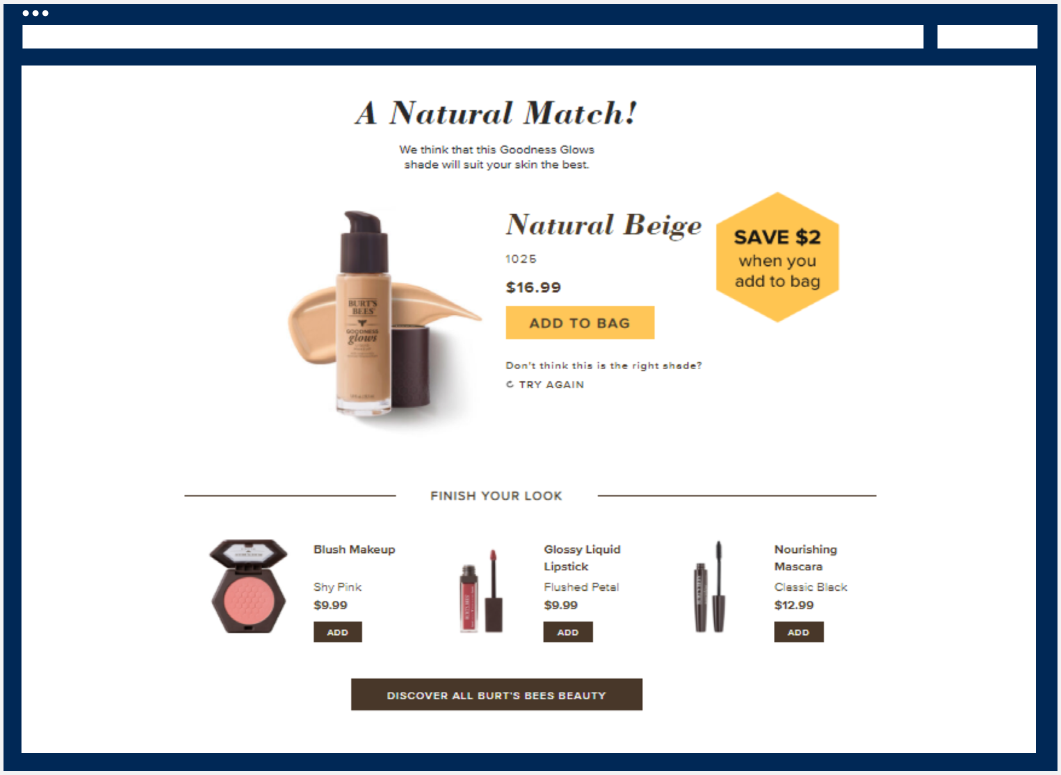
This may seem like an expensive effort. Fortunately, it is not radically different from what many organizations already do. Your organization is probably already investing in customer data and building customer journey maps. It also likely has existing projects and marketing content that can be adapted to enable exploration. It just requires refocusing efforts on learning about your customers; all business leaders should understand the full context of their purchase decisions. Start thinking like your customers instead of about them and you can hold them closer.

[1] "Is Content Marketing Dead? Here's Some Data," ProfitWell.

[2] "Consumer Disloyalty is the New Normal," Nielsen.

[3] 2019 Gartner Account Growth Buyer Survey

Figure 5: Burt's Bees' Foundation Shade Finder Tool



A Natural Match!

We think that this Goodness Glows shade will suit your skin the best.

Natural Beige

1025

$16.99

Don't think this is the right shade?

Source: Burt's Bees

Bring in the Business: How to Prioritize the Right Emerging Risks

by Sam Abrams

Executives take action on emerging risks when it's clear they pose a real threat to the company. But how do you figure out which ones those are and get buy-in from the business on those choices?

The answer is to include the relevant stakeholders in the selection process. ERM leaders should hold workshops with business unit leaders to identify emerging risks to prioritize and reach consensus on how they will impact the organization's bottom line. With a shortlist of risks that have been validated by the business, assurance leaders will be able to prepare their company to mitigate them effectively.

This is a two-part process. Risk leaders first narrow the universe of threats and then meet with appropriate colleagues to decide which ones to prioritize and to validate their business implications.

Emerging Risk List Selection

Risk management leaders can use our Emerging Risk Prioritization Tool (ERPT) to create a custom-made list for their organization from a database of 60 risk options. The risks are split evenly into four categories — economic/societal, geopolitical/regulatory, technological and environmental/biological.

Users select risks that satisfy two simple criteria:

1. Potential for significant impact on the enterprise
2. Potential for that risk to manifest in the next one to five years

From September 2019 through February 2020 nearly 100 ERM leaders used the tool. Collectively, they selected cybercrime, aging population and extreme weather events as the top emerging risks. The data reflects input from a broad swath of industries, including financial services, healthcare, government and energy (see Figure 1).

When 41 of these ERM leaders worked with the business to rank the risks (more about that process below), an economic downturn came out on top. Though they did not predict the pandemic, this data does show involving the business helped to identify and validate a threat that has become a reality.

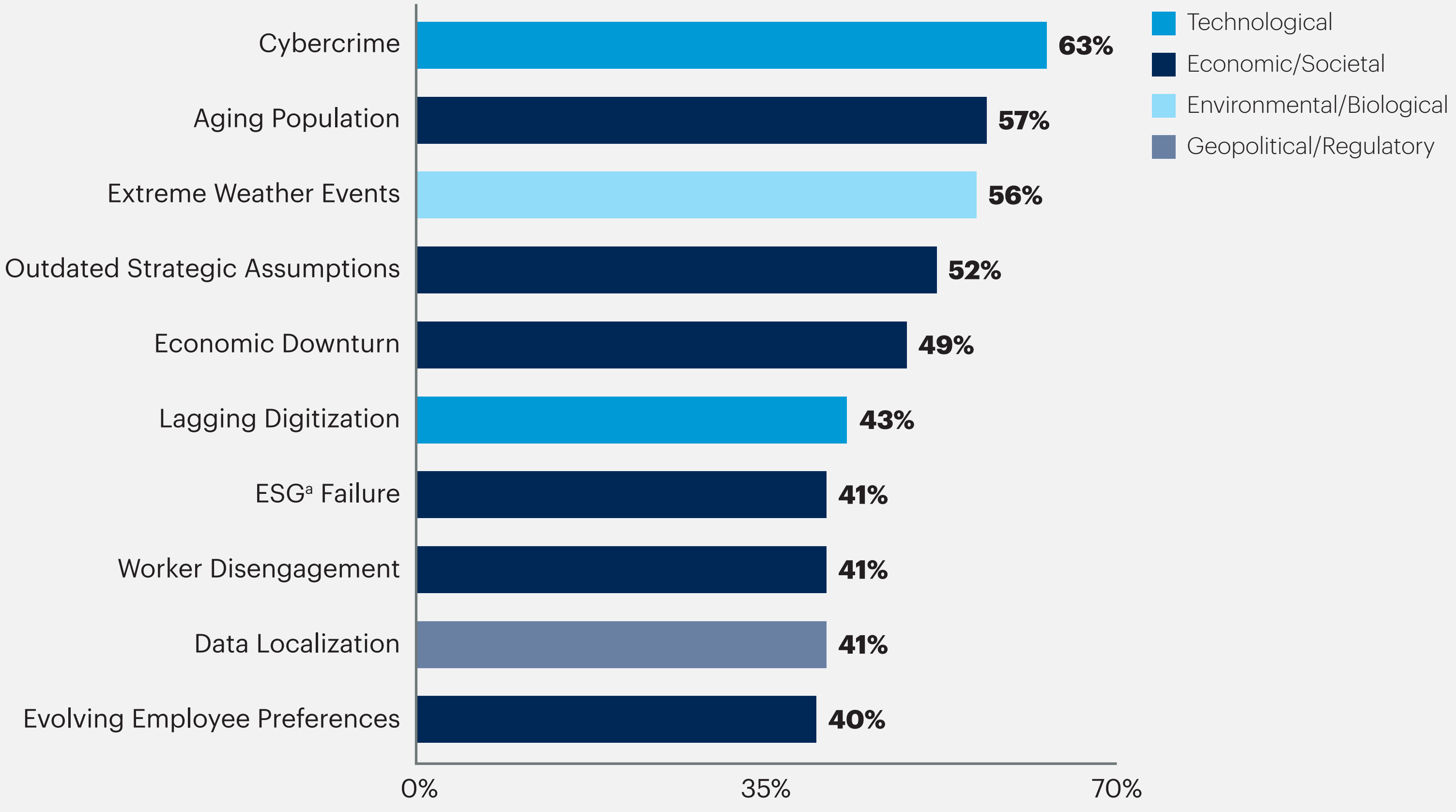
Emerging Risk Prioritization and Validation

Selecting an emerging risk list is a necessary step to effectively manage threats, but not a sufficient one. Presenting a list of unranked emerging risks to executive stakeholders won't drive action. Executives find this information interesting, but difficult to use when making business decisions. Similarly, presenting an emerging risk list ranked by traditional metrics leads to a pressure-testing discussion focused on how ERM arrived at those scores, and not on the risks themselves. To help executives act, ERM should provide a prioritized view of the emerging risk environment based on specific potential consequences for the business.

How to Bring the Business Into the Prioritization Process

For each emerging risk on its list, ERM selects several potential business consequences. The ERPT provides three generic business implications for each of the 60 available emerging risks. ERM then facilitates a workshop with risk liaisons, enterprise risk owners or frontline managers. Participants are chosen for their combination of fundamental risk

Figure 1: Top 10 Selected Emerging Risks



n = 91

Source: Gartner ERPT (September 2019 through February 2020)

[a] Environmental, social and corporate governance

management knowledge and familiarity with day-to-day business operations. ERM separates workshop participants into small groups and presents them with a full emerging risk list. Each group ranks the top five emerging risks using the same criteria employed earlier by ERM: their potential for significant impact on the enterprise and for that risk to manifest in the next five years.

After determining their own top five, each group decides which of the business implications proposed by ERM are most valid. If they don't think any are valid, participants share their subject matter expertise and suggest a new implication. ERM then records the top five emerging risks from each group and holds a collective discussion until everyone agrees on a top five overall.

After reaching consensus, ERM can present executives with a priority list of emerging risks vetted by risk owners who have subject matter expertise and frontline experience. ERM leaders earn credibility and position themselves to help their companies by providing executives this shortlist.

Alternative Method: Instead of facilitating an in-person prioritization workshop, create a simple online survey. Use participant responses to quickly determine the top five emerging risks and validate the business implications of those risks. Make sure to leave an option to create a custom business implication should participants find those provided unsatisfactory.

Out of the 91 ERM leaders who used our tool, 41 went on to facilitate a workshop with their colleagues in the business. Collectively, business stakeholders and assurance leaders were most likely to validate an economic downturn and aging population as the top emerging risks (see Figure 2).

The true value of the workshop lies in pinpointing the business areas most likely to be impacted by an emerging risk. For example, ERM at a multinational manufacturer proposed three potential business implications for the risks

Figure 2: Top 5 Business-Validated Emerging Risks

Emerging Risk	Rate Validated in Top 5
Economic Downturn	41%
Aging Population	39%
Cybercrime	32%
Outdated Strategic Assumptions	29%
Volatile Oil Prices	29%

n = 41
Source: Gartner ERPT

associated with Brexit aftershocks. The first two implications were validated by workshop participants, but the third was rejected (see Figure 3).

The company's ERM function now knows to focus its monitoring and mitigation planning on supply chain and data privacy and not on talent.

As a result of the emerging risk prioritization workshop, ERM can report the following to executives:

1. This risk has the potential to significantly impact our business.
2. This risk has the potential to impact our business in the next one to five years.
3. This risk is a top-five emerging threat to our company.
4. This risk will impact the core functions of supply chain and data privacy.
5. Items 1 to 4 have been validated by risk managers and subject matter experts at the front line.

The benefits of this prioritized approach are clear. The likelihood of executives taking timely action on emerging risks jumps from 3% when presented with an unranked list to 67% when presenting a prioritized subset of risks with specific business implications.[1] By increasing the business relevance of its emerging risk information and decreasing the quantity of risks presented, ERM can shift the emerging risk conversation from information sharing to decision making.

To create your own prioritized list of emerging risks and business implications, use our Emerging Risk Prioritization Tool.

[1] 2019 Gartner Emerging Risks Action Model

Figure 3: Business Implication Validation or Rejection

Emerging Risk	Business Implications
Brexit Aftershocks	• Drafting of the U.K.'s new trade deal with the EU could suffer significant delays, leaving businesses in a state of continued uncertainty in setting new supply chains and product licensing. ✓ Validated • Risks and costs for collecting, storing and sharing data could rise due to uncertainty over the U.K.'s status in relation to GDPR in the EU. ✓ Validated • Difficulties in navigating employment laws in the post-Brexit U.K. could force the company to rethink its talent strategy and/or invest more in mainland European real estate and talent. ✗ Rejected

Source: ERPT — data from multinational manufacturer

Craft a fair deal with Gartner BuySmart™

In this time of unprecedented disruption, business leaders need to drive efficiencies and optimize spend. Using the most recent insights on technology spend management, contracting practices and long-term risk mitigation, BuySmart™ helps you reduce costs and avoid common pitfalls through the entire technology buying life cycle.

Buy technology with confidence

- Determine what you really need to meet business outcomes.
- Pick the right provider.
- Align deal structures with business needs.
- Optimize spend.
- Reduce complexity and risks.

Contact your Gartner representative to learn more about BuySmart™

Go to: gartner.com/en/products/buysmart

Gartner®