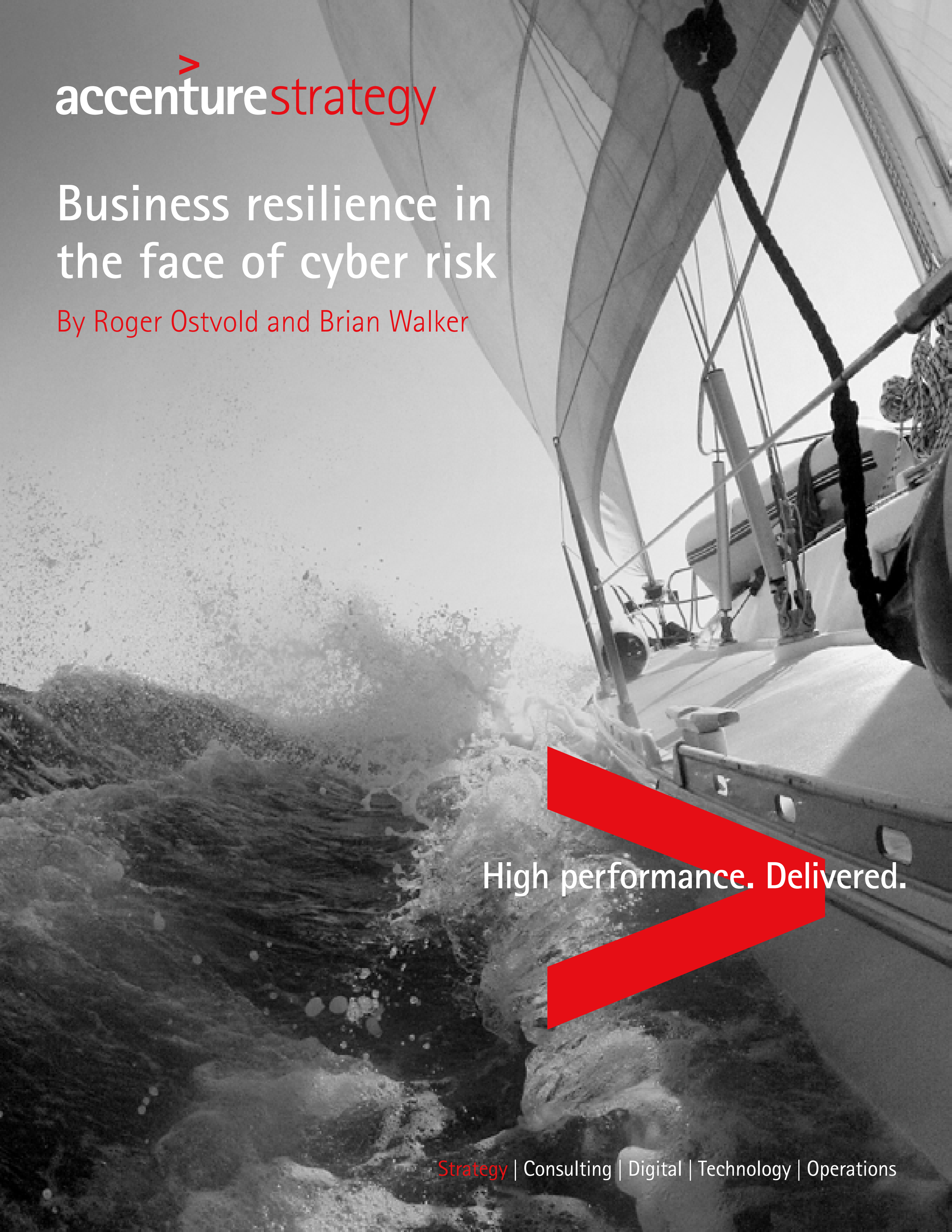
accenturestrategy

Business resilience in the face of cyber risk

By Roger Ostvold and Brian Walker



High performance. Delivered.

Strategy | Consulting | Digital | Technology | Operations

When it comes to experiencing failure of at least part of an enterprise's digital environment, it is a matter of "when" rather than "if." Two-thirds of executives surveyed by Accenture Strategy said that their organizations experience significant attacks that test the resilience of their IT systems on a daily or weekly basis. Operational technology systems are subjected to cyber attacks nearly every day.[1]

As digital capabilities increasingly become the glue that bonds sophisticated enterprises, downtime is not just costly but untenable. Failures and hostile cyber actions have profound impacts on enterprise performance—even enterprise viability. Yet, combined properly, the same technologies that are driving the digital enterprise can enable resilience at a level not possible before. Success requires a fundamentally different perspective on risk and technology portfolio management—and the leadership required to make it reality.

Accenture Strategy research into the intersection of business and technology—and extensive work with enterprises of all sizes and across each major industry—has provided some insight into what it takes to be prepared. The key to being fault-tolerant is to adjust quickly to disruption and minimize the impact on customers, supply chains or internal operations when they inevitably occur.

Know thy weaknesses

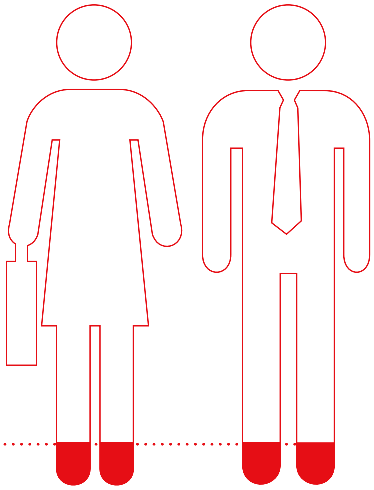
Savvy enterprises are self-aware, with a realistic sense of their own weak spots—in both information technology (IT) and operational technology (OT). Many enterprises, however, have a long way to go. Only nine percent of executives that Accenture Strategy surveyed stated that they proactively run inward-directed attacks and intentional failures to test their systems on a *continuous* basis. A mere 25 percent consistently design resilience parameters into their operating model and technology architectures.[2]

No enterprise is an island. Companies in all industries, government agencies and even private citizens operate in a complex ecosystem of partners and service providers that enable organizations and individuals to be almost anywhere they want to be. But this vast reach comes with a price—it leaves an organization critically reliant on processes, technology and people that it has limited or no control over. Managing an interconnected enterprise requires the ability to evaluate strengths and weaknesses of each element objectively to ensure the entire system is resilient to a vast array of threats.

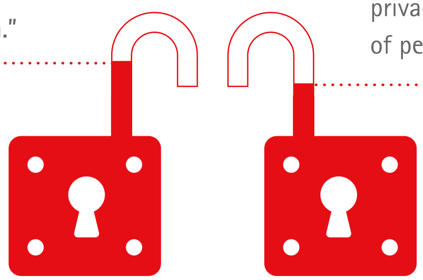
Given the number and complexity of elements involved in the digital value chain, breaches ranging from human and technical failure to cyber attacks are inevitable. According to research conducted by Accenture with the World Economic Forum, concerns about cyber attacks top all other fears. Seventy six percent of business leaders believe the likelihood of malicious attack to be "very or extremely high," and another 68 percent believe in the high likelihood of privacy breaches of personal data.[3]

While executives can assess and shore up security around their own enterprises, they must look farther and consider the impact of breaches from every other member of the network. Timely adjustment requires both resilience and agility, as organizations need to move quickly to maintain operations, address the outage and bounce back from any damage they may incur.

Of those surveyed, only **nine percent** of executives proactively run inward-directed attacks and intentional failures to test their systems on a continuous basis.



Seventy six percent of business leaders believe the likelihood of malicious attack to be "very or extremely high."



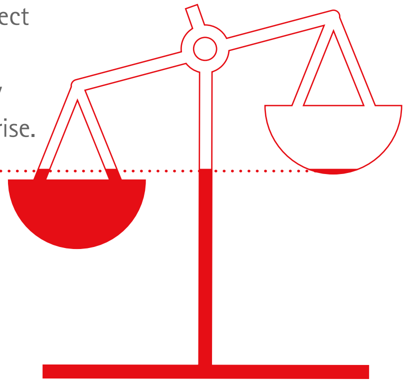
Sixty eight percent believe in the high likelihood of privacy breaches of personal data.

The battle between protection and enablement

In a perfect world, organizations would have unlimited resources to be able to institute iron-clad security measures while also pursuing the business' growth and innovation agenda. As business leaders from all areas get increasingly eager about digital connections and mobile apps, they do not want to be slowed down or stopped by concerns about security. Building an agile organization that can move quickly to seize marketplace opportunities while not moving so quickly as to be exposed to too much risk is yet another challenge of a multi-speed business and IT operating model.

Enterprises need to make difficult choices as to where to place scarce resources and how to strike the right balance between spending to protect the enterprise and spending to enable innovation and growth. These decisions require a detailed understanding of quantified value…as well as quantified risk. CEOs, CIOs and other C-suite leaders need not only to choose where to invest, but also to consider the residual portfolio risk that results from *not* investing. Just 38 percent of executives in an Accenture survey "strongly agree" that balancing spend-to-protect and spend-to-enable is mature and continuously managed in their enterprise. Another 49 percent merely "agree," signaling that there is still room to improve in this critical area.[4]

Just **38 percent** of executives in an Accenture survey "strongly agree" that balancing spend-to-protect and spend-to-enable is mature and continuously managed in their enterprise.



Resilience—not just for systems

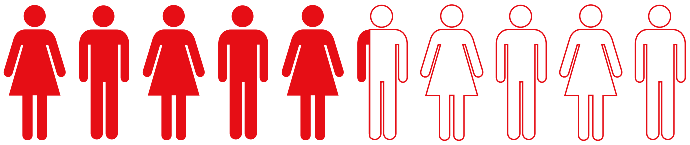
Resilience of the enterprise is not limited to enabling technologies alone. Just ask the CEO, CIO or other members in the C-suite of any enterprise who has suffered a major data breach.

A strong CEO will focus on harmonizing an entire organization's portfolio of capabilities—from physical assets through the ecosystem to people. All components are critical in ensuring the uninterrupted delivery of products and services, and all need to work together to both prevent and bounce back from an interruption in operations.

Most successful enterprises recognize that responsibility for resilience and agility does not fall to the CIO, CISO or CRO alone, as the impact of an outage or failure can topple leaders at all levels. Only half of the executives Accenture surveyed stated that they have a board-level committee in place focused on business resilience. There are, on average, two C-suite executives responsible for continuously monitoring and improving business resilience, with the CIO being involved more than half of the time.[5]

The CEO should also work hand in hand with the CIO and other business leaders to set the tone for the company's push/pull investment decisions between enabling and protecting. The CEO should advance the importance of business continuity with the entire executive leadership team and board of directors. That way, when a breach occurs (not if), the discussion pivots quickly from "what is our plan" to "how is our plan working?"

Here is some cause for alarm: Of all the organizations that Accenture Strategy surveyed, only 53 percent have a continuity plan that is refreshed as needed. Only 49 percent map and prioritize security, operational, and failure scenarios. Forty five percent have produced threat models to existing and planned business operations.[6]



Only **53 percent** of those surveyed have a continuity plan that is refreshed as needed.

When it comes to resilience, actions speak louder than words

Accenture Strategy research uncovered a gap between executives' perceptions and reality when it comes to their organizations' ability to address resilience. There are several steps that are vital to making a business resilient, agile and fault-tolerant.

Embrace a digital ecosystem. Isolationism does not work well as a risk management strategy. C-suite executives are seeing the advantage of robust digital capabilities and technologies outside the enterprise. It is vital that the power of such a digital ecosystem be at the core of strategic decision-making.

Manage digitally. Sequential, hierarchical and slow-moving methods of management do not work well in today's converged, evolutionary, dynamic and often hostile world. Multi-speed business and multi-speed IT requires real-time orchestration of myriad internal and external services. It also requires some redundant services and infrastructure that may not be called into service often, but are critically important when they are needed.

Institutionalize resilience. Resilience cannot be added after-the-fact or on a sporadic, discretionary basis. It must be part of the fundamental operating model—ingrained at the outset into objectives, strategies, processes, technologies—and even culture. From infrastructures to applications, and products to services, everything should be designed with resilience in mind. New mindsets and skills are required, not only within IT and operational technology, which are increasingly converging, but also with the board of directors and throughout the C-suite.

Stretching to become a more elastic enterprise

Risk management is sometimes thought of as an exercise in limitation. But managing risk in the context of business resilience is more about enablement. By gaining a full understanding of the potential issues that will inevitably arise from the highly connected digital world, organizations can plan a response and limit the impact of any breach on the business and its brand. Envisioning and anticipating worst case scenarios gives executives some room to stretch into new innovations and marketplace opportunities. With the right set of capabilities in place, managing cyber risk becomes both a part of the rhythm of the business and essential to maintaining the rhythm of the business.

Join the conversation:
@AccentureStrat

Authors

Roger Ostvold
roger.ostvold@accenture.com

Brian Walker
brian.d.walker@accenture.com

[1] In 2015, Accenture Strategy surveyed more than 900 executives around the world on a variety of topics related to business resilience, multispeed business and IT, technology led innovation, and the digital agenda.

[2] Accenture Strategy research on the intersection of business and technology, 2015.

[3] Industrial Internet of Things: Unleashing the Potential of Connected Products and Services; The World Economic Forum in collaboration with Accenture, 2015.

[4] Accenture Strategy research on the intersection of business and technology, 2015.

[5] ibid.

[6] ibid.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 336,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

About Accenture Strategy

Accenture Strategy operates at the intersection of business and technology. We bring together our capabilities in business, technology, operations and function strategy to help our clients envision and execute industry-specific strategies that support enterprise wide transformation. Our focus on issues related to digital disruption, competitiveness, global operating models, talent and leadership help drive both efficiencies and growth. For more information, follow @AccentureStrat or visit www.accenture.com/strategy

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademark.