Are you preparing for change or reacting to it?

Building resilience to move full speed ahead

The better the question. The better the answer.
The better the world works.

Building a better working world

COOs navigating the complexities of a changed and volatile world are rebuilding their operations from the ground up to thrive in the future.

Until recently, chief operating officers (COOs) have focused primarily on fine-tuning the value chain for speed to market, efficiency and profitability. But the world has changed – at first gradually and now suddenly.

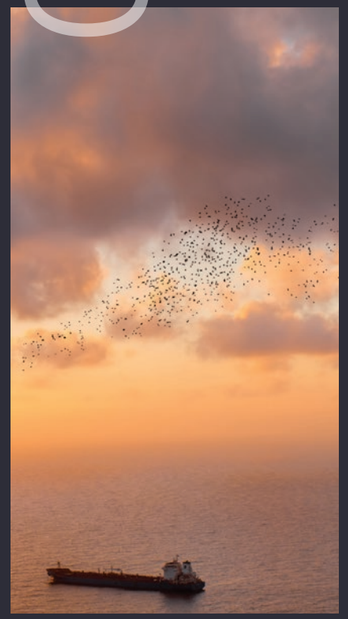
Over the last several years, empowered consumers, employees and investors; climate change; geopolitics; and technology innovations have disrupted organizations, pushing them to change how they operate. Over the last 18 months, the COVID-19 pandemic turned that slow push into a giant, forceful shove. And COOs have had to figure out on the fly how to operate in this changed environment.

Organizations may still be making similar products and services, but everything about how these products and services are designed, manufactured and delivered to customers is different. This shift is forcing COOs to reimagine their supply chains for agility and sustainability as much as optimization.

Across the enterprise, technology innovations are helping COOs transform how the business operates to meet multiple, simultaneous demands from a range of stakeholders – and increasing the chances of cyber infection. Reskilling and upskilling the workforce can help accelerate digital transformations and address cyber risks. All of this is happening in the context of economic and techno nationalism.

To help COOs determine where to start and how best to navigate operational resilience and sustainability, we break these action items down in three e-books.

01



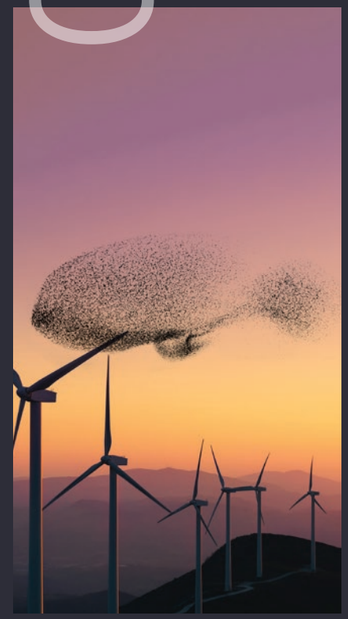
E-book 1

Setting a course for sustainable and resilient operations

As COOs navigate this increasingly complex and volatile world, they need to cast their gaze across the entire value chain as they seek to reframe their future for operational resilience and sustainability.

Request document

02



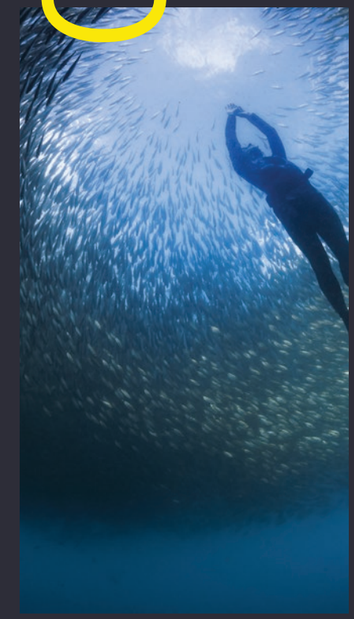
E-book 2

Mapping a sustainable future

Increasing pressure from consumers, employees, investors, governments and regulators is pushing COOs to consider the future of their operations in the dual context of what's best for the business, society and the planet.

Request document

03



E-book 3

Building resilience to move full speed ahead

After a year of disruption, organizations need to transform to build resilience for themselves, for their teams and across the enterprise to improve agility and the ability to pivot at speed.

Current book

Building resilience to move full speed ahead

COOs are building resilience to improve agility and pivot at speed.

68%

of corporate business leaders say that ecosystems and partnerships are the only way to succeed in the market.[1]

COVID-19, with all its indirect impacts, has been the most critical event COOs have recently faced, but it is hardly the only one.

The days of going it alone to conduct or transform businesses are long gone. Today's organizations are part of a much larger ecosystem of clients, vendors, suppliers, alliances, partners and other stakeholders. The end-to-end, value chain nature of a networked ecosystem demands end-to-end transparency and visibility. More so, the dependencies each member of the ecosystem has on one another means that risk management and resilience have to reach well beyond the confines of the organization.

Robust resilience programs play a critical role in an organization's adaptation and survival. As COO, you need to understand the organisms and environmental elements of your operational ecosystem, how each impacts the other, and what steps you can take to adapt and evolve.

Here are four ideas for rebuilding your operations for resilience so that you can move full steam ahead into the future.

1 *Four essential ingredients of successful ecosystem partnerships*, EY, February 2020

01

Improve operational visibility and risk monitoring

Given the waves of disruption ahead, resilience needs to be a priority every day – not just in times of crisis – to meet changing expectations, minimize potential risks and seize opportunities.

While the pace and scale of today's global supply chain disruption is unprecedented, the means for dealing with it are attainable, with real solutions to improve visibility, simulation and risk monitoring. Advances in technology – such as internet of things (IoT) sensors, artificial intelligence (AI) and software such as control towers – have put the goal of end-to-end visibility and the means to act on it in reach.

Driving end-to-end visibility

In the wake of pandemic-related lockdowns, companies made investments in greater supply chain visibility and inventory management – crucial steps toward gaining a full picture to help contend with sudden or long-term disruption. However, EY research[2] shows they still need to work on the data connections and end-to-end visibility, beyond their own internal operations. Key steps to take for additional monitoring include:

- **Identifying critical parts and critical Tier N suppliers (the suppliers of your suppliers and beyond).** It would be a cost-prohibitive and perhaps impossible effort for most organizations to gain full visibility down to the Tier N level for all their suppliers. Setting priorities based on risk is a worthwhile starting point. The supply chain visibility that businesses require must factor in data from these suppliers to adequately surface risks and create contingencies.
- **Develop relationships centered around trust.** Organizations have best succeeded in working with their key suppliers by focusing on building trusted relationships and developing areas of mutual interest as business partners to plan for disruption. With trust, ecosystem partners can leverage platforms that encourage collaboration and transparency, gaining the ability to collectively adjust plans and make better decisions based on real-time performance.
- **Revisit contracts and create benchmarks.** Contracts with suppliers can stipulate expectations around what data should be made available, such as inventory levels, and include access, audit and review rights. Many companies today are also introducing such stipulations around meeting environmental, social and corporate governance (ESG) objectives.
- **Deploy technology in your operations to build a control tower.** For companies with more mature supply chain capabilities, IoT sensors on manufacturing equipment and tracking mechanisms in logistics – along with external data from suppliers – can be united with AI and machine learning to produce actionable insights. Relying on these technologies and dashboards, control towers act as visibility solutions for surfacing bottlenecks, responding to events, optimizing resources and making recommendations on what to do next.

of executives say that the autonomous supply chain is either here or will be by 2025.[2]

2 *How COVID-19 impacted supply chains and what comes next*, EY, February 2021

Enabling simulations and risk monitoring

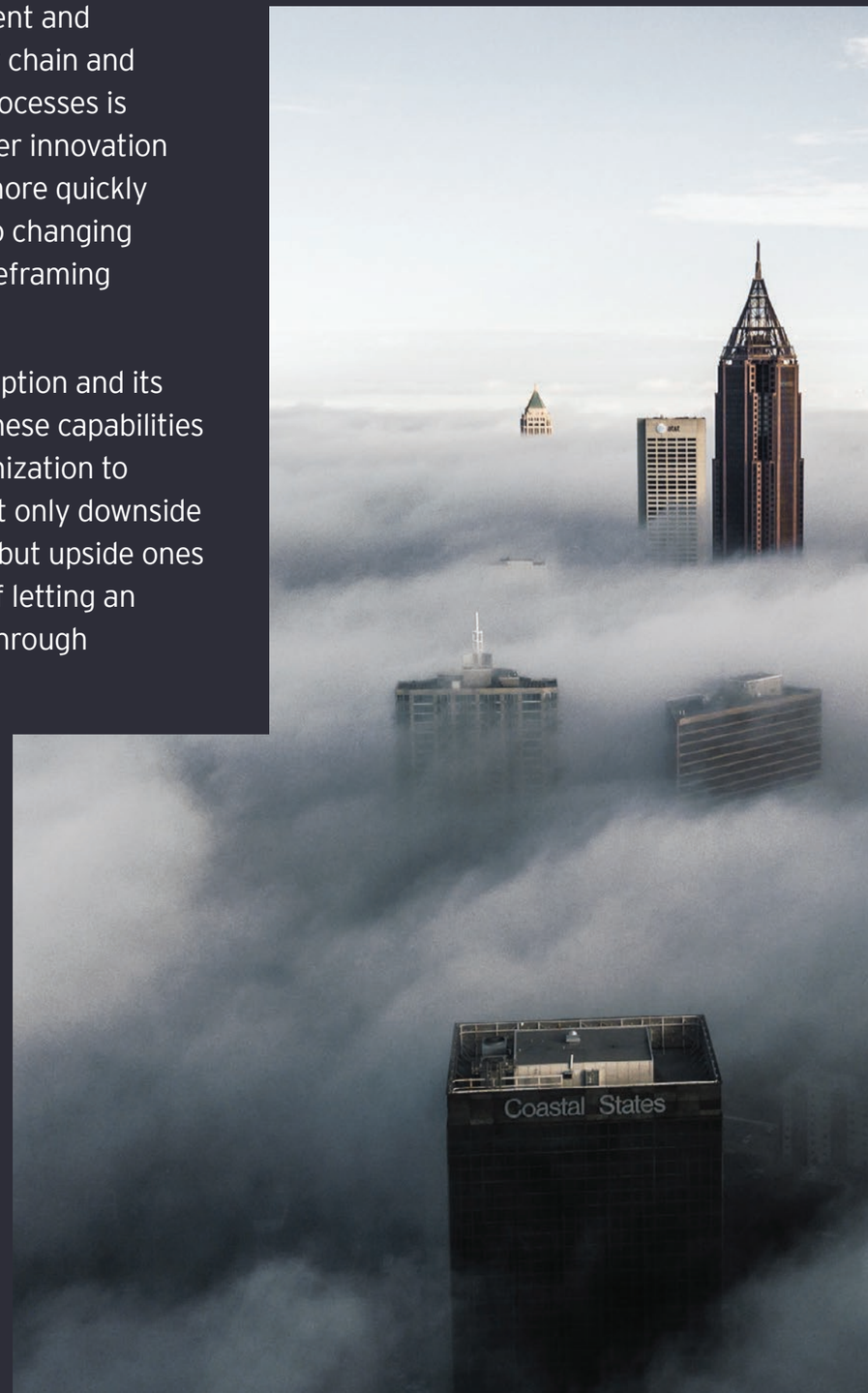
Many companies today lack a sophisticated capability for scenario analysis in their supply chains. These efforts not only prepare you to minimize risk, but also to consider how sudden changes can trigger new opportunities for those who are most prepared. Along with technical advances in supply chain visibility and data capabilities, here are four actions you can take:

1. **Set priorities and shift your mindset as a first step to modernizing risk management.** Maintain an adaptive risk universe to identify emerging upside, outside and downside risks to prepare for change and take actions as needed. Narrowing your focus to what's most important is a crucial place to begin for developing foundational business continuity, disaster recovery and crisis management plans, including critical dependencies and alternate recovery strategies. Analyze the cause and effect of key risks to perform scenario planning based on your organization's strategic priorities, and quantify the risk impact to priorities. Technology is providing new ways to strengthen these plans with actual data.
2. **Explore tools for scenario planning and simulations.** For example, today's supply chain simulation software can bring in data about weather patterns or disasters, hotspots for social unrest, and geolocation information on parts — allowing you to predict and quantify risks, such as a tsunami in East Asia, a blockage in a major canal or political unrest anywhere in the world.

   Risk intelligence engines can also monitor news sources and other external data to anticipate scenarios and risk events. Routine scenario planning not only helps minimize disruption, but also identifies new business opportunities. Companies can look at their entire supply chains and ask questions about where products are made, how they're distributed and whether their supplier bases are diverse enough to withstand shocks. Integrate these analyses into governance, risk and compliance (GRC) programs to be dynamic on how the second and third lines of defense are monitoring emerging risks. It's also vital to routinely test and update these plans as the business landscape shifts and your strategies evolve.
3. **Go further with a digital twin.** Digital twins can connect to your enterprise resource planning (ERP) system or the systems from your suppliers, and (less ideally) manual data downloads can be used as well. This parallel version of the supply network supports prescriptive decision-making based on the world as it is, not gut instinct. As noted earlier, if digital twins are focused on the right areas, they can be a powerful tool to improve resilience.

Maintaining resilient and networked supply chain and manufacturing processes is critical to customer innovation and responding more quickly and proactively to changing dynamics — and reframing your future.

Anticipating disruption and its impact through these capabilities equips your organization to better identify not only downside and outside risks but upside ones as well: the risk of letting an opportunity slip through your fingers.



02

Boost supply chain resiliency with sustainable and diverse sourcing

A resilient supply chain is one that's both diverse and sustainable. It needs to flex when stressed; remain resilient to geopolitical, meteorological, health or economic shocks; and be secure for the long term.

As a COO, you need to understand exactly where your suppliers are and what they supply. Multi-tier mapping of suppliers and reviewing supplier sourcing approaches for critical parts are fundamental to resilient supply chains. Often, it's the delay to deliveries of small but crucial components that can halt production.

Economic nationalism is also increasingly impacting supply chains. For some COOs, the answer is to localize or nearshore their suppliers. Another option may be "glocalization." Driven by the pandemic and sharp changes in global trade policies, glocalization focuses on balancing localized and globalized business options to stay competitive.

If you choose glocalization, you will need to look to suppliers that the organization hasn't dealt with before. Use of diverse suppliers, given their vast and unique footprint can contribute to resiliency, better ESG outcomes — and more cost-effective and innovative approaches.

Diversifying supply to cut costs, drive innovation and feed broader goals

Exploring new diverse suppliers could help your supply chain be more agile. Their product or service may be more innovative. As your supply chain strategy changes, you may find diverse suppliers are more open to proofs of concept. Another advantage is that diverse suppliers tend to be more localized to your manufacturing and distribution sites, which in turn has a ripple effect of helping local businesses buy the goods and services they need to sustain their own operations.

Closer to home, diverse suppliers could be more flexible in helping to meet on-demand requirements as global supply chains crack under pressure. And they may be better placed to respond to market trends and help you be more innovative. As COO, you can support your organization's sustainability initiatives by integrating supplier diversity into broader ESG goals.

There are some short-term and longer-term ways to build greater diversity into your supply chain.

In the short term

- **Adjust procurement requirements.** Many companies have a requirement to include diverse suppliers in tenders based on a dollar threshold or a requirement in their tender process.
- **Rethink insurance requirements.** Finance departments often have somewhat arbitrary criteria for suppliers' insurance. For example, would it make a huge difference if the certificate was $80m rather than $150m?
- **Review payment terms.** Are they punitive? Could they be relaxed a little to take advantage of all the benefits of diversity in sourcing?
- **Change RFPs.** Many diverse companies are small to medium-sized enterprises that don't have bid response teams ready to respond immediately. Try making RFPs shorter, less complex and less urgent.

In the longer term

- Make diverse suppliers part of your end-to-end procurement processes.
- Pivot from a mindset of pure cost savings to one that combines social value, sustainability and cost savings.
- Set up the structure and process for organizational change. Position someone who is dedicated but not ultimately responsible for delivering supplier diversity goals, then embed new approaches into business-as-usual, category strategy and all normal day-to-day activities.

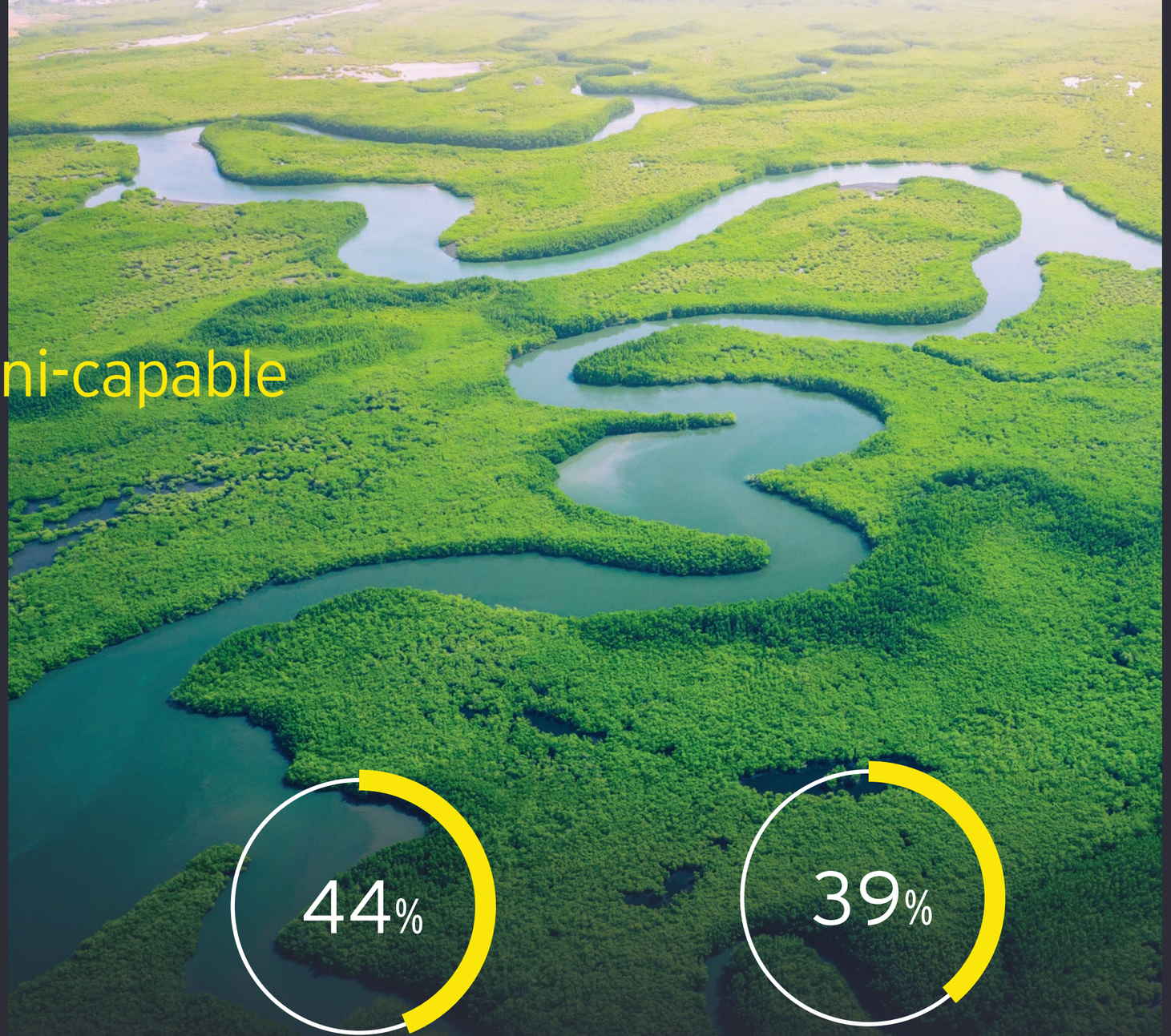
No organization can afford to ignore or lag behind this peaking wave. Supplier diversity is a business imperative; long gone are the days when we look at this as simply the right thing to do.
As supply chain disruption is the new normal, supplier diversity is one key strategy to help you weather the next major disruption.

03

Become omni-capable

In the fallout from the pandemic, organizations are asking challenging questions about the nature of how they fulfill expectations from customers – even if they don't sell products directly to them today.

Retail is leading the charge to a great extent, with the latest customer preferences shifting to dramatic increases in home delivery or "curb-side" pickup for online orders, adding supply chain complexity where inventory management systems may not be up to the task. Many brands and manufacturers, whether B2B or B2C, even in sectors such as chemicals or medical devices, are reconsidering whether they should sell directly to consumers online, alongside their traditional sales channels – or even open physical locations and grapple with retail inventory management.



of consumers expect to do more grocery shopping online over the next one to two years.[3]

of consumers expect to do more durables shopping online over the next one to two years.[3]

Because by not doing so today, they are surrendering vital data to middlemen about their customers – hobbling efforts to innovate and better meet their needs through new products, services and enhancements. Even worse, they may be gaining a short-term boost in sales on leading global online marketplaces but potentially losing their business entirely, as the data gives sellers a blueprint to compete by offering their own private label products at better prices and with preferred placement.

For all these enterprises, the solution lies in becoming "omni-capable," an evolution of the omni-channel fulfillment strategy: to be able to deliver a product and accept it as a return, whether from brick-and-mortar stores, regional distribution centers, e-commerce sites, third-party networks or any other node in the journey to the end customer. Achieving this, with ambidextrous flows, will be table stakes for delivering optimal customer experiences. Retailers and manufacturers interested in direct-to-consumer[4] share the same goal, even if they're approaching it from different angles.

While many hurdles exist in building agile and omni-capable supply chains, new tactics and technologies offer methods for moving forward more confidently.

3 *Future Consumer Index: How to serve the 'Anxious Consumer' after COVID-19*, EY, May 2020

4 *How to accelerate online direct to consumer strategies beyond COVID-19*, EY, June 2020

Making the change

Organizations today must be relentlessly focused on shaping a cost-effective supply chain that meets consumer expectations and offers regularly updated inventory visibility. In doing so, they can also potentially spend less on fulfillment while better understanding how to orchestrate their ecosystem of suppliers and partners, as well as how to adjust operations to ensure business continuity.

As a COO — whether you're building out new capabilities or optimizing existing ones — you should consider these transformative efforts:

1. **Add distributed order management (DOM) software to your systems.** Such software brings together internal and external data sources and looks through your network when each order comes in, from any channel. It examines where existing inventory exists and how close it is to the customer, and the most efficient method for fulfilling that order according to customer preferences, factoring in shipping and labor.

2. **Optimize your network.** Truly delivering an optimal and cost-efficient customer experience, with agile order fulfillment, will likely require you to scrutinize the locations in your network so they are as close as possible to your end customers. Assess first where their demand comes from. How accurate is your forecasting process, and are you capturing the right demand signals — at a state or regional level, for your varying customer segments? Again, software can help. This will guide your strategy on putting the right products in the right locations. At the same time, determine where you want to fall on the cost spectrum, whether it's to minimize expenses to the greatest extent possible or to deliver a better, but more costly level of service.

3. **Explore a control tower and radio frequency identification (RFID).** As we mentioned previously, control towers are the ultimate tool for enhancing inventory accuracy and visibility across all nodes in a supply chain. And through radio frequency identification (RFID), you can use tags, readers and software for real-time tracking without costly labor requirements.

Regardless of which strategies you decide to pursue, it's best to think of the options within long-term sales and operations planning, over the next two to five years. How big are you hoping to grow, and in which markets? Defining the vision and the infrastructure to sustain it is critical, as that should guide the supply chain from the beginning, rather than attempting to improvise later. COOs that thoughtfully build a scalable architecture with robust technology enablement and software up front and then expand footprints will likely position themselves for success.

P&G's response to the COVID-19 crisis

Global consumer goods giant Procter & Gamble (P&G) has fine-tuned supply chain management so effectively over the last decade that they've been able to significantly reduce supply chain costs while improving results and supporting a growing business. And when the disruption of COVID-19 hit, they weren't caught off balance. Not only did P&G persevere, the company's supply chain model was agile enough to shift some manufacturing lines to the production of PPE, to be donated globally.

So, what are the elements of a solid supply chain foundation from which agility can emerge? Julio Nemeth, P&G Chief Product Supply Officer, says:

> "[First,] you have to start with the conviction that the supply chain is a driver of innovation. If the supply chain's only job is making, packing and shipping, then its potential is limited. You must embark on a journey to make the supply chain an engine for total shareholder return.

Across the entire supply chain, digital made a significant difference in P&G's response to the COVID-19 crisis. The company's supply chain model included self-sufficient supply chain teams that could operate without a manager on premises and could be physically fragmented as needed for social distancing.

Nemeth points out that supply chain resiliency does not require large stockpiles of inventory or safety stock. And adding additional production capacity "just to be more resilient" can have exactly the opposite effect. "Resiliency is not something you install," he says. For P&G, supply chain resiliency is about minimizing the time needed to get back to normal performance (e.g., service levels, costs, cash generations and more) when disruption occurs.

04

Build cyber-resilient operations

The upheaval of the global pandemic has created a perfect storm of conditions in which threat agents can act. The situation is likely to get worse before it gets better. COOs want to invest in technology and innovation for the post-COVID-19 era, and they need to ensure resilience for the next major disruption, but many have yet to address the deferred risks and potential vulnerabilities that were introduced during their transformation efforts at the height of the pandemic.

Ransomware has become a threat actor's weapon of choice

Over the last year, every business has had to adapt to disruption in one form or another. Within timeframes that would have been thought impossible just a short time ago, progressive organizations rolled out new customer-facing technology and cloud-based tools that supported remote working and kept the channel to market open.

But the speed of change came with a heavy price. Many operations leaders did not involve cybersecurity in the decision-making process, whether through oversight or an urgency to move as quickly as possible. As a result, new vulnerabilities entered an already fast-moving environment and continue to threaten the business today.

of executives say that the pandemic forced their organizations to bypass cybersecurity processes.[5]

of executives say they have seen an increase in the number of disruptive attacks over the last 12 months.[5]

5 *Cybersecurity: How do you rise above the waves of a perfect storm?*, EY, July 2021

According to the EY Global Information Security Survey 2021, 81% of executives surveyed say that the pandemic forced organizations to bypass cybersecurity processes. At the same time, 77% of respondents say they have seen an increase in the number of disruptive attacks over the last 12 months.

Our experience with clients indicates that ransomware has become the cyber attacker's method of choice for data breaches. These attacks take advantage of security gaps across people, process and technology. And the consequences can be significant.

To pay or not to pay? This isn't the only question

Because a ransomware incident is not a reportable event in most jurisdictions, there are few statistics on how many organizations pay the ransom, although this is changing. Some jurisdictions, such as Australia and the US, are introducing or enacting legislation that makes reporting mandatory if ransoms are paid. Anecdotally, based on our experience with clients, we find that most organizations do pay because in many cases, it's cheaper to pay than to recover.

However, paying is no guarantee that an organization will fully recover its data or that the attack will be a one-off event. Often, cyber attackers encrypt the organization's systems in segments, requiring the organization to pay for individual keys that unlock each segment, not all of which may work.

Assume you will be attacked and be prepared to act

The first rule in building ransomware-resilient operations is to assume you will be attacked. It's not a matter of if; it's a matter of when. Further, having detection and response in place is key to disrupting and preventing ransomware attacks.

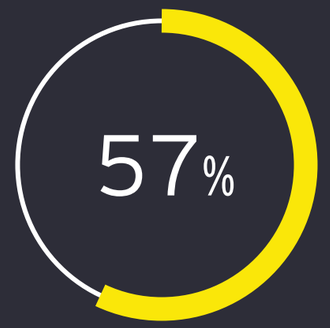
If you don't have a policy or processes in place to act, start now. Test response processes and determine what your policy is for paying or not paying. Organizations tend to be binary when making this decision, but there are a number of intricacies and "what ifs" that you need to consider. For example, what if the threat actors exfiltrate data? Go after individual clients? Come back for a second extortion payment? There also needs to be a clear line of authority for crisis commanders, escalation paths for decision-making and initial decision boundary criteria that establish guardrails for handling the unique nature of a ransomware attack.

As an operational or cybersecurity leader, you will want to test the policy you develop to understand the risks and tradeoffs of the decision to pay or not to pay, who the stakeholders are, what the process will be, who will have the authority to make the decision to pay, and at what point the organization will have to disclose the attack.

Once the policy and processes are in place, CISOs will want to conduct, at least annually, internal assessments of implemented controls to determine their effectiveness and basic maturity assessments of key controls to make certain that the organization can withstand a ransomware attack.

Over the longer term, the COO and CISO will want to team to create a culture shift across the business that puts cybersecurity at the forefront of technology planning rather than in the background as an afterthought. Security by design, where security becomes embedded into the design process for every new technology initiative, is one of the best ways to protect the organization from cyber attacks generally and ransomware attacks specifically. Consider embedding a member of the cybersecurity team into technology projects at their inception, with the role of providing guidance around security architecture and controls throughout the project lifecycle.

According to the EY Global Information Security 2021, 57% of respondents believe the current cybersecurity crisis provides an opportunity for the cybersecurity function to raise its profile within the organization. However, CISOs will need to more visibly position the cybersecurity function as a value-add part of every technology project.



of respondents believe the current cybersecurity crisis provides an opportunity for the cybersecurity function to raise its profile.[6]

6 *Cybersecurity: How do you rise above the waves of a perfect storm?*, EY, July 2021

As an operational or cybersecurity leader, you will want to test the policy you develop to understand the risks and tradeoffs of the decision to pay or not to pay, who the stakeholders are, what the process will be, who will have the authority to make the decision to pay, and at what point the organization will have to disclose the attack.

Once the policy and processes are in place, you will want to conduct, at least annually, internal assessments of implemented controls to determine their effectiveness and basic maturity assessments of key controls to make certain that the organization can withstand a ransomware attack.

Ultimately, to limit the impact of ransomware attacks, you will need to instill the company-wide importance that every worker at every level of the organization and across the ecosystem — from the board to the C-suite to management to entry-level employees to suppliers and partners — is responsible for thinking about the cybersecurity risks and acting to mitigate them. Create training programs to promote ransomware awareness.

Go from ransom-aware to ransom-resilient

The rise and acceleration of digital transformations are spreading the cyber attack surface, increasing the chances of a ransomware attack. By working together, COOs and CISOs can strengthen relationships between the business units and the cybersecurity function, and develop a cohesive detection and response plan for protection that takes an organization's operations from ransom-aware to ransom-resilient.

EY contacts

Kristina Albang
Consulting Managing Director,
Ernst & Young Global Limited
kristina.albang@ey.com

Josh Axelrod
US-West Region Cybersecurity,
Privacy & Trusted Technology Leader,
Ernst & Young LLP
joshua.axelrod@ey.com

Matthew Burton
EY EMEIA Consulting Center Partner
and Digital Operations Leader,
Ernst & Young LLP
mburton@uk.ey.com

Tonny Dekker
EY Global Consulting Enterprise Risk Leader
tonny.dekker@nl.ey.com

Sean Harapko
EY Americas Supply Chain Transformation and
Global Supply Chain RPA Leader
sean.harapko@ey.com

Theresa Harrison
EY Global Environmental Social Governance
Services Leader
theresa.harrison@ey.com

Frank Leenders
EY Global Digital and Innovation Leader
frank.leenders@nl.ey.com

Cate Mork
EY US Supply Chain Sustainability Lead,
Ernst & Young LLP
cate.mork@ey.com

Regenia Sanders
EY Consulting US-Central Supply Chain
and Operations Leader,
Ernst & Young LLP
regenia.sanders@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYG no. 010001-21Gbl
ED None

ey.com