CULTIVATING TRUST TO GAIN COMPETITIVE ADVANTAGE

How to Rebuild Confidence in the Way Business Is Done

Trust Is a Cornerstone of the Digital Era

DR. RICHARD FORD
CHIEF SCIENTIST
FORCEPOINT

In the digital era, fast-paced, hypercompetitive business environments reward those who are quick to respond to new opportunities and market challenges. Trust plays a vital role in the success of these initiatives, providing a cornerstone for building strategic partnerships, establishing a reputation, embracing digital transformation, and more. Today, this once-stable foundation is crumbling under the pressure of large-scale data breaches faced en masse by organizations in every industry, and we're quickly losing our footing.

This sobering trend is made apparent in this new survey conducted by Harvard Business Review Analytic Services, in which nearly two-thirds (63%) of senior executives at large enterprises throughout the world stated that trust among people, businesses, and institutions has declined over the past two years. What's even more telling is that a large majority (88%) named large-scale cybersecurity exploits as a significant contributor to that decline.

These findings clearly show that, over time, data breaches and data loss-related incidents have chipped away at the confidence of investors, partners, and customers alike. In partnering with Harvard Business Review Analytic Services, we wanted to understand how this might be turned around, and what tools and technology have the greatest impact on promoting trust externally—with customers and partners—and internally among business units and staff.

In the end, we uncovered a small but effective group of "trust leaders"—companies that are reaping significant ROI from their trust-related investments and policies.

Research shows that, in order to preserve institutional trust, leader organizations focus on the following:

Adopting cybersecurity technology that assesses behavior to quickly identify potential problems before they can cause harm. Leaders are implementing technology tools that facilitate real-time risk monitoring and enable automated system interventions when anomalous behavior is detected.

These integrated, analytics-driven solutions are not only easier to manage than traditional security approaches but less cumbersome to the end user, specifically designed to protect an increasingly remote workforce and follow data as it leaves the confines of the enterprise. It's no surprise that 60% of leader organizations plan to automate cybersecurity trust management based on real-time human behavior.

Understanding what contributes to trust in today's interconnected business environment. Leaders demand greater assurances than their peers do, prioritizing their partners' data security and privacy policies and selecting partners with governance, risk management, and compliance processes that are aligned with their own, rather than focusing solely on previous dealings and direct relationships. The business landscape is more interdependent today than ever before—accountability is paramount now that data and systems are so widely shared.

Adopting a culture of trust to promote internal collaboration and foster innovation. Trust is essential for high levels of collaboration and innovation. To reduce risk and enhance trust, leaders are crafting comprehensive strategies with policies that cross departmental boundaries. Addressing cyber risk while preserving trust requires alignment between management and stakeholders from all areas of the organization, including those from compliance, human relations, communications, and legal.

Trust must be reprioritized to cultivate the robust and secure environment necessary for companies to thrive in today's digital marketplace. We at Forcepoint see behavior-based, analytics-driven cybersecurity solutions as the tip of the spear, allowing organizations to better quantify and adapt to risk in real time in a way that is far less cumbersome and invasive to end users. It starts small—understanding each person's behavior as they interact with critical data—but in the grand scheme of things, what we call a "human-centric" approach to cybersecurity has the potential to change the trust landscape forever.

CULTIVATING TRUST TO GAIN COMPETITIVE ADVANTAGE
How to Rebuild Confidence in the Way Business Is Done

Business was once done on a handshake, with your word being your bond, but in today's digital-centric world, trust is becoming scarce. This sobering trend became apparent in a new survey conducted by Harvard Business Review Analytic Services, which found that nearly two-thirds (63%) of senior executives at large enterprises throughout the world say trust among people, businesses, and institutions has declined over the past two years. What's more, nearly a quarter (23%) of the respondents describe the decline as being significant. FIGURE 1

What's eroding trust in our personal and professional lives? A new answer surfaces almost every day: opinions and outright falsehoods taint stories presented as containing factual reporting on social media sites as homeowners receive foreclosure notices from financial services companies that later reveal their decisions were based on erroneous data. Cathay Pacific, one of the world's leading airlines, and other recognizable brands like Yahoo!, report massive security breaches that give hackers access to sensitive information that customers entrusted to familiar vendors. In addition, sophisticated phishing techniques enable hackers to compromise corporate credentials and pass themselves off as trusted employees and business partners to undermine trust in internal systems and stakeholders. Breakdowns like these are clearly on the minds of top global executives. Eighty-eight percent of the respondents to the survey name large-scale cybersecurity exploits that expose corporate or personal data as a significant contributor to the decline in trust.

For businesses, the breakdown of trust can have severe consequences. A company's market value may fall by more than $1 billion when cyber thieves steal customer financial data, a report by a group of world economists concludes.[1] Similarly, data losses can slow sales growth by more than 3%, according to the same study.

On the flip side, companies that maintain and enhance their reputations for trustworthiness will increasingly gain an edge over competitors. More than half of all global executives say being seen by customers as trustworthy gives them a market advantage over competitors and contributes to higher productivity in internal operations.

HIGHLIGHTS

63%
OF SENIOR EXECUTIVES AT LARGE ENTERPRISES THROUGHOUT THE WORLD SAY TRUST AMONG PEOPLE, BUSINESSES, AND INSTITUTIONS HAS DECLINED OVER THE PAST TWO YEARS.

88%
OF EXECUTIVES NAME LARGE-SCALE CYBERSECURITY EXPLOITS THAT EXPOSE CORPORATE OR PERSONAL DATA AS A SIGNIFICANT CONTRIBUTOR TO THE DECLINE IN TRUST.
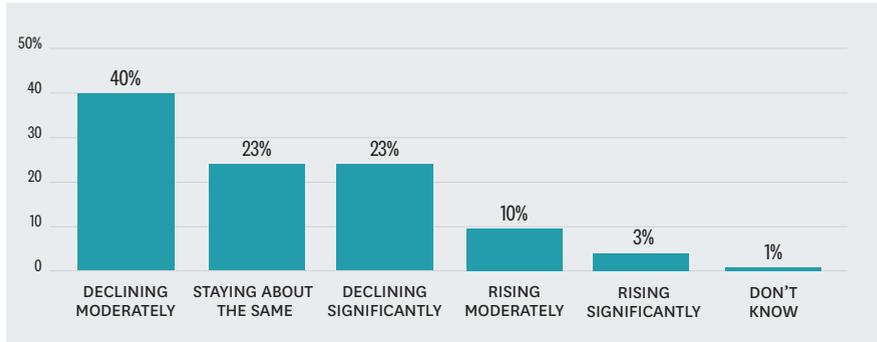
85%
OF EXECUTIVES FROM COMPANIES WITH MATURE TRUST POLICIES AND PRACTICES CITE TRUST AS A NECESSARY PRECONDITION FOR COLLABORATION AND INNOVATION.

FIGURE 1

TRUST IN PERSONAL AND PROFESSIONAL RELATIONSHIPS IS DECLINING

Respondents stating the level of trust rising or declining in professional relationships

40%	23%	23%	10%	3%	1%
DECLINING MODERATELY	STAYING ABOUT THE SAME	DECLINING SIGNIFICANTLY	RISING MODERATELY	RISING SIGNIFICANTLY	DON'T KNOW

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

HOW WE IDENTIFIED TRUST LEADERS

All corporations claim to be confident about the degree to which their organization is a trust-based one, both in terms of how it's perceived externally and in terms of the strength of internal, trust-based relationships. But few can measure this trust and back up their claims. In fact, just 9% of executives say their organizations are currently able to accurately measure the value of trust for their businesses. After correlating this segment with high levels of performance in other key areas, such as the C-suite's commitment to trust, this group distinguished itself as leaders in business trust.

DON'T KNOW

LEADERS
Strongly agree

9%

8%

39%

44%

LAGGARDS
Disagree

FOLLOWERS
Neutral/somewhat agree

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

"As more data breaches and other threats arise, trust will become a significant competitive advantage, similar to how a solid credit rating is a business benefit," says Stuart Russell, senior director of customer systems based at the London office of the global publisher McGraw-Hill. "Companies that haven't been investing in resources that foster trust will find it much more difficult to succeed in the future."
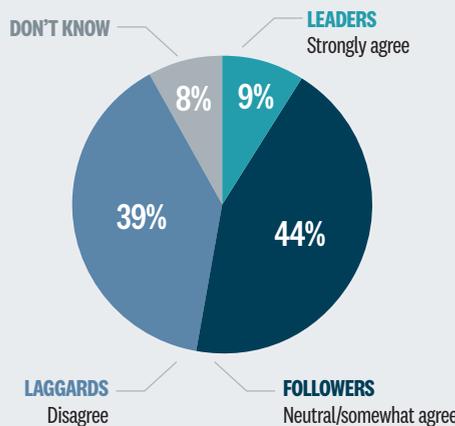
What resources will have the greatest impact on promoting trust externally, with customers and partners, and internally among business units and staff? Some leading executives are finding effective ways to answer that question, according to the Harvard Business Review Analytic Services survey. The research identified a small but effective group of companies that are reaping significant benefits from their trust-related investments and policies. In turn, these leaders offer a model for others that want to develop a modern approach to promoting greater external and internal trust. This approach applies a handful of core elements as a foundation:

- Ongoing relationships remain essential for assessing trust, but today's dynamic business environment requires additional measures for vetting and monitoring trustworthiness.

- Digital entities and people must continuously earn trust based on prevailing behavior.

- Leading organizations are implementing digital tools to detect and respond to anomalous behavior that threatens sensitive data, intellectual property, and critical systems.

- To bolster trust in internal and external people and systems, cybersecurity investments must go beyond traditional perimeter-protection technologies.

This report explores why trust is vital for success in today's global economy and the forces that undermine trust among companies and their customers, partners, and employees. In addition, this analysis will describe the new technologies and policies trust leaders

are adopting to achieve their elite status and then promote their reputations for trustworthiness to the marketplace.

Trust and Business Success

Trust is vital for global businesses in the age of digital transformation. So-called trust platforms, such as Airbnb and eBay, attempt to create low-risk environments that encourage strangers to come together to conduct financial transactions for goods and services. The influence of these online interactions has quickly spread to more venerable industries so that consumers and business partners routinely use digital platforms to purchase retail goods, obtain life insurance, manage supply chains, and perform myriad other activities. While digital transformation has created new and innovative business models and opened additional revenue streams, it also creates new risks. Over time, for example, ongoing reports of large-scale cybersecurity breaches and misuse of data may cause consumers and business partners to balk at sharing sensitive information, threatening the success of business models built on capturing, analyzing, and acting on client data.

Looking beyond the latest headlines, the survey identified many reasons why business trust has eroded in recent years. Two of the top three trust busters relate to the misuse of data by organizations, by intentionally or carelessly mismanaging the sensitive information that clients entrusted to them. Numerous examples of these breakdowns have come to light in recent months. For example, a news report at the end of 2018 revealed that Facebook gave select business partners special access to its members' messages, online viewing habits, and lists of friends, all without disclosing these practices to consumers.[2] Trust also takes a hit when well-known companies intentionally fudge facts, as when engineers at Volkswagen rigged cars with software that altered performance data in order to pass emissions tests.[3] FIGURE 2

Also ranking high are cybersecurity breaches, with 88% of respondents saying large-scale cybersecurity breaches and vulnerabilities that exposed corporate or personal data contribute to declining trust. That high percentage isn't surprising given the mound of evidence to fuel mistrust: nearly 179 million records were exposed in the U.S. alone in 2017, many resulting from the 1,579 cyber breaches that occurred that year. FIGURE 2
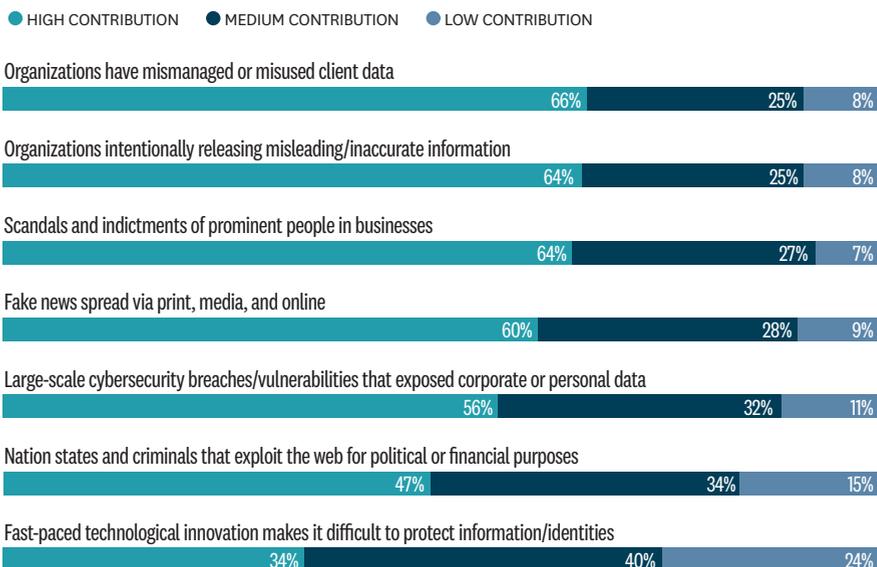
But outside forces aren't the only assaults on business trust—problems also result from missteps within organizations, starting at the top. The survey found that only half of C-suites are aware of and are actively encouraging trustworthy behavior. Even more worrisome is the fact that a third of them are doing nothing about it. This lack of senior-level involvement in promoting policies designed to advance and preserve trust may communicate, intentionally or not, that this isn't a high priority for the organization. FIGURE 3

TRUST PLATFORMS ATTEMPT TO CREATE LOW-RISK ENVIRONMENTS THAT ENCOURAGE STRANGERS TO COME TOGETHER TO CONDUCT FINANCIAL TRANSACTIONS FOR GOODS AND SERVICES.

FIGURE 2

MISMANAGED DATA IS A PRIME TRUST BUSTER

Organizational misuse of data accounts for two of top three trust decline factors

● HIGH CONTRIBUTION ● MEDIUM CONTRIBUTION ● LOW CONTRIBUTION

Organizations have mismanaged or misused client data
66% | 25% | 8%

Organizations intentionally releasing misleading/inaccurate information
64% | 25% | 8%

Scandals and indictments of prominent people in businesses
64% | 27% | 7%

Fake news spread via print, media, and online
60% | 28% | 9%

Large-scale cybersecurity breaches/vulnerabilities that exposed corporate or personal data
56% | 32% | 11%

Nation states and criminals that exploit the web for political or financial purposes
47% | 34% | 15%

Fast-paced technological innovation makes it difficult to protect information/identities
34% | 40% | 24%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

This executive abdication may help explain why employees at a large U.S. bank padded sales figures by creating millions of accounts without their clients' consent. "There aren't formal meetings where people get together to plan violations like these," says Robert Hurley, a Fordham University professor specializing in leadership and management and author of the book *The Decision to Trust: How Leaders Create High-Trust Organizations*. "Problems happen because of 'organizational drift' when capital-market-based exogenous pressures, myopic short-term incentives, aggressive goal setting, and constraints on legitimate organizational capabilities combine with self-interested behavior

and failure of moral agency among senior executives. This causes rogue microcultures to develop and pursue strategies that are at odds with espoused cultural values. These microcultures nudge behavior and culture toward unethical actions that serve the interests of powerful people at the expense of weaker stakeholders. The result is often shocking violations of trust that leave stakeholders and regulators asking, 'How could this have happened?'"

As organizational drift occurs, he adds, the normal countervailing forces charged with governance are weakened, and drift continues because it serves the powerful microculture's interests. "But it's the job of the board to do more," Hurley says. "It must ensure that the achievement of aggressive goals happens without crossing ethical lines. This requires metrics that measure stakeholder trust and the trustworthiness of the organization in deep ways. Then the company must undertake continuous improvement. Boards need to understand that, like people, organizations are at risk of moving down a slippery slope to gain short-term benefit at the expense of long-term reputation. Boards need to lead a process of meaningful improvement in organizational trustworthiness year in and year out if they want to achieve both financial and reputational results."
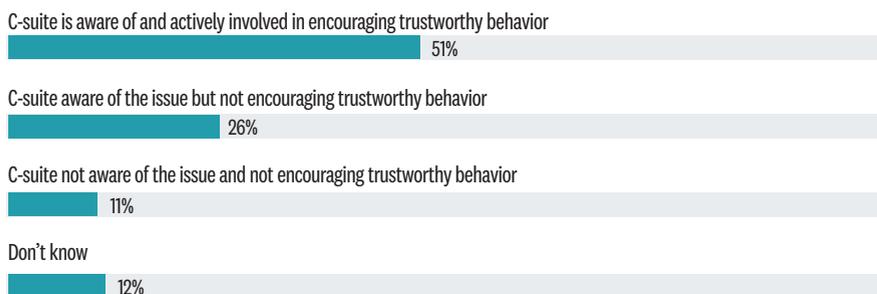
Trust as a Business Driver

Although the survey didn't find a direct correlation between revenue growth and the ability to quantify trust, it determined that trust plays a vital role in business success. For example, companies that lagged competitors in trustworthiness also were more likely to have posted flat or declining revenues over the past two years. In addition, 85% of leaders—the select group of executives from companies with the most mature trust practices—cited trust as a necessary precondition for collaboration and innovation. These are two essential factors that help ensure companies stay competitive in a volatile business world that rewards quick responses

FIGURE 3

C-SUITES NEED TO STEP UP

A third of C-suites are not encouraging trustworthy behavior

C-suite is aware of and actively involved in encouraging trustworthy behavior
51%

C-suite aware of the issue but not encouraging trustworthy behavior
26%

C-suite not aware of the issue and not encouraging trustworthy behavior
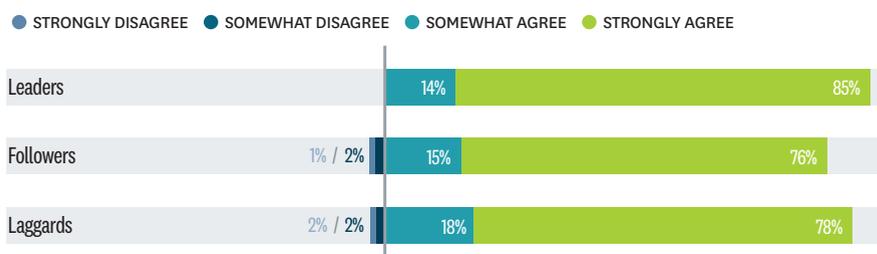11%

Don't know
12%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

FIGURE 4

TRUST FUELS INNOVATION

Respondents stating "Trust is a necessary precondition for collaboration and innovation"

● STRONGLY DISAGREE   ● SOMEWHAT DISAGREE   ● SOMEWHAT AGREE   ● STRONGLY AGREE

Leaders		14%	85%
Followers	1% / 2%	15%	76%
Laggards	2% / 2%	18%	78%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

to new opportunities and market challenges.

Companies with strong safeguards for protecting client data understand the competitive implications. "We see in news reports how data breaches have impacted trust, so UPS is vigilant in our data protection efforts to retain the trust and confidence of our clients," says Erik Archambault, a survey respondent and director of enterprise health care accounts at the logistics company UPS.

But trust demonstrated by effective data management can be an even more compelling business driver when companies can exhibit their value in helping clients succeed with their customers. "We focus on the value of trust in our client relationships, which includes how we mitigate risk. This helps them get critical products to market more effectively, which in turn enhances brand trust with their consumers, patients, or overall end users," Archambault says. "For us, that means managing the global chain of custody for high-value pharmaceuticals, medical devices, and specimens. Quality assurance, high visibility, regulatory compliance, and temperature controls are critical for these complex, sensitive shipments."

Accurate audit trails also reduce regulatory risks for clients in health care, one of the most scrutinized industries, he adds.
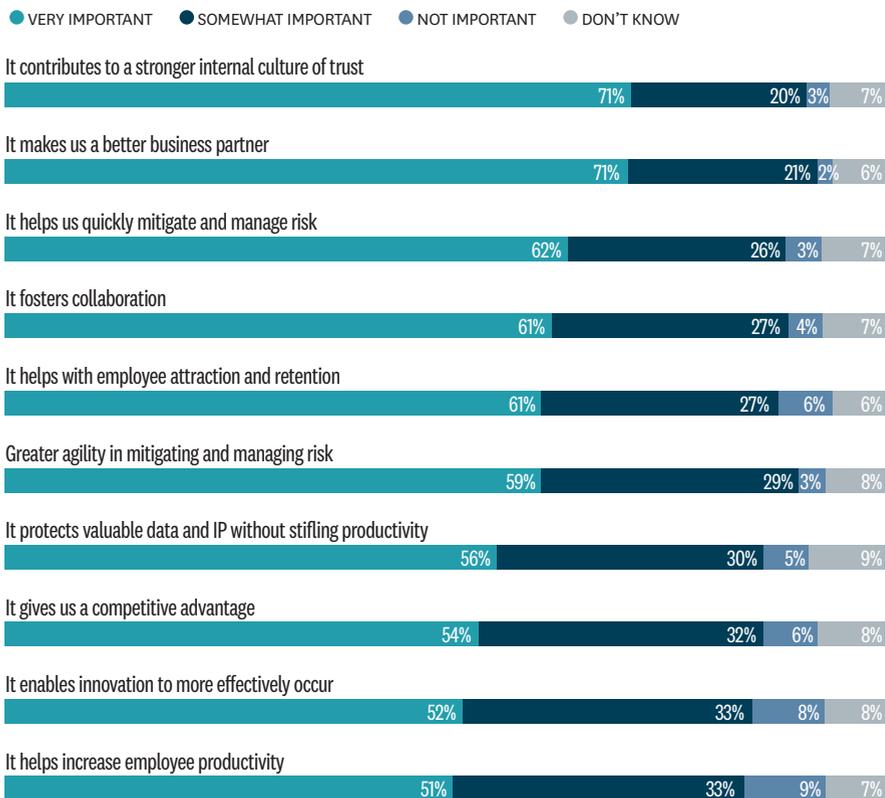
Zeiss Group, a manufacturer of precision optics and optoelectronics headquartered in Oberkochen, Germany, works with clients that have similarly exacting standards, says Axel Zibold, vice president of sales and customer support and a participant in the survey. Success depends on convincing the company's customers that its leading-edge products will meet complicated specifications. "In this challenging environment, trust becomes very important," Zibold says.

Trust is also critical for companies that establish long-term relationships with life insurance customers. "Our oldest customer is more than 100 years old," says Marc Mathis, executive vice president of product and market

FIGURE 5

HIGH-TRUST ORGANIZATIONS GAIN A COMPETITIVE EDGE

Respondents rating the importance of the following benefits associated with an effective internal trust assessment and management policy

● VERY IMPORTANT ● SOMEWHAT IMPORTANT ● NOT IMPORTANT ● DON'T KNOW

It contributes to a stronger internal culture of trust
71% | 20% | 3% | 7%

It makes us a better business partner
71% | 21% | 2% | 6%

It helps us quickly mitigate and manage risk
62% | 26% | 3% | 7%

It fosters collaboration
61% | 27% | 4% | 7%

It helps with employee attraction and retention
61% | 27% | 6% | 6%

Greater agility in mitigating and managing risk
59% | 29% | 3% | 8%

It protects valuable data and IP without stifling productivity
56% | 30% | 5% | 9%

It gives us a competitive advantage
54% | 32% | 6% | 8%

It enables innovation to more effectively occur
52% | 33% | 8% | 8%

It helps increase employee productivity
51% | 33% | 9% | 7%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

COMPANIES THAT LAGGED COMPETITORS IN TRUSTWORTHINESS ALSO WERE MORE LIKELY TO HAVE POSTED FLAT OR DECLINING REVENUES OVER THE PAST TWO YEARS.

management at Swiss Life Group, a Zurich-based company that the survey identified as a trust leader. "In our industry, relationships are about trust that is earned when actions meet words even under sometimes-stressful circumstances. We need to demonstrate that we are keeping our promises and being consistent even if outside economic forces change."

Some insurance companies are taking a different approach, however. Various challenges over the past year have prompted some insurance companies to resell policies to others to improve their financial position. Clients may understandably see this as a breach of trust with a company they assumed would be handling their affairs through the end of their lives, Mathis says.

Develop a Comprehensive Trust Strategy

The stakes are high when it comes to business trust—missteps can give competitors opportunities to steal customers, while demonstrable confidence in how business is conducted can foster profitable, long-term relationships for all parties. In this context, what models do leaders offer to guide less-mature peers in their efforts to improve external trust and as a result gain business benefits? Here's where leaders will focus in the months ahead.

High-trust organizations will redouble efforts to involve senior managers from throughout the organization.

To reduce risk and enhance trust, leaders—those who can quantify the business value of trust—are crafting comprehensive strategies with policies that cross departmental boundaries. "Companies can't approach trust in a piecemeal fashion—it takes an integrated approach to build a trustworthy company," Hurley says. "That means bringing together people from compliance, human relations, communications, and legal. They're all part of a larger whole."

Trust leaders will move to automated, real-time behavior monitoring to continuously assess the ongoing trustworthiness of partners and employees.
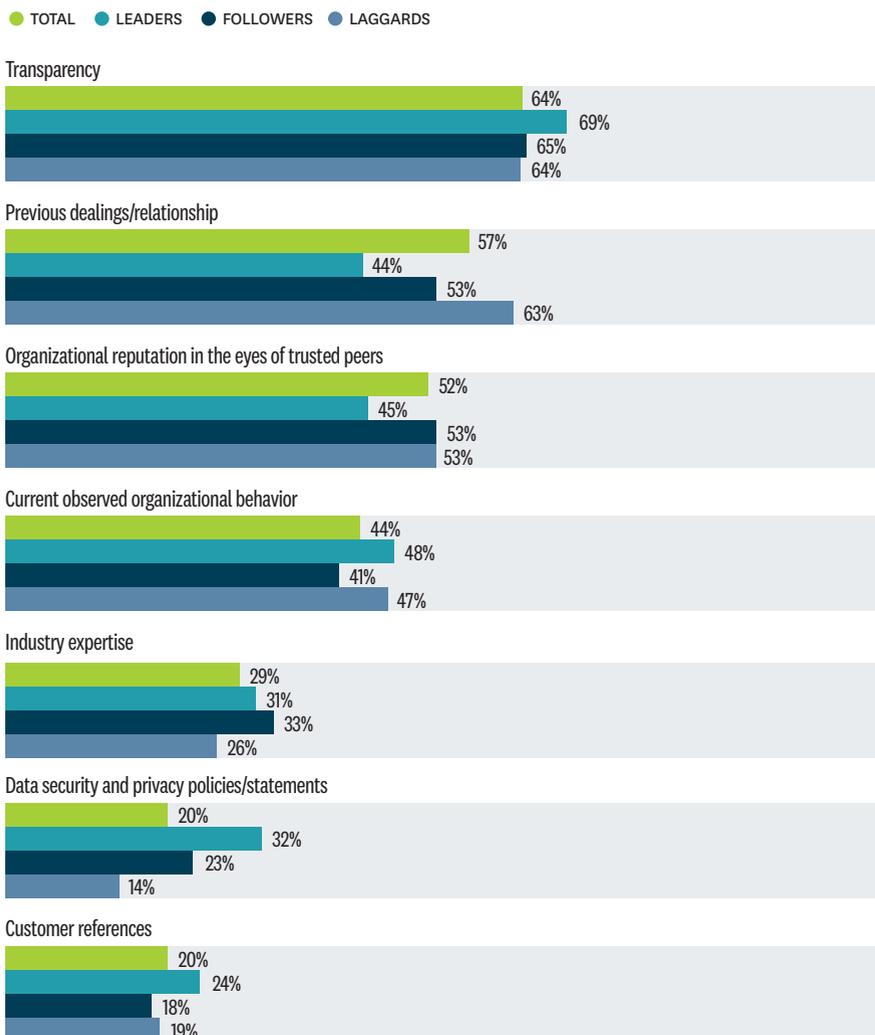
Leaders are also investing in new technology for bolstering cybersecurity and assessing internal and external behavior to quickly identify potential problems before they can cause harm.

Improving internal operations starts with a comprehensive understanding

FIGURE 6

DATA SECURITY OUTWEIGHS PAST RELATIONSHIPS WHEN GAUGING TRUST

Organizational factors that are most important in establishing trust between multiple parties in business relationships

● TOTAL ● LEADERS ● FOLLOWERS ● LAGGARDS

Transparency
- 64%
- 69%
- 65%
- 64%

Previous dealings/relationship
- 57%
- 44%
- 53%
- 63%

Organizational reputation in the eyes of trusted peers
- 52%
- 45%
- 53%
- 53%

Current observed organizational behavior
- 44%
- 48%
- 41%
- 47%

Industry expertise
- 29%
- 31%
- 33%
- 26%

Data security and privacy policies/statements
- 20%
- 32%
- 23%
- 14%

Customer references
- 20%
- 24%
- 18%
- 19%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

of what contributes to trust in today's business environment. All respondents consistently name the insights gained from previous dealings and direct relationships as a key factor in gauging the trustworthiness of business associates and employees. But leaders are looking for greater assurances when it comes to the organizations they are confident in doing business with. They want to ensure that people and organizations seen as low risks in the past continue to deserve this status. For example, leaders are more likely than their peers to evaluate the data security and privacy policies of partners to assess their organizational trustworthiness. In fact, leaders consider data security to be just as important as industry expertise when it comes to fostering trust.

In addition, leaders highly rate the ability to observe organizational behavior to gauge how well they can trust partners and employees. FIGURE 6
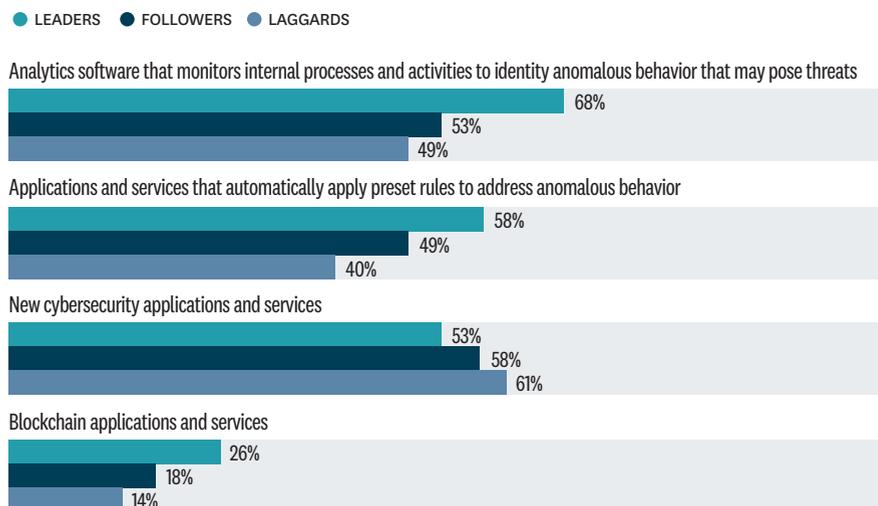
To monitor behavior, leaders are looking to new technology for help. When discussing investment plans for 2019, more than 60% of leaders say they will automate cybersecurity trust management based on real-time human behavior. Top investment areas include analytics technology that tracks internal activities to quickly identify any risky or anomalous behavior arising in their operations. Examples of this may include a health care employee trying to access the records of people not directly under his or her care or a departmental computer trying to send internal financial data to an external entity. Related investments will target digital tools that automatically apply established rules for responding to anomalous activities so any unauthorized access or data exfiltration as described above can be blocked before sensitive information is exposed. FIGURE 7

Trust leaders will expand efforts to promote internal collaboration to foster innovation. Trust is important not only for external relationships with customers and partners. It is also crucial for the high levels of collaboration and innovation that drive business results.

FIGURE 7

ANALYTICS ARE TIED TO REDUCING RISK

Respondents who will invest in risk reduction technology

● LEADERS ● FOLLOWERS ● LAGGARDS

Analytics software that monitors internal processes and activities to identity anomalous behavior that may pose threats
68%
53%
49%

Applications and services that automatically apply preset rules to address anomalous behavior
58%
49%
40%

New cybersecurity applications and services
53%
58%
61%

Blockchain applications and services
26%
18%
14%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

"When trust levels are high, companies run more efficiently because various stakeholders can more easily collaborate to make better decisions," says survey respondent Rightwell Laxa, senior vice president for satellite operations at Sasol Ltd., an energy and chemicals company in Sandton, South Africa. (The survey identified Sasol as a leader in trust.) His responsibilities include oversight of pipeline operations in Mozambique for supplying natural gas to South Africa. "We see a lot of value in promoting trust among our employees, including a correlation between trust and productivity and how valued people feel," Laxa says. "But when trust is low, companies often implement a series of governance controls, which can impede efficiency and decision making. For me, these considerations are especially important because I manage remote teams, and it takes extra effort to make people feel valued when they're away from headquarters."

Sue Capstick works for one of the U.K.'s National Health Service (NHS) organizations in a new department devoted to technology, digital health, and innovation. Working

TRUST IS CRUCIAL FOR THE HIGH LEVELS OF COLLABORATION AND INNOVATION THAT DRIVE BUSINESS RESULTS.

"We see **a lot of value in promoting trust** among our employees, including a **correlation between trust and productivity and how valued people feel**," says Rightwell Laxa, senior vice president for satellite operations at Sasol Ltd.

mainly with frontline staff in a small, highly collaborative team, she's given autonomy to make decisions without a lot of oversight by other, more-senior colleagues. She says this freedom enables her to cultivate a culture of trust, which translates into achieving the best outcomes for projects. "It's all about having a can-do attitude," she says.

This environment is in stark contrast to her experience in a former NHS organization that exhibited what she describes as a culture of fear and blame. "The lack of trust was stifling in terms of getting things done," Capstick says.

Internal trust can also spark new ideas that fuel business success. "When everybody is on the same page and teams and their managers are communicating, they create a level of trust that can foster discussions about innovation," says Margaret Lee, supervisor of general accounting at Kintetsu World Express, a global logistics company and a trust leader whose U.S. operations are based in Jericho, N.Y. "People are more open about discussing how certain processes or activities may be done better so there are more chances for the company and the team to be successful."

Other survey respondents also see a link between internal trust and innovation. "When I've been able to cultivate close working relationships with clients, we created new products and services," says survey respondent Pia Sanedrin, managing director at Sanedrin Consulting, based in Manila,

the Philippines. "Those relationships fostered ideas for re-bundling or repackaging services into new solutions and for developing new business models that contribute to growth."

Leaders will take additional steps to cultivate and promote a culture of trust based on clear codes of conduct.

Leaders understand that technology solutions are only part of what's necessary to strengthen the trustworthiness of their organizations. Cybersecurity solutions go together with staff training and other cultural factors when it comes to elevating trust levels. By contrast, fewer than half of the followers and laggards plan to invest in important employee-related areas, such as behavior monitoring, training, and changes to management responsibilities. FIGURE 8

"While the latest cybersecurity products and services are important, they must be augmented by a strong cultural and policy commitment to security and data privacy. The most important control is having a company culture designed to create trust among employees and vendors," Sanedrin says.

Senior management is a potent force for promoting a trust-based culture. "Trust is one of the core values of our company, and it's important for senior staff to display that to employees," Sasol's Laxa says. "We have a code of conduct that guides how leaders conduct themselves with employees and stakeholders—along with clear consequences if the code isn't followed."

To enforce these values, Sasol works with a third-party management consulting firm that employees can contact if they see any ethics violations. Some departments have their own ethics officers who report directly to senior vice presidents when complaints arise. These safeguards are bolstered by employee surveys with questions about trust, corporate values, and related cultural areas.

Zeiss's Zibold concurs. "To promote trust within your organization, you have to be sure people understand

your rules about protecting data and managing intellectual property," Zibold says. "That requires a commitment to training and clearly defined policies."

Part of developing effective trust policies is having a clear idea about the risks and rewards of managing sensitive data. At McGraw-Hill, one of the survey's trust leaders, Russell oversees IT operations related to customer relationship management. "[The European Union's General Data Protection Regulation (GDPR)] has forced us to look at not only the value of the data we're collecting from customers, but also the associated risks of managing this information," he says. "This is causing us to ask ourselves whether having certain data actually justifies those risks."

The answer becomes complicated because various departments measure value differently. McGraw-Hill brings together Russell's group, a chief privacy officer, and managers from individual business units to discuss the trade-offs in value and risk. "Our goal is to get people in business units to make these considerations an intrinsic part of doing their jobs," Russell says.

To demonstrate to customers that McGraw-Hill is a trusted keeper of their private information, the company makes senior security and privacy staff available to address any questions and concerns about global privacy regulations, such as GDPR.
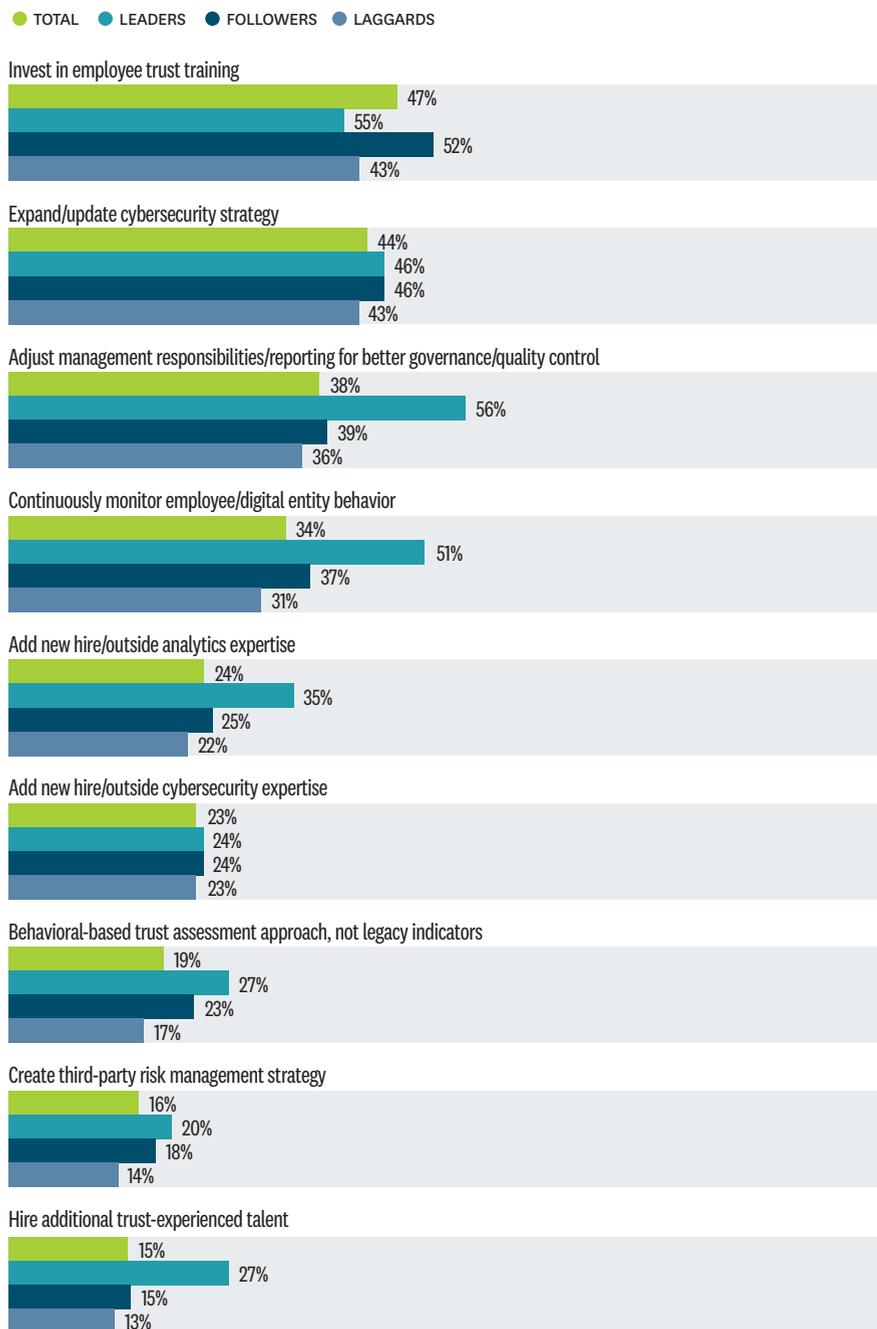
How to Demonstrate Trustworthiness

New technologies and a focus on organizational cultures can strengthen trust, but these improvements alone won't necessarily yield competitive advantages. Organizations must also demonstrate what sets them apart from others as valuable enterprises for customers, partners, and employees. Demonstrating trustworthiness begins with some basic steps. "We start at a fundamental level by focusing on day-to-day tasks," says Mathis at Swiss Life. "For example, when we state that we will respond to someone's question within a defined time frame, we aim

FIGURE 8

ORGANIZATIONAL CULTURES ARE ALSO KEY

Respondents stating steps related to internal business operations strengthen trust and protect critical data and IP

● TOTAL   ● LEADERS   ● FOLLOWERS   ● LAGGARDS

Invest in employee trust training
47%
55%
52%
43%

Expand/update cybersecurity strategy
44%
46%
46%
43%

Adjust management responsibilities/reporting for better governance/quality control
38%
56%
39%
36%

Continuously monitor employee/digital entity behavior
34%
51%
37%
31%

Add new hire/outside analytics expertise
24%
35%
25%
22%

Add new hire/outside cybersecurity expertise
23%
24%
24%
23%

Behavioral-based trust assessment approach, not legacy indicators
19%
27%
23%
17%

Create third-party risk management strategy
16%
20%
18%
14%

Hire additional trust-experienced talent
15%
27%
15%
13%

SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2018

86%

OF LEADERS SAY THEY ARE SEEING A CLEAR RETURN ON THEIR TRUST AND RISK INVESTMENTS.

to do that in the vast majority of the cases."

In addition, the company regularly conducts customer satisfaction surveys and then pays special attention to any areas where scores are low. "We contact all the people who voice problems to get a better understanding of the underlying causes," Mathias explains. "We then ask the permission of customers to keep them informed about our efforts to resolve and overcome those bad experiences, which demonstrates that we are taking each person's problems seriously."

Another trust builder is communications that explain why the company requests and maintains personal data about individual clients. "We let people know what data we store within our company, and if asked, we will share a person's data file," Mathias says. "If someone is convinced we have information that's not relevant to our business relationship, we'll discuss how it may, in fact, help us determine a more granular price for their premium. If the person still isn't persuaded that the data is necessary, we'll delete it."

Catalent Biologics is a contract developer, manufacturer, and supplier of biologic therapies and a trust leader with corporate headquarters in Somerset, N.J. Its facility in Bloomington, Ind., uses live video streams to bolster trust with global clients who can't regularly be on-site during their molecule's manufacturing process. Clients can remotely control cameras to watch certain stages of their product's production process and ensure that Catalent associates are complying with requirements spelled out in the quality agreement. Customers can also zoom in on order-filling processes in enough detail to read bar codes on pharmaceuticals and devices. "Almost all the companies we work with take advantage of this resource," says Wayne Heminway, Catalent's account executive. "It's something that only a small number of our competitors can offer."

UPS also takes extra steps to satisfy customers. It developed software for pharmaceutical clients that creates a more secure and auditable chain-of-custody record. In addition, UPS may schedule quarterly business reviews with customer compliance, operations, and procurement professionals to address any logistics questions or concerns. "It's all part of a vision to inspire trust and empower innovation that improves patient care across the health care and life science ecosystem," Archambault says.

Efforts such as these require significant amounts of time and money, but leaders say the investments are worthwhile. A significant majority of leaders (86%) say they are seeing a clear return on their trust and risk investments. "Trust builds strong partnerships," says UPS's Archambault. "Whenever we sign a new contract, we identify what factors led to that success, such as the combination of our proprietary software and the expertise of our people. In some cases, it's the proprietary software [that archives digitized signatures]. So, if we win X amount of dollars with a pharma client because it values our supply chain technologies and competence, we see those as part of a winning recipe for logistics success."

The Journey Never Ends

The results of the survey clearly illustrate the importance of trust for global businesses. Enterprises that remain good stewards of sensitive information create opportunities for attracting new customers, fostering innovation, defending against market challenges from competitors, and helping customers and partners succeed with mutually beneficial business relationships.

While only a small percentage of large enterprises have established themselves as trust leaders, they can point the way for others to confidence-building investments and policy updates. This includes updated strategies that integrate new approaches to cybersecurity and behavioral analytics and policies that cultivate cultures of trust promoted by the most senior members of enterprises. Management experts say there's one other essential ingredient for organizations to become and remain trusted—a lasting commitment to continuous improvement. "You can never stop working at being trustworthy," Fordham's Hurley says. "It's not a once and done effort. Companies have to continually measure, manage, and improve what they achieve and how they achieve it."
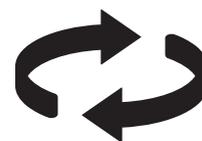
"YOU CAN NEVER STOP WORKING AT BEING TRUSTWORTHY. IT'S NOT A ONCE AND DONE EFFORT," FORDHAM'S HURLEY SAYS.

METHODOLOGY AND PARTICIPANT PROFILE

A total of 818 respondents drawn from the HBR audience of readers (magazine/ newsletter readers, customers, HBR.org users) completed the survey.

SIZE OF ORGANIZATION

ALL RESPONDENTS' ORGANIZATIONS HAD 499 EMPLOYEES OR MORE.

52%
2,500 OR MORE
EMPLOYEES

13%
1,000-2,499
EMPLOYEES

10%
500-999
EMPLOYEES

24%
100-499
EMPLOYEES

SENIORITY

22%
EXECUTIVE
MANAGEMENT/
BOARD MEMBERS

33%
SENIOR
MANAGEMENT

28%
MIDDLE
MANAGERS

17%
OTHER GRADES

KEY INDUSTRY SECTORS

12%
MANUFACTURING

11%
TECHNOLOGY

11%
EDUCATION

11%
FINANCIAL
SERVICES

9%
GOVERNMENT/
NOT-FOR-PROFIT

8%
OR LESS OTHER
SECTORS

JOB FUNCTION

14%
HR/TRAINING

13%
OPERATIONS/
PRODUCT
MANAGEMENT

11%
GENERAL
MANAGEMENT

8%
OR LESS OTHER
FUNCTIONS

REGIONS

41%
NORTH AMERICA

25%
EUROPE

20%
ASIA PACIFIC

8%
MIDDLE EAST/
AFRICA

6%
SOUTH/CENTRAL
AMERICA

Figures may not add up to 100% due to rounding.

ENDNOTES

1 https://www-bloomberg-com.cdn.ampproject.org/c/s/www.bloomberg.com/amp/view/articles/2018-04-13/how-hacking-affects-a-company-s-market-valuation

2 https://www.nytimes.com/2018/12/19/technology/facebook-data-sharing.html

3 https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/