№02 - MARCH 2022

RISK & Resilience

RELIABLE RISK INSIGHTS FOR A RESILIENT FUTURE

The Power of Information Sharing in Business Continuity Management

Best Practices for Navigating the Path to Resilience

What Business Continuity Testing and Compliance Can Learn from A Fire Drill Response

The Path to Organizational Resilience

Courtesy of:

ARAVO

RISK & Resilience

Chief Marketing Officer
Kimberley Allan

Editors in Chief
Hannah Tichansky
Rebecca Waltz

Editorial Advisors
Barbara-Ann Boehler
Jackie Risley

Contributors
Barbara-Ann Boehler
Kimberley Allan

Creative Director
Cindy Rucker

Production & Advertising Manager
Rebecca Waltz

Content Manager
Hannah Tichansky

Website Manager
Carrie Parecki

riskandresilience.co

LinkedIn: risk-&-resilience-magazine

Be a Part of R&R:
Interested in being featured in the next issue of Risk & Resilience?

We are always looking for experts, thought leaders, and practitioners to participate in interviews and articles.

Email info@riskandresilience.co to let us know.

SUMMARY

Building Better Business Resilience Together

Today's world is undeniably volatile. The ability for businesses to weather diverse strategic threats, adapt and emerge stronger – in other words to be resilient – is critical for success.

A recent study of more than 200 senior risk and insurance executives by McKinsey and the Federation of European Risk Management Associations (FERMA), found that risk management is now clearly encompassing the broader mandate of resiliency management. The majority of respondents to the study stated that the global pandemic has made risk and resilience more important to their organizations, with nearly two thirds expressing that resilience is central to their organizations' strategic process.

While many enterprises have capabilities in place to manage their financial resilience, the survey revealed that the management of business operations and the supply chain emerged as particular weak points during the pandemic – and were areas in need of addressing.

In order to move from risk to readiness, business leaders need to take a more strategic, integrated approach to risk and resilience management. This is not going to be easy; the breadth of the challenge is vast: business ecosystems are complex and interdependent, risks are diverse and interconnected, and the pace of change continues to accelerate.

But, if one thing is clear - when it comes to managing risk and promoting better business resilience - there is a lot for us to learn from. We can draw learnings from studies such as this, from history, from first responders, from regulated industries, and from each other. This is a team effort – we're in it together.

Which is why this issue of Risk & Resilience is so timely. Here we learn from a range of experts and leading thinkers about their approaches to building resilience, lessons learned, and the steps that will take us all forward on the path towards better organizational resilience.

I would like to thank all our contributors for sharing their expertise. Shared themes include collaboration, removing silos, adaptability, and taking a more holistic approach to risk and resilience. Ultimately, organizations that are more prepared and invest in risk and resilience management are those that are better positioned to adapt, rebound and succeed.

Finally, like always, I hope every single reader takes something of value away from this issue. I hope it sparks ideas, inspiration, and collaboration amongst your teams. Resilience is, after all, a team effort. We all achieve better business outcomes if we work together.

"Here we learn from a range of experts and leading thinkers about their approaches to building resilience, lessons learned, and the steps that will take us all forward on to the path towards better organizational resilience."

Michael Saracini

Michael Saracini
CEO
Aravo Solutions

"So many threats with the potential for severe disruption exist today that 'resilience' is no longer just some esoteric term... thrown around in a few highly regulated industries. It's a business imperative."

-Matt Kelly, Founder of Radical Compliance

"Resilience: What the Rest of Us Can Learn from the Financial Sector"
Page 10

THOUGHT LEADERSHIP

No Really... is this a Drill?

What Business Continuity Testing and Compliance Can Learn from Fire Drill Response

Barbara-Ann Boehler
Regulatory Compliance Analyst
at Aravo Solutions

Anyone who has attended school (in person) or worked in an office building is familiar with the concept of the fire drill. There seems to be a clear difference between fire drill compliance by children in elementary school and fire drill compliance by adults in the suburban office building. There are some interesting insights that we can gather from a review of how people respond to an alarm during a fire drill (or really from business continuity testing) and how compliance might be improved.

During elementary school unannounced fire drills students are required to immediately stand up from their desks, form an orderly line, and file (quietly please!) out of the building and to designated locations at the far-reaching edges of the schoolyard. Commonly, you might hear commentary such as, "No, there isn't time to get your coat/book bag/snack/class hamster. Please stop talking, all eyes should be facing in front, this is serious, do you want to stay after class? We will return to class when the fire department has given the 'all clear'." By and large students file out in an orderly fashion to complete the drill.

Fast forward some (many) years later the firm alarm is sounded in suburban office complex. Depending upon the evacuation plan (which is generally communicated to employees via email multiple times by the facilities department or building management) employees may be required to find their floor warden (who is wearing an orange hat and waving an orange flag) and follow them outside of the building in an orderly fashion to a pre-designated meeting place away from the building at the far-reaching edges of the parking lot. Once the alarm sounds, heads pop up from cubicles. Commonly, you might hear commentary such as, "...um, does anyone know if there was a scheduled fire alarm testing today? Good grief that's loud, can someone turn that off? Is that meant for us? Do we really need to evacuate? Isn't this just a drill? Who was my floor warden again, where do we go? Okay, I'm coming, just let me finish this call, send this email, finish this thought, grab my phone, get my purse, collect my laptop, get my keys..."

This is perhaps (assuredly) an oversimplification. And certainly, in a post 9/11 world, the speed and efficiency with which a large downtown high-rise office building can be evacuated was proven to be instrumental in the saving of many, many lives: an estimated 13,000 to 15,000 people are estimated to have evacuated from the World Trade Center. However, interesting insight on employee behavior can be gathered from a review of what makes people comply with the evacuation directive. Research indicates that there are three factors: personal, organizational, and structural. Released in

2003 the Mailman School of Public Health at Columbia University in conjunction with the CDC initiated, "The World Trade Center Evacuation Study," a multiyear research study designed to assess factors that affected evacuation of the two WTC towers.

Study respondents indicated that there were four issues impacting their decision to evacuate 1) their ability to walk down multiple flights of stairs; 2) their previous experience in evacuation of a WTC tower, including knowledge of stairwell locations and whether stairwells actually led to street level exits; 3) concern over leaving without the approval of managers; and 4) lack of information regarding what had occurred, what floors were involved, and lack of direction on how to respond.

The study further indicated that after a decision to evacuate was made, many stopped to attend to last-minute activities (e.g., making telephone calls, shutting down computers, or gathering up personal items). Deciding which route to take (e.g., stairs or elevators) might have delayed evacuation progress for others.

"In my experience there is a clear difference between fire drill compliance by children in elementary school and fire drill compliance by adults in the suburban office building setting."

Progress was reportedly slowed for some poor physical condition or inadequate footwear. Some persons also delayed their progress to stop and assist others.

Two major organizational factors affecting evacuation were identified: 1) workplace preparedness planning and training, including evacuation drills and 2) inadequate risk communication. An announcement broadcast in WTC 2 (South Tower) shortly after the first aircraft had struck WTC 1 (North Tower) urged persons to remain in the building and likely led many to return to their workstations.

"The most essential aspect of any policy or procedure is that it has been widely adopted and understood. The most important competency of any compliance officer is the ability to communicate. Adults need the why. Communicate the why."

Given the results of the 2003 study, what might be the difference between elementary school compliance with the fire alarm and cubicle dwelling office workers? Children aren't given a choice, they are compelled to evacuate and given their experience with the world may be more compliant towards authority figures in general. When the alarm sounds for the adults, they perceive a choice to evacuate or not. Adults always need the why.

Fire drills and evacuation procedures are merely one aspect of a holistic business continuity and corporate disaster preparedness plan, but the analogy can be extended to other critical areas necessitating an employee response. How do we as help to ensure that our critical testing of the plans is taken seriously? The study of compliance and the work of compliance officers has some fundamental truths, rooted in common sense. The most essential aspect of any policy or procedure is that it has been widely adopted and understood. The most important competency of any compliance officer is the ability to communicate. Adults need the why. Communicate the why. Additionally, the culture of the organization will help to demonstrate the serious business that are our continuity tests and planning.

Employees see that senior management takes time to participate in these tests and takes them seriously, senior leaders need also to proverbially line up and file quietly to their designated spot. Results of tests are evaluated thoroughly. It's true that we test to determine weakness. Then, we attempt to shore up the weakness and we test again, and again, and again, the fire department might have called the "all clear" but the real work begins when we get back to the classroom… or the cubicle.

Barbara-Ann is an attorney and adjunct lecturer with over twenty years of compliance experience. Barbara-Ann currently serves as a Product Marketing Director/ Regulatory Compliance Analyst at Aravo Solutions, Inc. and teaches "Compliance Practice Skills" at Suffolk University Law School and Boston University Law School. Barbara-Ann formerly served as the Director of Programming and Education at Compliance Week, Securities SME at Wolters Kluwer Financial Services, global chief compliance officer for Arete Research, a limited-purpose, FINRA-registered broker/ dealer specializing in equity research. Barbara-Ann also held compliance roles at Fidelity Investments, JP Morgan Invest, Standish Mellon Asset Management, and Babson Capital Management. Barbara-Ann holds a BA from Suffolk University, a JD from Suffolk University Law School, and an LL.M. from Boston University School of Law.

The Power of Information Sharing in Business Continuity Management

A Conversation with Andrew Goldman, Head of Business Continuity and Supply Chain Risk Management at MilliporeSigma

Andrew Goldman
Head of Business Continuity and Supply Chain Risk Management at MilliporeSigma

"In sports, you never root for somebody to get injured... helping other companies or other individuals understand how to better manage their risk is really important. Work together to ask how to prevent supply disruptions."

Risk & Resilience Magazine sat down with Andrew Goldman, Head of Business Continuity and Supply Chain Risk Management at MilliporeSigma, a division of Merck KGaA. Andrew holds 20 years of experience, focusing on supply chain operations and operational excellence. For our conversation, we discussed his work in business continuity management and supply chain risk management, where he is responsible for the development of these plans across manufacturing and distribution sites. These plans include end-to-end supply chain risk assessments for critical products, as well as disaster recovery plans, including recovery timeline objectives.

Thanks for sitting down with us, Andrew. Tell us- what are your top priorities for improving business continuity in 2022?

Our company plays a critical role in life science and biotech- we support manufacturers of life-saving drugs and vaccines that are addressing COVID. It's all about making sure that our products are available because ultimately, they save lives. So, in my role, it's about minimizing supply chain disruptions and the first step is identifying risks across our network. My role starts with the business impact analysis, a critical focus area in terms of understanding which products and which supply chains are the most impactful in terms of saving lives and supporting the global effort to end the pandemic. Then, the focus area becomes more tactical in terms of ensuring that we have our business continuity plans and end-to-end supply chain risk assessments in place to address these critical products and critical manufacturing sites.

How should business continuity strategies evolve for the upcoming year following recent challenges like data breaches, the pandemic, etc.?

These challenges affect all industries. I think the priority for organizations should be to ensure that they have a program in place and dedicated resources to start looking at this risk. Priority number one should be to make sure that you are starting to take this topic seriously and start to be proactive in terms of identifying potential failure points across your supply chain, assessing those risks appropriately, and then mitigating where necessary or putting contingency plans in place if mitigation actions aren't possible.

Priority number two is making sure that this program or resource is properly supported from the executive level. This means getting visibility into the risks identified in business continuity plans or supply chain risk assessments and making sure there's support. We also need support from the manufacturing sites of

the distribution network in terms of putting the work in to complete those assessments or continuity plans, and then ultimately taking the mitigation actions that accompany it.

Have you seen an uptick in due diligence for third parties based on the pandemic?

I can certainly speak to our industry and how critical our products are even before COVID. If we have a supply chain disruption on our end it can lead to manufacturing shutdowns for drug manufacturers and then ultimately lives could be lost here. It's always been a very, very hot topic and there's always been a lot of due diligence from our customers and from other third parties in terms of understanding what we're doing to mitigate and prepare for potential disruptions. With that said, we've seen an uptick as a result of the pandemic, because now we have this whole new line of products including COVID-related therapeutics, both in development and the start of the commercial level, as well as the vaccines that weren't in existence three years ago.

How important is visibility and eliminating organizational silos when it comes to business continuity plans?

When it comes to supply chain management, communication and visibility are critical. There's this great concept in supply chain literature about a bullwhip effect where one small change is made and your decision can cause massive disruption and chaos downstream. Regarding business continuity management and business continuity plans this is certainly the case, but I see it at a few different levels. When plans like supply chain risk assessments are being conducted, they must be a cross-functional exercise because there are inputs that certain individuals will have that can drastically alter the risk score for either raw material or a piece of equipment, or something along the logistics chain. If they're not included and if there's no communication, these things will certainly be ineffective… You need to have a cross-functional effort in conducting these risk assessments and with that lens, to look at supply chain risk.

"Priority number one should be to… start to be proactive in terms of identifying potential failure points across your supply chain, assessing those risks appropriately, and then mitigating where necessary or putting contingency plans in place if mitigation actions aren't possible."

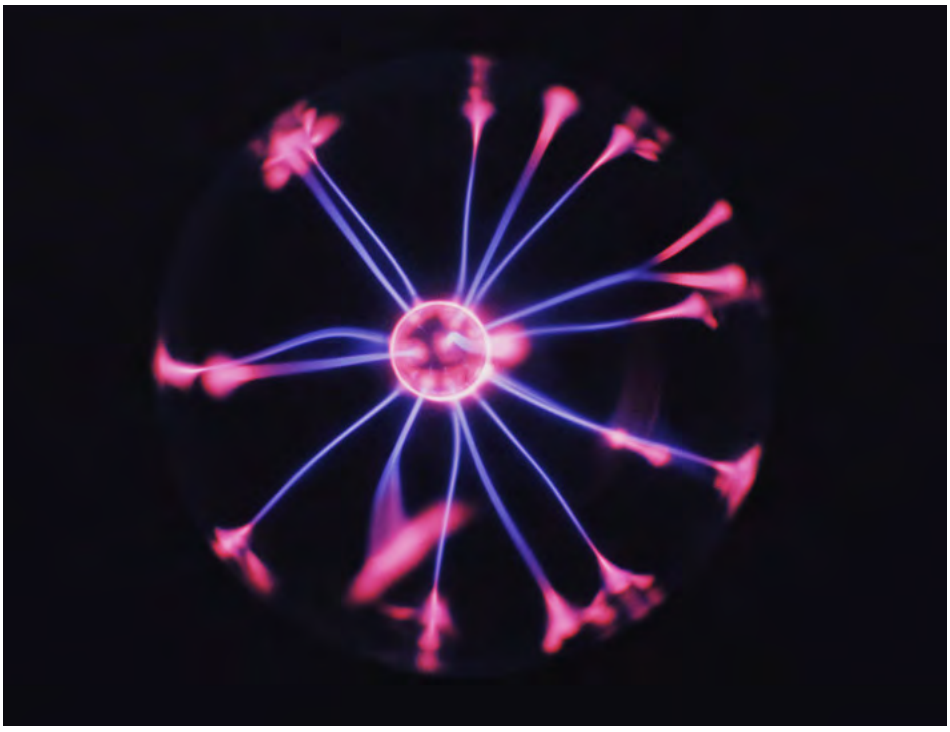
In many cases, the disruption has already happened. It's no longer a risk, it's an event. Having a nimble organization that can communicate and share knowledge upstream and downstream throughout the supply chain can mitigate the potential impact of disruptions.

What are steps organizations can take today to help boost their business continuity plans?

Make sure that you have dedicated resources where it's not just 10% of somebody's time. Ideally, there is at least one individual that's running the program full-time. If they don't have anything in place there's a lot of literature and best practices out there to help an organization launch the program, so I encourage you to do research. This topic has just skyrocketed over the last decade, with COVID even more so.

There are a lot of consortiums out there as well that are helpful. The opportunity to be able to collaborate across industries to understand how other companies are handling these topics is really helpful to see, especially since some of these programs are still in their infancy.

In sports, you never root for somebody to get injured. I think it's similar to this topic as well- helping other companies or other individuals understand how to better manage their risk is really important. Work together to ask how to prevent supply disruptions because ultimately society suffers when there are major supply chain disruptions, even if it's not a product you're purchasing. Nobody likes waiting longer for items or seeing shelves bare. There is a lot of collaboration and a lot of information sharing which is fantastic. That's why it's a pleasure to be able to share whatever knowledge I can- it's a very important topic.



THOUGHT LEADERSHIP

Resilience

What the Rest of Us Can Learn from the Financial Sector

Matt Kelly
Editor and Founder of
Radical Compliance

RADICAL COMPLIANCE
SHARP THINKING ABOUT COMPLIANCE, AUDIT AND RISK

Businesses today are besieged by disruption, and that makes resilience — the ability of an organization to withstand disruption and keep providing services to customers — more important than ever before.

Of course, that's an easy point to say; putting the idea into practice is the tricky part. How, exactly, does a business go about developing resilience? What capabilities should the company foster, especially when the disruptive threats range from pandemics to cybersecurity to climate change to supply chain collapse, and much more? What reports does one give to the board?

Compliance officers and risk managers need to answer those questions somehow. So many threats with the potential for severe disruption exist today that "operational resilience" is no longer just some esoteric term of art thrown around in a few highly regulated industries. It's a business imperative. Every organization needs to get better at withstanding disruption.

One place to look for guidance on that journey: the financial sector.

The Financial Sector & Resilience

Regulators in the financial sector have talked about operational resilience for the better part of a decade. That's because banks and other financial firms (a) play a crucial role in supporting the greater economy, and (b) are enormously complex operations with a huge range of enterprise risks.

More to the point, those regulators learned painful lessons during the 2008 global financial crisis (and in subsequent mini-disasters, like the "flash crash" of 2010) about just how much damage disruptions in this sector can cause. The agencies have closely watched financial firms' ability to withstand disruption ever since and churned out numerous pieces of guidance about operational resilience along the way. For example:

- In 2017, a Treasury Department report flagged banks' reliance on third technology providers as a potential risk that needed attention. If those tech providers failed or suffered a cybersecurity breach, the report said, that could threaten the whole financial system. So the banking sector needed some way to assure it could persevere through such failures.

- FINRA, the regulator for broker-dealers, has published several pieces of guidance over the years explaining how firms should prepare for pandemics, weather disasters, and other disruptions. The advice all flows from FINRA Rule 4370, which requires broker-dealers to have an effective business continuity plan.

- The Federal Reserve (and other banking regulators) published a paper in 2020 outlining several practices large banks can follow to strengthen operational resilience.

We could go on from there. Some of the guidance focuses more on vendor risk and how to manage it; some talks about the duties financial firms have to keep providing services to customers. Most of the material is light on jargon and details specific to the financial world, so risk managers in any industry can give it a read and put it to good use.

Lessons We Can Learn

When one does give the guidance from financial regulators a close read, several themes quickly emerge.

First is **the importance of IT risk management**. Especially in today's world, where hybrid work environments are the norm and employees might need to isolate themselves at home on short notice, the ability to keep providing services amid disruption depends on technology. So, a company's ability to manage its IT systems — for privacy, cybersecurity, data availability, and the like — is paramount.

Second, because most corporate IT systems now depend on cloud-based technology providers, **IT risk management and third-party governance have fused into a single challenge**. That is, a company **can't** keep its IT risks in check without effective third-party governance. Your ability to identify and monitor third-party relationships is crucial to operational resilience because those third parties are crucial to the technology you use to provide services to customers.

Third is the **importance of business continuity planning and disaster recovery**. For example, these plans need to consider how disruptions to your physical assets (say, a weather disaster shutting down offices and data centers) could pressure your IT assets (everyone working from home, handling confidential data with personal devices and unknown networks). The plans should first address how to restore mission-critical services immediately, and then a resumption of normal services as soon as possible.

Those are the points that financial regulators have stressed to banks, broker-dealers, clearinghouses, and other financial firms for at least a decade — and they apply just as well to any large organization that wants to assure its resilience in the modern world.

"So many threats with the potential for severe disruption exist today that operational resilience is no longer just some esoteric term of art thrown around in a few highly regulated industries. It's a business imperative."

Turning Those Ideas into a Program

As sensible as the above ideas may be, companies still need to turn them into an actual program that can improve operational resilience. We can break that down into one important decision to make and several important capabilities to develop.

The important decision is **who takes ownership of this responsibility**. The most logical candidates are either the CISO or a chief risk officer since many of the duties for both roles already relate to operational resilience. If your company doesn't have a chief risk officer or head of enterprise risk management, or if your CISO can't devote the necessary time, a chief audit executive could do the job too.

Regardless of who leads your resilience project, in practice, **he or she will need plenty of help and input from compliance officers and leaders of the operating business units**. If you already have an in-house risk committee that reviews risk management periodically, don't be surprised if that committee evolves into a "resilience advisory committee" of some kind.

The important capabilities you will need to develop revolve around **understanding what data, processes, and third parties you have**, and how all those things relate to your operations and compliance obligations.

For example, you'll need to identify the business processes that are mission-critical to your company, and then map out the data and third parties necessary for those

"IT risk management and third-party governance have fused into a single challenge. That is, a company can't keep its IT risks in check without effective third-party governance."

processes to run normally. That lets you understand which assets and third parties are critical to your company's resilience, so you can prioritize their availability. Maybe that means creating redundant data archives; maybe it means maintaining a list of emergency suppliers or strengthening contract clauses with the suppliers you have. Either way, resilience first depends on identifying your critical business processes and mapping out the assets that make them work.

Conclusion

Building operational resilience is no easy task. A company must first identify its critical business processes, data, and third parties, and the relationships among all three. Then it needs to catalog the threats to those mission-critical items and develop strategies to assure that those critical processes can continue even when the threats come to pass.

That's complicated work. To succeed, a large enterprise has to use a proven technology tool. There's simply too much at stake (and too many details to track) to rely on spreadsheets, emails, and manual processes. A company should equip itself accordingly.

Then get on with the task of building operational resilience, because the number of threats to modern business won't be receding any time soon.

Matt Kelly is the founder of Radical Compliance, which provides consulting and commentary on corporate compliance, audit, governance, and risk management. Radical Compliance also serves as the personal blog for Matt Kelly, the long-time (and now former) editor of Compliance Week. Kelly writes and speaks frequently on corporate compliance, audit, and governance, and now works with various private clients to understand those fields and to develop go-to-market strategies or provide other assistance in reaching audiences of compliance professionals.

Examining Financial Health Ratings and Supply Chain Resilience

A Conversation with James H. Gellert, Chairman & CEO of RapidRatings

James H. Gellert
Chairman & CEO of RapidRatings

RAPIDRATINGS®

For the second issue of Risk & Resilience Magazine, we sat down with James Gellert, Chairman & CEO of RapidRatings. RapidRatings is a SaaS technology company providing financial health ratings on public and private companies globally.

Thanks for sitting down with us, James. To begin, can you explain how your financial ratings or assessments differ from a credit report?

Traditional credit reports focus on a company's ability to pay its bills… which is a very limited perspective of a company, and financial health ratings go significantly deeper. Financial statements of companies look deeply at longer- and shorter-term aspects of the business, how well positioned is it to compete against its peers? How resilient is it? What kind of working capital and cost structure efficiencies does it have? How well is it able to generate returns on its asset size and on its sales volumes, things like that, as well as what its shorter-term risks are from a default perspective. All of that creates a set of lenses into a company that gives a much more dynamic perspective on risk and opportunity than a credit report.

One key element in supply chain risk is understanding suppliers' ability to grow with you as well as avoiding the pitfalls where a weakness in a supplier can cause disruption or reputation risk, or some other degradation of a risk category. Credit reports just don't give that kind of insight.

What's the connection between financial risks and other risk areas?

Financial risk is an underpinning of a company's ability to be resilient in the variety of risk areas that supply chain risk managers have to focus on; things like quality of product, timing of delivery, their research and development, commitment, their product development timeline, as well as risk areas like compliance, ESG, and cybersecurity. Financial is intertwined into all of these other areas and in a supply-chain context, it's a leading indicator of whether companies are going to be a good partner or may have problems. The earlier you can identify those problems and collaborate with the private company or their supplier, the better off you're going to be able to manage risk and continue to work with them. It's not just about trying to eliminate weak suppliers. It's about trying to lean in with the suppliers that you have a reason and desire to work with on a longer-term basis.

How has the pandemic shined a light on the importance of financial health ratings?

Financial ratings have always been important. Understanding the financial health of suppliers is something that should have been done for a long time, and the pandemic has only shined a brighter light on the need—understanding partners and how resilient they are, and how well they are able to invest in their own futures and be a strong partner going forward. The pandemic has also created more focus on supply chain risk at the board and C-suite levels, across organizations, and among shareholders. Ultimately that means that supply chain organizations have to do more risk management and financial assessments of their suppliers than ever before because there's more scrutiny.

"Understanding the financial health of suppliers is something that should have been done for a long time, and the pandemic has only shined a brighter light on the need."

Have you seen an uptick in requests for due diligence for third parties based on the pandemic?

The consistent theme across clients of ours in different industries, financial institutions, and non-financial institutions has been more focus on their current suppliers and on more suppliers. And why is that? In the past, there's been a trend towards lean manufacturing, just-in-time manufacturing, and a consolidation of business with suppliers. There's more sole-source supply and the pandemic has demonstrated that there's a major flaw to that plan. If your sole-source suppliers are experiencing disruption you're in a lot of trouble. More companies are looking to evaluate redundancy in their supply chains and are going to add more dual sources, where before they might've been content working with one major supplier in an area of criticality… more diversification in supply chains means more suppliers to evaluate and a greater need to have an automated and predictive analytics toolset around doing all of that.

Do you have any best practices you can share for those that are looking to manage programs through challenging times?

Today, any practices are about about data cleanliness and consistent identification and evaluation of suppliers. We see lots of companies that are still early in their journey towards digitalization and creating clean data inside of their organizations. That goes right down to things like: can you provide a clean contact list of all of your suppliers, or can you determine which suppliers are most critical as measured by two or three different lenses of criticality? Companies have to be able to do these things in order to manage risk because you have to know who your suppliers are and you have to be able to contact them.

You also have to understand who your suppliers are and internally embrace the idea of collaboration with them because collaboration leads to transparency and transparency leads to better business relationships. As long as you are looking to understand them better through financial evaluations, cyber security evaluations, and ESG compliance, you need more information from them. If they don't trust you, they don't want to provide the information. But if they trust you and believe that there's a commercial benefit to the transparency, they'll provide it. We see the most successful and sophisticated programs embracing the ideas of collaboration and trust and being able to work more closely with our suppliers so that both sides benefit.

"You… have to understand who your suppliers are and internally embrace the idea of collaboration with them because collaboration leads to transparency and transparency leads to better business relationships."

James H. Gellert is the Chairman and CEO of RapidRatings International. Previously, he was the Managing Partner of Howland Partners, LLC, and Howland Securities LLC—firms that provided consulting, business development, capital raising, and M&A advisory to companies in the financial information and technology markets. Prior to those positions, he served as CEO of a number of technology companies including wireless software and research companies SkyScout and Unstrung.

James is the President of Young Audiences/Arts for Learning Inc, the nation's leading source of arts-in-education services. His views are frequently sought by major media outlets as well as federal regulators and the United States Congress.

ARTICLE

Managing Through Crisis:

Lessons Learned from the Street to the C-Suite

By, Barbara-Ann Boehler, with contributions from:

Fabiana Lacerca-Allen
Senior Vice President and Chief Compliance Officer at Aimmune

Randy Bagwell
Senior Director International Services-US Programs at the American Red Cross

Donna Kinsey
President and CEO of Training Enhancement Center

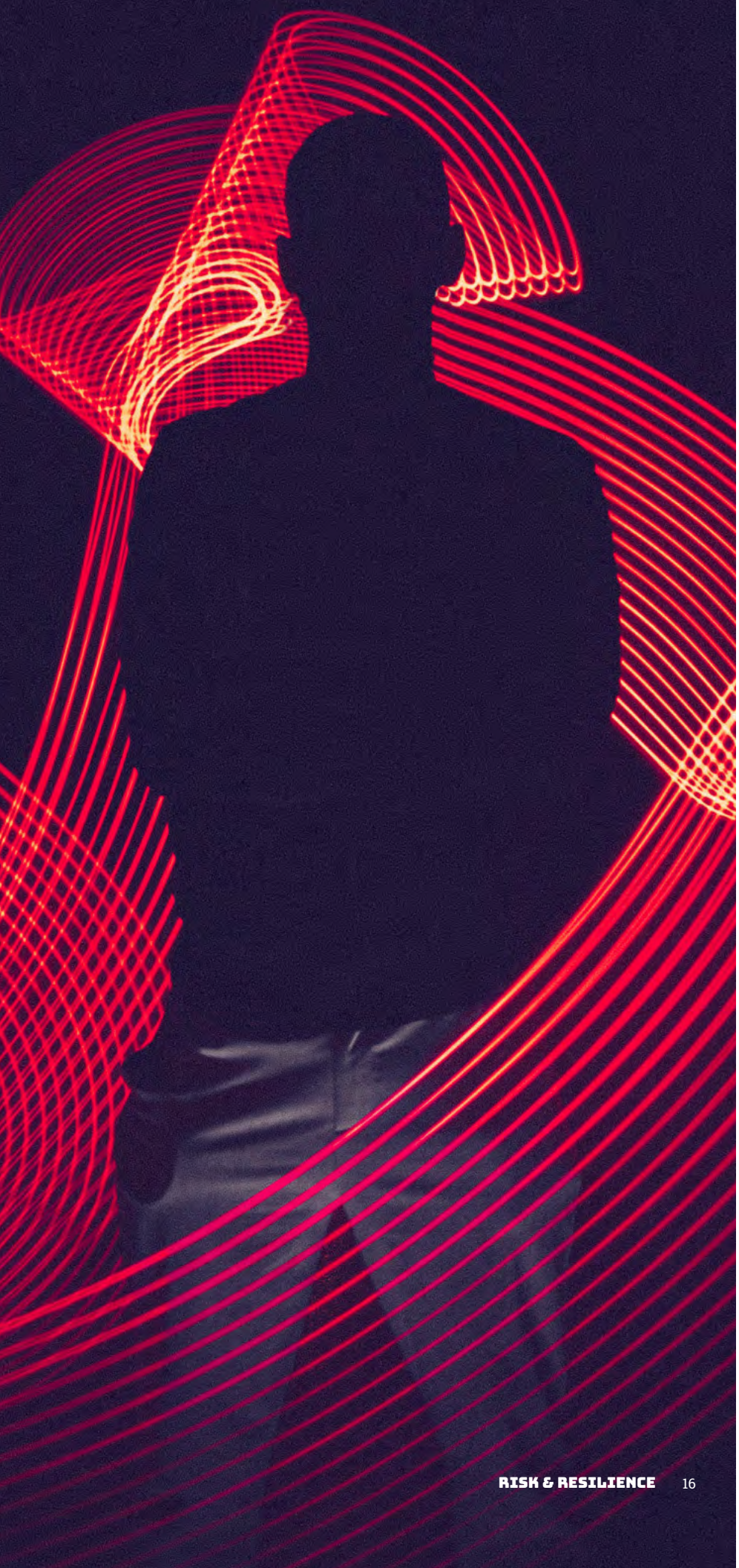
Early in December, Aravo had the pleasure of (virtually) sitting down with Fabiana Lacerca-Allen, Senior Vice President and Chief Compliance Officer at Aimmune in San Francisco, CA, Donna, Kinsey, President and CEO of Training Enhancement Center in Elkton, VA, and Randy Bagwell, Senior Director International Services - US Programs at the American Red Cross currently working in Tokyo, Japan.

Randy, Donna, and Fabiana all have first-hand experience in managing through crisis – the kind of crisis in which life and death often hang in the balance. Randy spent 36 years as an officer in the Army and currently works at the Red Cross; Donna spent nearly 30 years in the North Miami Police Department, and currently provides training to help corporations and their senior leaders manage through crisis; and Fabiana grew up in politically charged Argentina and experienced multiple kidnapping attempts.

Their first-person experiences in managing through crisis have given Randy, Donna, and Fabiana unique points of view and the ability to offer practical guidance. The conversation centered around how compliance officers (who are on the proverbial front lines of corporate crisis) might learn from their experiences and apply a common framework to both the everyday and exceptional (hello 2020) challenges facing them. Clear themes emerged during our conversation focusing on planning and risk management, developing a strong team and surrounding yourself with talented collaborators, and focusing on training staff in crisis management response.

Crisis Management is Risk Management

There is very little magic in risk mitigation and in ensuring that your organization is prepared for the unknown. It is an analysis of data, thoughtful planning, and consistency. However, we as compliance officers can take some comfort in the fact that many of the same skills that help us to design solid compliance programs are those that we employ to help manage through any challenge. Randy shared his philosophy on managing through crisis, it is based on his observations of his time in the military. Randy indicated, "the military does certain things well with risk.



They assess it well; they have programs and tools for risk mitigation, and they accept risk."

Randy described his approach to risk management as a methodical paper-based exercise where risk is evaluated in quadrants, taking into consideration how likely the risks are to occur and what the potential impact is if they do occur. So, perhaps the organization may be comfortable with taking on risk as long as the potential impact is minimal. According to Randy, "when you get to the top right of the quadrant and you get to a high impact and a high likelihood of occurring, you really have to plan against that risk, and really invest in that quadrant." The evaluation of risk is one of balance.

A methodical risk assessment based on a repeatable and consistent framework, e.g., the evaluation of potential risks, the likelihood of occurring, and the following impact analysis and mitigation plan is also best practice in any kind of organization, no matter the size, complexity, or industry. The analysis distilled from this thorough assessment of risk is essential data to take away to inform where resources and attention need to be focused. Additionally, the data helps us to have critical conversations with commanding officers, CEO, and board of directors alike.

Crisis Management Is a Team Sport

While certainly being prepared for the unknown is about planning, evaluating, mitigating, and balancing risk, having a strong team in place is a critical component to successfully managing through

"When you get to the top right of the quadrant and you get to a high impact and a high likelihood of occurring, you really have to plan against that risk, and really invest in that quadrant."

– Randy Bagwell

conflict to resilience. Fabiana shared the importance of having the right people in the right places. In addition to having both Donna and Randy in her corner in a crisis, Fabiana shared that, "having the right people in the right place having the right discussions applies to any scenario." A strong team is a key aspect of a strong mitigation plan, Fabiana further notes, "I think none of us expected a global pandemic in the way that this happened. The speed that this happened and with the different reiterations that it's happening now. The ability to assess a situation and make a quick, instinctive decision is important."

> **"Training is so important during an emergency situation, you will absolutely react how you're trained"**
>
> – Donna Kinsey

Fabiana described her ideal team as those with, "high emotional intelligence, and high intuition" as well as "leaders who others will follow." The concept of trust in leadership was endemic to the conversation, and while the ability to make a swift decision was important, leaders are encouraged to thoroughly investigate and be consistent so as not to undermine their authority, Fabiana noted, "You should show that you follow the same processes every single time. It gives you the best chance of success." Randy cautioned, "If you were too quick trying to gather the facts and tried to put it in the best light, but end up being wrong, it undercuts trust, and you can never recover fully from that initial response." Additionally, as Donna points out, "actions speak louder than words, you have to perform exactly how you would expect your officers or your employees to perform."

Successful Crisis Management Takes Practice

Compliance officers share several key competencies with those in the military and in law enforcement. In addition to the appreciation for a thorough (and thoughtful) approach to risk assessment and surrounding themselves with strong collaborators, compliance officers know the value of training. Randy referenced an axiom, "Training doesn't make perfect, it makes permanent." In the heat of the moment, employees will revert to what they know. We may recall from our grade school days the directive to "stop, drop, and roll" during a fire. Similarly, responses during crisis often become muscle memory. Donna indicated, "training is so important during an emergency situation, you will absolutely react how you're trained."

Scenario-based training is a particularly effective tool. Randy indicated, "too often people worry about training against a predicted crisis, however, you are training the process of the crisis, this is a template that you can put up against any situation that comes along."

Additionally, tremendously useful information can come out of a less than perfect response to a training scenario. Fabiana noted, "strong leaders learn from their mistakes. Every human being after this pandemic is going to learn differently about a reality that has changed so rapidly across the globe. We're going to study differently, travel differently, work differently."

Lessons Learned

Randy, Donna, and Fabiana shared valuable perspectives on maintaining calm and managing through charged situations that are as applicable to them in the military, government, and law enforcement arenas as they are in the C-Suite, the Board Room, and the halls of the office building (virtual or brick and mortar). The focus on fundamental planning and managing risk, the concepts of developing a strong and agile team, and preparing staff through training will serve you as well in your compliance practices. If you would like to listen to the entire webcast you can access it in Aravo's resource library.

"I think none of us expected a global pandemic in the way that this happened... The ability to assess a situation and make a quick, instinctive decision is important."

– Fabiana Lacerca-Allen

About the Contributors:

Randy Bagwell:

As the Senior Director for the Asia Pacific Division, Randy Bagwell is responsible for all American Red Cross services provided to the U.S. military in Japan and Korea. In this role, he oversees fourteen Service to the Armed Forces offices that deliver emergency communications messages, provide disaster response on U.S. military installations, and teach training services classes. Additionally, Randy serves as the senior International Humanitarian Law expert for the American Red Cross.

Before joining the American Red Cross, Randy was a career U.S. Army officer serving as an officer in both the infantry and the Judge Advocate General's Corps. His last position on active duty was as Dean at the U.S. Army Judge Advocate General's School in Charlottesville, Virginia. This school is the only American Bar Association accredited law school within the U.S. federal government.

As a Judge Advocate, Randy held several senior leadership positions and advising military commanders at all levels. He served as the Staff Judge Advocate for U.S. Army Alaska, 3rd Infantry Division, and I Corps. Randy's combat deployments include two deployments to Afghanistan and one to Iraq. Randy retired from the Army in June 2018 at the rank of colonel with over 36 years of service. He has four times been awarded the Legion of Merit and three times the Bronze Star for meritorious service. Randy is a frequent speaker and writer in IHL and legal leadership.

Donna Kinsey:

Major Donna Kinsey is a retired veteran law enforcement officer who has been actively involved in training and program development for over 30 years. During the course of her career, she was awarded the FBI Women in Law Enforcement Leadership Award, and was the three-time recipient of the Department's top honor, the Administrative Excellence Award.

While serving in the Career Development Unit, she instituted the Department's first set of professional hiring standards. Her accomplishments include being the first women in the history of her department to attend the FBI National Academy, (session # 222). She was appointed as the Department's Range Master, responsible for the firearm qualification and training of all sworn members of the Department. She developed and instituted the Department's Law Enforcement Response to Active Shooter protocol, administering the training at local schools including Johnson and Whales University, where she served as an adjunct professor. She was editor and feature writer of the North Miami Police Department's first Annual Report, saluting women in law enforcement and military women who lost their lives in the line of duty.

Post retirement, certified by the Florida Department of Law Enforcement as a high liability trainer, she continues to develop and conduct general and high liability training seminars. Donna completed her Bachelor's Degree in Organizational Leadership at St. Thomas University, Miami, Florida and earned her Master's Degree in Public Administration at Barry University, graduating summa cum laude from both institutions.

Fabiana Lacerca-Allen:

With over 30 years of experience in Compliance and Legal, Mrs. Lacerca-Allen has been a leader in developing and implementing global compliance programs within Top Fortune 100 companies. She has extensive experience delineating compliance strategy, leading global teams and negotiating, implementing, and executing on corporate integrity agreements, deferred prosecution agreements and consent decrees.

Ms. Lacerca-Allen currently serves as a Board of Director Member at Shield Therapeutics, and The Center of Excellence in Life and previously ArthoCare Corporation. Prior to joining Aimmune Therapeutics, Mrs. Lacerca-Allen held several leadership positions at Elan Pharmaceuticals, Mylan Laboratories, Bristol Myers & Squibb, Microsoft, Merck Sharp & Dohme, AT&T Capital.

Mrs. Lacerca-Allen received her Juris Doctor degree from the Universidad de Buenos Aires and obtained her LLM degree from UCLA where she was the recipient of 1992 UCLA's tuition waiver based on merit and recognition. She has been recognized by Compliance Week as Top Minds 2019, Hispanic Executive Magazine as Legal Industry Leader and by The Guardian as Women in Leadership, Inspiring Leaders among other recognitions.

INTERVIEW

When You Can't Outrun Disaster: How Risk Intelligence Helps Companies Monitor, Mitigate, & Recover

A Conversation with Bob Miller, CEO of DisasterAWARE Enterprise

Bob Miller
CEO of DisasterAWARE Enterprise

DisasterAWARE Enterprise by Tenefit

"I think every corporation in the United States today has to be working on resilience in some form."

Risk & Resilience Magazine sat down with Bob Miller, CEO of DisasterAWARE Enterprise, a cloud-based, SaaS risk intelligence platform for monitoring global hazards.

How does hazard monitoring differ from other kinds of risk intelligence?

The key about hazard monitoring is, you know about the hazard long before it creates disruptions. You get all these data sources, you run it through machine learning and artificial intelligence, and you say there's a hurricane forming in the Caribbean. It could be six days away from the mainland, but hopefully what you're going to do is identify the hazard with enough time so that you can mitigate the damage it does. And so, risk intelligence is theoretically when you've got the information that tells you what the hazard and damage are going to be.

The other part to this is making organizations aware of what the potential impact of this hazard's going to be in a timeframe that somebody can either mitigate or, in a best-case scenario, actually improve the business outcome based on proactive planning.

What is the driving need for monitoring risk?

Let me give you a real-life example. We have a customer, a large petroleum company who had offshore drilling rigs in the Gulf of Mexico. For an upcoming hurricane, they had to decide whether to shut the rigs down and evacuate them. You can imagine how expensive it is to shut a drilling rig down, evacuate all the people, and then have to bring them back and restart it. But by us being able to identify this early and giving them days to figure out what to do, they had the time to run it through their own decision analysis. In the end, they decided to evacuate the rigs. Early identification, monitoring, and decision-making are so important. The cost of shutting down and evacuating was very expensive, but there were no lives lost or injuries.

I think the thing that is causing everyone to put so much focus on hazards, in general, is climate change. In the past, a company may have experienced one

or two of these events every couple of years. Now, they're experiencing multiple events each year. As a result, companies are saying this is something they need to deal proactively with on a regular basis. So, they need risk intelligence and impact intelligence, and they need it as close to real-time as possible.

How does hazard monitoring fit into an organization's business continuity management strategy?

I think it goes back to the fact that we're experiencing a lot of things that we didn't experience very frequently in the past. And I think the pandemic has really highlighted how fragile our supply chains are. Companies are now looking to improve, and need the advantage of a global supply chain that's still resilient. Disruptions happen and you need to be able to adapt to them as rapidly as possible. And to do that you need impact data.

The more warning you get, the more you're able to minimize significant impacts… the key thing is that every large organization usually has a group whose whole job is to determine where are they going to have disruptions and how they'll still be able to meet their business objectives. And so, relative to business continuity, the whole idea of what we do is to give you the time.

How can hazard monitoring help companies increase the resilience of their supply chain?

It's about getting ahead of risks and having an outlook that acknowledges the risk and deals with the fact it's going to happen. We need technology that mitigates risk and avoids locating critical facilities (such as a nuclear power plant) where there's the likelihood of a tsunami, for example. I think every corporation in the United States today has to be working on resilience in some form.

Some of the clients we're currently working with have outlets that number in the tens of thousands and suppliers that number in the thousands. They're trying to get a global picture. We're living in a world where every corporation needs to have a picture of where their exposures are and where the safety of their employees is at risk. We can only supply the information. At the end of the day, humans have to make decisions. But our job is to give you the best information to hopefully help you make the best decision.

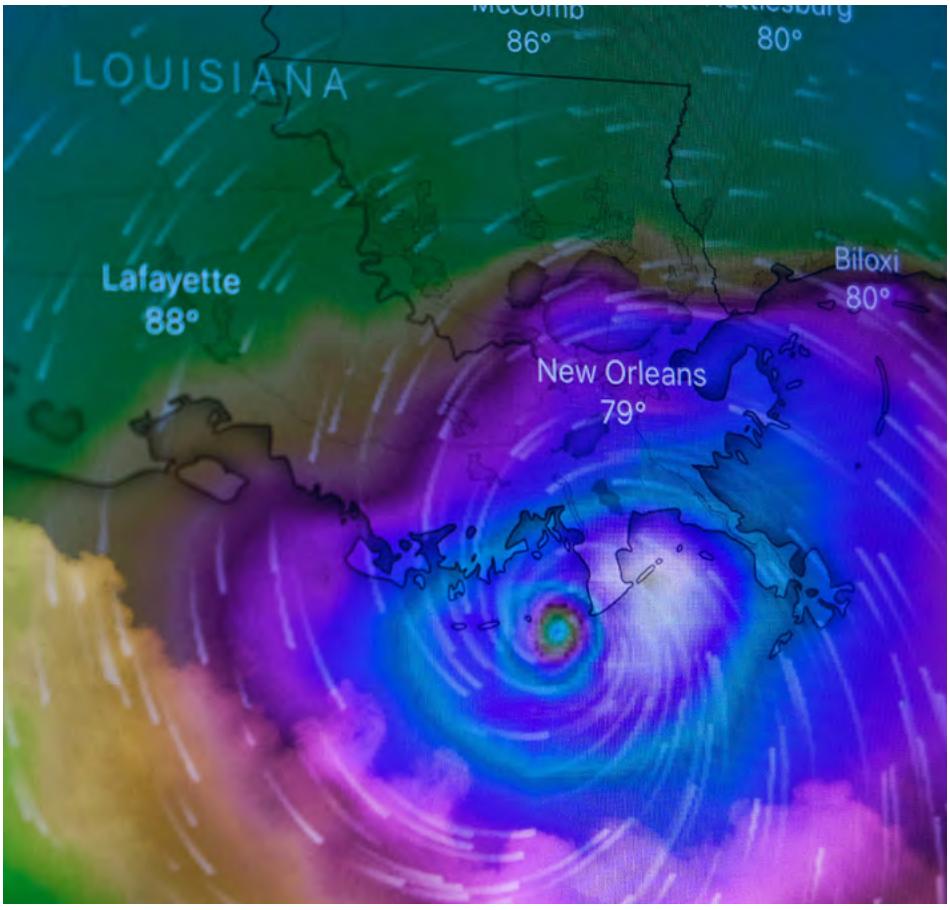
Looking ahead to this year, what sorts of disruptive events do you think organizations should be concerned with?

I don't think they're going to be very different from what we've been experiencing the last two or three years. The frequency will increase. But another area of concern where we're really going to focus attention on is manmade disasters such as active shooter events and civil unrest.

So, we're going to try to do more to get ahead of these things to give more of a warning roadmap into man-made disasters. What do you do after the initial warning? Where's the best place to shelter? Where are there emergency services on the scene? We can shift through an enormous amount of data, while also helping to avoid false positives.

And when it comes to manmade disasters, it's all about being hyper-local because, for example, a thousand people marching might be very disruptive to the factory that's across the street from it, but it may not be terribly disruptive to the store three blocks away. So, it has to focus on what impact it's having on a specific area. And that's what we hope our manmade product will provide- impact resilience and intelligence risk.

"We're living in a world where every corporation needs to have a picture of where their exposures are and where the safety of their employees is at risk."



Are there overlooked indicators that people should be paying attention to in terms of the vulnerabilities of their organizations and/or their vendors?

When people are looking at resilience, they should look into all possibilities, such as how long power grids will be down. What if I lose it for a day? What if I lose it for a week? What if I lose it for three months? We do provide impact analysis. We say, this is how many people are currently exposed, but by then you're in the fight. By the time we give you an impact analysis within three or four days, hopefully, you'll have that much to try to figure out how to deal with it. But it's always helpful if you thought about it ahead of time.

And it's not just the analysis, it's setting up the processes in your organization so that when something happens and you get the alert, you know what to do. This is how you keep your people safe. This is how you keep the company's assets safe. And this is how we all come back the next day or the next week, and continue our lives. That's the key thing you need a well-defined process and people trained to behave accordingly in the event that a disruption happens.

This interview has been edited for length and clarity.

Bob Miller is CEO at DisasterAWARE Enterprise and is a strong technology leader with more than 30 years of experience in both Fortune 500 companies and private startups. Prior to Tenefit, Bob was CEO of a number of technology companies including MIPS, which he led to its IPO. Bob is a distinguished alumnus of Bucknell University and earned an MBA from Stanford University.

"It's not just the analysis, it's setting up the processes in your organization so that when something happens and you get the alert, you know what to do. This is how you keep your people safe. This is how you keep the company's assets safe... And that's the key thing you have to have a well-defined process and people trained to behave accordingly in the event that a disruption happens."

Destinations on the Path to Organizational Resilience

Organizational resilience is comprised of many different types of programs, relying on everyone in an organization to step up and be empowered to help address disruptions. While each of these initiatives and programs vary in terms of complexity, they all play a role along the path to organizational resilience. Analyzing and improving upon each of these is necessary to becoming truly resilient.

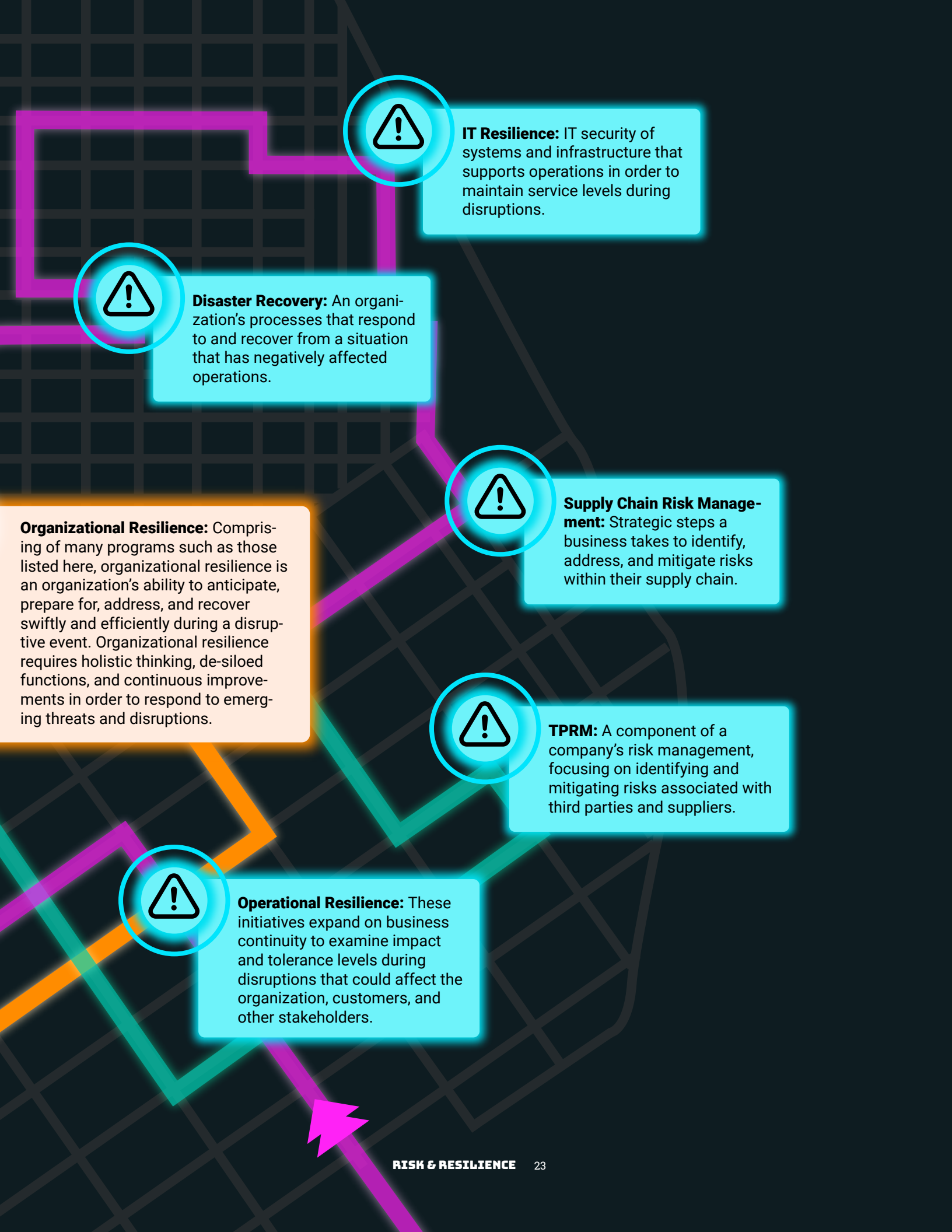
Cybersecurity: Processes and tools to protect critical systems and information from digital attacks. Within resilience, this includes cybersecurity of vendors and along the supply chain.

GOAL

Business Continuity Management: A framework for identifying and addressing organizational risks and maintaining normal business operations during disruptive events.

Crisis Response and Management: The processes an organization has to address a major situation or disruption that has the potential to cause harm to the business, the stakeholders, the public, or other entities.

Training and Development: Organizational resilience training helps build new routines and improvisation techniques so that employees and leaders are prepared to act comfortably and efficiently during uncertain situations.



IT Resilience: IT security of systems and infrastructure that supports operations in order to maintain service levels during disruptions.

Disaster Recovery: An organization's processes that respond to and recover from a situation that has negatively affected operations.

Supply Chain Risk Management: Strategic steps a business takes to identify, address, and mitigate risks within their supply chain.

Organizational Resilience: Comprising of many programs such as those listed here, organizational resilience is an organization's ability to anticipate, prepare for, address, and recover swiftly and efficiently during a disruptive event. Organizational resilience requires holistic thinking, de-siloed functions, and continuous improvements in order to respond to emerging threats and disruptions.

TPRM: A component of a company's risk management, focusing on identifying and mitigating risks associated with third parties and suppliers.

Operational Resilience: These initiatives expand on business continuity to examine impact and tolerance levels during disruptions that could affect the organization, customers, and other stakeholders.

BEST PRACTICES

Navigating the Path to Organizational Resilience

Hannah Tichansky
Marketing Campaign Manager
at Aravo Solutions

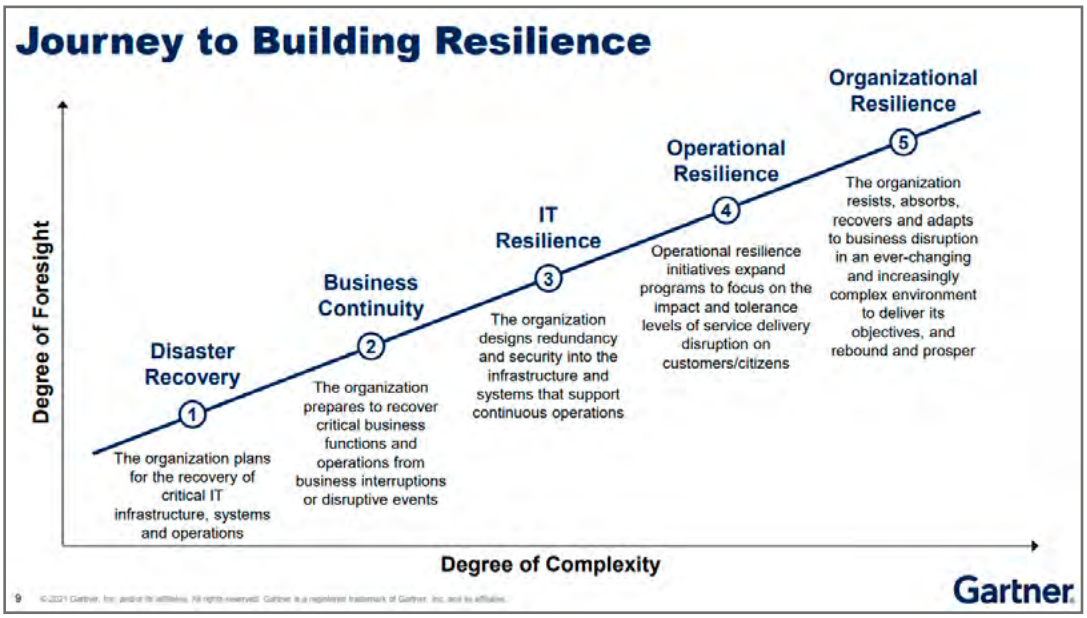
Resilience. It's more than a buzzword – it's catapulted into our daily conversations through the shared experience of having to confront significant change in our lives as we continue to live and work through a global pandemic.

"Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context. Enhancing resilience can be a strategic organizational goal, and is the outcome of good business practice and effectively managing risk." (ISO 22316:2017)

Resilience is a key business imperative, and enhancing resilience must be a strategic organizational goal. In this business landscape of increased uncertainty and considerable change, organizations must adapt to how they can better anticipate and respond to threats and disruptions confronting their extended enterprise. While they can't plan for everything in a changing environment, they can become more adaptive and responsive, putting them in a greater state of readiness for any risks that lie ahead.

Today, change is happening faster than ever. In this fast-paced environment, those who survive are shifting from 'the same old way' of doing things with fixed pathways and siloed information, to a much more unified, fluid, and agile approach. The path to resilience is going to take a fresh approach to people, processes, and technology.

"Resilience is a key business imperative, and enhancing resilience must be a strategic organizational goal."



A Shift to Integrated Risk & Resilience

From cyberattacks and regulatory updates to consumer demands, changes in the market, and natural disasters, it can be difficult to imagine being prepared for every possible risk variable. Compounding this are operations that flow well under business-as-usual routines, but tend to break down when there are large events and unprecedented strain. In order to meet the evolving, complicated risks we're seeing post-pandemic, there is a need to move quickly with systemic processes for uncertainty, while also leaving room for improvisation and quick decision making.

To help meet these needs, businesses need to start developing practices to support organizational resilience, holistic management of practices, and processes to tackle risks on the horizon in a way that takes into account uncertainty. According to Gartner[i], building resilience is a journey (see Figure 1). In our opinion, each of these elements needs to work in unison in order to become truly resilient.

Managing this path to resilience not only includes business continuity and crisis response, but also includes resilience plan testing, simulation of disruptive events and how they would affect an organization, education and training, and continuous improvement. And at the heart of this are flexible business models that allow for quick, adaptive decision-making.

It's not just about surviving a crisis. Implementing organizational resilience will set you above competitors and give you critical advantages. "Firms with more mature resilience capabilities grew at a rate of 2.4 times their industry average," says Forrester's Q3 2020 North American Future Fit Technology Survey[ii].

The Backbone of Organizational Resilience

A cornerstone of resilience is how organizations effectively anticipate and respond to a diverse and changing range of risks. These risks can be operational, cyber, compliance, reputational, or financial in nature and extend beyond the four walls of the enterprise into its entire business ecosystem, including its third parties and supply chain. With this level of complexity, organizations need to be agile in their approach to managing risk.

There are several practices and schools of thought that help organizations navigate how to approach these risks and other potential future threats. The Harvard Business Review has defined three components at the core of organizational resilience including:

- **Organizational routines:** These are reliable routines and practices that have been stress tested, allowing for a systemic knowledge about how things relate, and who does what. These routines require constant examination and adjustments to allow for better ways of doing things.

- **Simple rules:** These rules help organizations prioritize decisions and resources when a disruption occurs. For example: what is the top priority when a data breach occurs?

- **Improvisation:** These are more spontaneous, situation-driven decisions that companies, teams, or individuals will need to make if a disruptive event were to happen. While it is impossible to predict the exact disruption that could occur, training can be done to help companies become more comfortable in making strategic, improvised decisions without sacrificing simple rules and organizational routines already set.

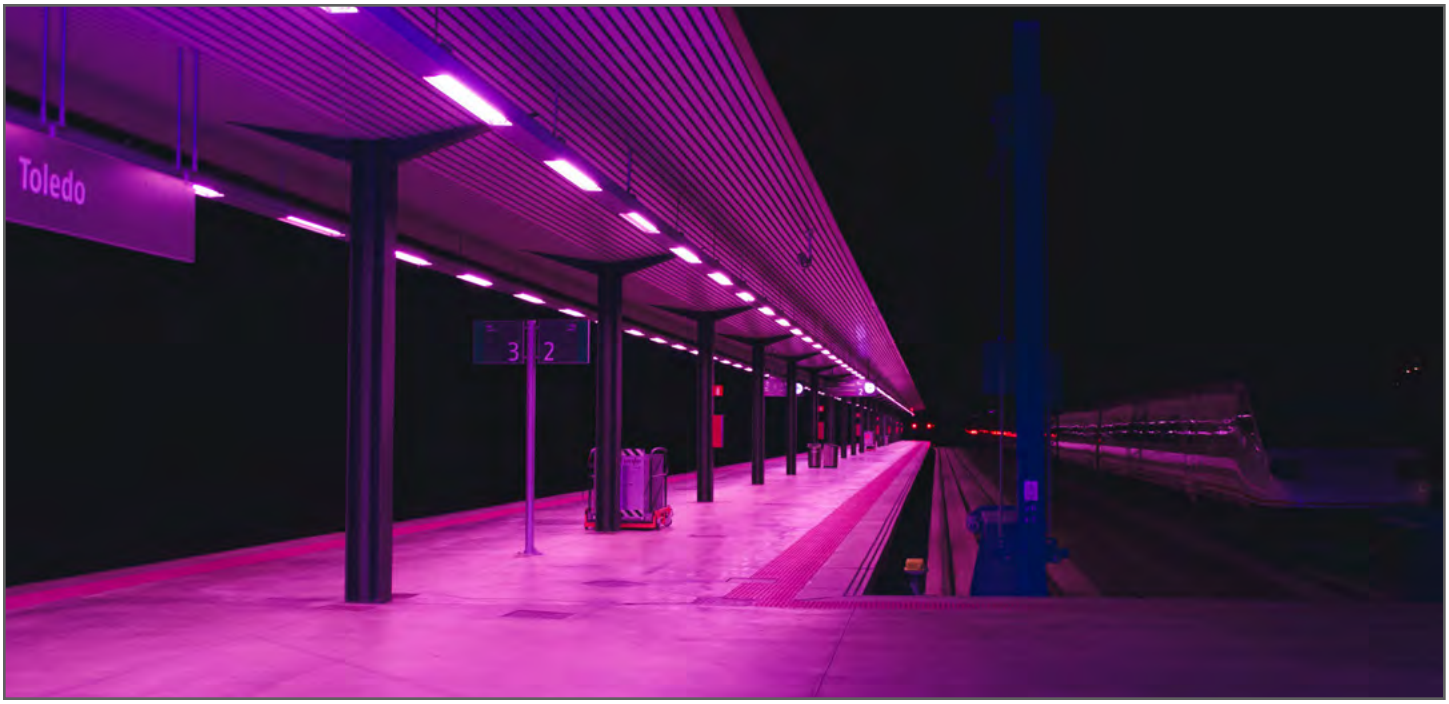
These three practices should be used together as a toolkit to create awareness around organizational resilience, run simulations for potential future threats, build new processes, analyze the effectiveness of current or potential tools, and gauge overall effectiveness. In addition, each of these practices should not be used in a vacuum; they are interdependent. Rules, for example, might prompt improvisations under certain situations. Running simulations and crisis response training helps map out how these relationships work and what variables contribute to certain decisions and actions.

Considering these three components, many organizations are going to have to reconsider the technology they have in place to manage risk and resilience programs. Domain expertise and best practice ways of automating organizational routines and embedding simple rules are important, but the ability to adapt and improvise according to context is becoming even more critical.

Shake Things Up and Question the Status Quo

According to Gartner's *How to Build a Resilient and Responsive Organization*, 52% of CHROs surveyed are planning to "shift from designing organization for efficiency to designing for flexibility."[iii] It's not rocket science that routines are comforting, as well as useful in setting benchmarks. However, when routines become over-utilized, not customizable, or outdated, gaps in protection can begin to appear and grow. Organizational resilience calls for constant questioning of the status quo: what's working, what should be changed, what are we missing, etc.

To help pave your path to resilience, sit down with your risk and resilience stakeholders and spend time analyzing current tools, their effectiveness, what they do, what they could do better, and if you need to swap tools out and invest in new tools.



A key element of this process is to question assumptions behind routines; are you doing things because it's right or because it's how things have always been done? Questions to ask include:

- What processes or decisions have traditionally needed to be made, or signed-off on by executives or higher management? How has this worked in times of crisis/how does this change?
- How often do you update these processes to optimize? Do you assume you're doing enough? How has this historically worked under pressure?
- Where in workflow processes have issues historically arisen? Are there areas that need more resources to help mitigate these problems? How do these processes break down if you need to work quickly under pressure?
- Do resources have the budget allocation that is needed to work effectively? If so, does this budget still work in times of crisis?
- Are there assumptions being made regarding workflows that need to be further scrutinized/questioned? Have these assumptions been tested under pressure, or only during business-as-usual operation?
- Have you overcomplicated processes, or created too much information or process silos?
- How simple is it to adapt these processes in supporting technology?

Preparing for Uncertainty

So, if you find resilience gaps in your processes, how do you begin to test them under pressure, and find out what works? The answer lies in simulations and training. With the complex risk landscape we live in there will be unexpected events that happen down the road that you'll need to mitigate quickly to avoid disruption. But how do you prepare for these events if you don't know what they will be? It can seem like a catch 22.

Even though specific situations that arise may be unfamiliar, you can train yourself and your workforce to be prepared for uncertain situations and you can be trained to react confidently. According to the Harvard Business Review, this type of training and shift in mindset produces positive results:

"By actively training the organization to alter the combination of routines, heuristics, and improvisation on the fly to match the changing requirements of different possible scenarios, leaders can build resilience throughout their organizations. Organizations that regularly deal with fast-evolving situations—think SWAT teams and military commandos—know that it pays to practice and prepare for the unexpected while you have the luxury of time and resources, instead of trying to learn how to adapt in the middle of a storm."

Incident Response Training, Business Resilience Training, and Business Continuity Training are all exercises that help companies prepare for and respond to a crisis. This could include training for physical threats such as natural disasters and active shooters but also preparing for threats like cyber breaches and supply chain disruptions. These types of training routines help companies identify risks, identify priorities, create incident response plans, determine chains of command, and what steps are prioritized over others.

"It's not just about surviving a crisis. Implementing organizational resilience will set you above competitors and give you critical advantages."

In addition to ensuring familiarity with chains of command, it is also important to practice more with having less. Run simulations in which one key supplier is eliminated from your value chain, or communications are down with one of your facilities; what happens to operations, and what types of contingency plans need to be developed to move forward? In addition, know your priorities for certain situations; what can be sacrificed in order to best mitigate an issue?

While an actual disruptive event or crisis may not occur in the exact way a simulation is run, performing these exercises (much like performing fire drills) will help develop muscle memory if and when an actual incident was to occur. But keep in mind that one-off simulations are not effective; make sure these are tested frequently and updated as new information, personnel, and processes are introduced.

It's not about having all the answers. Rather, it is important to have the tools and be familiar with them in order to use them if an unknown situation arises in the future.

Best Practices for Organizational Resilience You Can Start Implementing Today

Organizational resilience does not happen overnight. Rather, it can be a massive shift in company culture and risk management strategies, and frankly, it can be uncomfortable. Everyone wants to assume that they are contributing to mitigating risks within their organization. Unfortunately, as the risk landscape evolves, so too does managing these risks. And while these practices take time, some items can be implemented at the outset to help increase efficiency and productivity.

Commit to a culture of learning: As mentioned, becoming organizationally resilient means embracing a certain level of uncertainty. Committing to training to act quickly and with thoughtful intentions during unknown situations can help ensure continued operations during and after an event. Providing training and resources on current trends and relevant events, continued crisis response training, and encouraging employees to challenge preconceived notions is critical to building resilience.

> **"In order to meet the evolving, complicated risks we're seeing post-pandemic, there is a need to move quickly with systemic processes for uncertainty, while also leaving room for improvisation and quick decision making."**

Triage emergency and crisis response plans: A large part of this type of training involves executing simulations based on possible future events such as cyber breaches, supply chain disruptions, physical security events, natural disasters, and even audit and compliance investigations. Make sure that workforces are familiar with what needs to be done during an event and what the incident command structure looks like.

Embrace flexibility and breaking down silos: While employees need to understand their roles in case of a crisis, also embrace the idea that roles can be fluid and should not be overly pigeonholed into what they traditionally were. Avoid silos and encourage flexibility so people are not too entrenched in their own job responsibilities and can act in any situation. Digital processes help this as they eliminate silos and increase communication.

Have cross-divisional teams: Ensure everyone is aware of larger business strategies and how they fit into them. Traditionally, many risk-related functions were siloed from other areas of the business, such as compliance, procurement, legal, etc. With enhanced risks on the horizon, continuing to isolate functions, processes, and technology leaves you vulnerable to supply chain and other risks. By integrating or centralizing formerly siloed processes such as third-party risk, supply chain risk, business continuity, and IT resilience, professionals can gain greater security and resilience for their organization.

Know what makes your business run: Understand what your critical products and services are and, in turn, what is critical to your organization being able to continue to deliver them. This will include your internal operations and systems, but also third parties, suppliers, and your supply chains.

Understand how your third-party ecosystem works: Using your TPRM tools, closely evaluate each of your suppliers and their resilience against supply chain disruption. This may involve examining their own inventories, if they operate in a concentrated region, their business continuity plans, and other risk data. In addition to the suppliers that you have direct contracts with, it is also important to know your fourth parties and nth parties- i.e., your third parties' subcontractors and potential risks they can bring.

Ensure compliance across suppliers: Likewise, understand how your business depends on its IT, and its third parties. Manage cyber supply chain risks by ensuring that suppliers follow cyber security standards, conduct continuous monitoring, and have contingency plans in place.

Avoid concentration risks: Concentration risk is direct or indirect exposure, or group of exposures, that has the potential to lead to large losses that can threaten an organization's ability to perform its core business. This type of risk can be the result of dependence on a geographic area, single vendors, or fourth parties. Make sure your suppliers are balanced across a variety of regions so that if a disruption were to occur, you have other channels to pursue. In addition, invest in a variety of vendors and contingency plans so that if a single vendor's operations are disrupted you have other options.

Take an integrated approach to risk and resilience: Collectively all of the above add up to the need for a new way of managing risk and resilience programs across the extended enterprise. These programs need to be unified. People, processes, and technology must all come together to make this work.

There will always be new threats, players, and shocks on the horizon that could disrupt business as usual. It will be the resilient organization that prospers through these.

---

i Gartner, Outlook for Organization Resilience, 2021, Roberta Witty, David Gregory, Jan. 12, 2022

ii Forrester Research, Q3 2020 North American Future Fit Technology Survey, April 2021

iii Gartner, How to Build a Resilient and Responsive Organization, 2020

Technology's Role in Strengthening Business Continuity

A Conversation on Security Ratings with:

Stephen Boyer
Co-Founder and CTO
of BitSight

Victor Gamra
Chief Executive Officer
at FortifyData

Mike Wilkes
Chief Information Security
Officer at Security Scorecard

Have you seen market impacts of the pandemic for cybersecurity and third-party risk management? How has this shifted over time?

Victor Gamra (VG): The pandemic has definitely played a significant role in cybersecurity, particularly in remote workforce management. As the shift to working from home became the new normal, it brought along a list of challenges for managing risks associated with remote access and networks. However, I believe this is an important evolution in the cybersecurity market. Now, more than ever, companies are becoming more aware of how easy it is for hackers to compromise networks through employee accounts and devices, or third-party vendor solutions. These risks are very real, but they create opportunities to develop and implement new solutions that address these emerging threats.

Mike Wilkes (MW): Most definitely. When folks were sent home and asked to work remotely a lot of companies were unprepared from a security controls and tools standpoint. Even having enough laptops for everyone was a problem, so a very significant percentage of those companies had to allow the use of personal computers which, in most cases, were un-protected by anti-virus or other security policies and settings. So, your own company became much more vulnerable to ransomware and malware… One of the lesser discussed aspects, however, was printers. Some finance and HR staff needed printers at home to do their jobs. This created an "information-rich" garbage risk. In the office, there are document shredders and bins for secure document disposal. Bad actors have taken advantage of this and have undoubtedly found sensitive data in the garbage.

Stephen Boyer (SB): The pandemic has certainly accelerated the digital transformation which is happening for organizations across the globe. With this, we're seeing attack vectors that hit organizations at the heart of their digital supply chains. Solarwinds, Kaseya, and ransomware attacks continue to make headline news. This means that cybersecurity and third-party cyber risk management are becoming must-have business requirements.

Are there overlooked indicators that people should be paying attention to in terms of the cybersecurity vulnerabilities of their third-party vendors?

VG: Often, third-party risk managers rely on outdated reports or vulnerability assessments while performing due diligence on vendors. These assessments provide little to no value if they aren't using a risk-based approach. This means additional indicators are necessary to inform the criticality of the issue based on

"The pandemic has certainly accelerated the digital transformation which is happening for organizations across the globe. With this, we're seeing attack vectors that hit organizations at the heart of their digital supply chains."

– Stephen Boyer

the importance of assets, the impact on the business, and the likelihood of compromise. Vulnerability assessments are a good starting point but do not paint the entire picture of risk without the additional data.

SB: There are many signals and indicators in the data and it's really about being able to find that information and validate the correlation.

MW: One of the overlooked indicators that is worth mentioning here is concentration risk. Recent disruptions such as the 2020 Amazon outage caused many companies to realize that lack of fault tolerance and high availability designs by their third parties could result in impacts on their own platform availability. So, it's important to have a view into the concentration risk of your third parties and select vendors with good security ratings, but also vendors with good security architecture, design, and multi-region digital footprints.

How does continuous monitoring play a part in business continuity management?

SB: Continuous monitoring is vital in understanding the state of your third-party risk at any moment, and responding to changes in risk when they happen. Having programs and workflows in place to help proactively monitor your third-party environment is crucial when maintaining your business continuity. While it certainly can be a challenge to monitor and reassess your vendors with a regular cadence, cyber risk is dynamic and fluid which makes it so vital to firm up your continuous monitoring program.

MW: There is a saying that if you have one of something, you have none of that thing because it is a SPoF (Single Point of Failure). Business continuity planning involves looking for and mitigating the risk of SPoFs. A company with no continuous monitoring of their service endpoints will suffer more frequent and longer-lasting disruptions. And this monitoring is not just a simple ping check or network connection test. The monitoring needs to become more sophisticated and evolve into what is being called "continuous verification" or "continuous validation" which is verification of business logic, security compliance, configuration drift, and fault tolerance. This requires an approach to engineering systems monitoring that understands how failures occur and how to ensure business remains operational despite extreme conditions.

VG: Continuous monitoring enables the enterprise to stay vigilant and aware of the ever-changing threat landscape. This should be a critical aspect in every cybersecurity program, as it allows businesses to become more resilient to various types of attacks, and even in some cases, zero-days. There is a saying that, "it's not if you're going to be breached, but when." Enterprises need to have effective business continuity procedures that have accounted for various risk scenarios informed by new threats through continuous monitoring capabilities.

What are steps organizations can take today to build resilience and strengthen business continuity management?

MW: Look into the emerging practice of "security chaos engineering" and find DevOps talent that can move beyond the fear of failure. Security chaos engineering is the thoughtful experimentation with infrastructure and services to identify how

"Enterprises need to have effective business continuity procedures that have accounted for various risk scenarios informed by new threats through continuous monitoring capabilities."

– Victor Gamra

to make our complex web of dependencies and infrastructure more resilient... To this end, tabletop exercises are inexpensive ways to surface gaps in documentation. Just like an unused muscle will atrophy over time, strengthening business resilience comes with practice and exercise.

SB: Some of the steps that organizations can take today include building out cyber risk governance across your organization where you set a standard for cyber security programs across your organization to drive accountability and to measure performance over time... Another key element is validating your vendors quickly and confidently to ensure new vendors are within your organization's risk tolerance.

VG: A really key step is leadership buy-in to implement effective policies and procedures. Without clear visibility into what risks impact business resiliency, it may be difficult for leadership to understand the criticality of the issues. With effective risk management that can be communicated effectively. However, the next step should be implementing policies and procedures to support the initiatives that drive business resiliency.

"We need to achieve widespread change as current practices are inadequate to meet modern threat actors. This comes down to working on the 'three A's' of change: awareness, acceptance and action. If we don't reach the third stage of change then we have failed."

- Mike Wilkes

What can security ratings tell us about the cybersecurity of our third parties?

SB: Security ratings empower you to easily compare the level of inherent risk to prioritize assessments and mitigation efforts of your third parties. Through security ratings you are able to set a risk threshold for each vendor tier, allowing you to right-size your due diligence process based on where there are gaps.

VG: They're traditionally used to quickly determine security issues from an external perspective. Although many cybersecurity ratings providers may lack the comprehensiveness of data to define a truthful score, I believe newer technologies could fill in those gaps and give a better understanding of risks linked to any third-party entity. The combination of an effective security rating and questionnaires for assessing third parties will provide any organization with more risk intelligence that drives business decisions.

MW: A key point to also think about is that security ratings have only to prove correlation, not causation. Many CISOs confuse the two. Yes, the investor relations website has no critical or sensitive data, and having vulnerabilities on that website does not usually turn out to be the root cause of an attack being successful... But with a sufficient number of observations, with the application of objective scoring, and weighting of the risk indicators, the correlation between security breaches and risk indicators is mathematically demonstrable and unassailable.

How do you think security ratings will evolve and what priorities do you see arising?

MW: Complex systems behave in unexpected ways and exhibit what is called systemic risk, an emergent property of modern digital economies… We need to achieve widespread change as current practices are inadequate to meet modern threat actors. This comes down to working on the "three A's" of change: awareness, acceptance and action. If we don't reach the third stage of change then we have failed. If we cannot get companies to be aware of their third-party or supply chain risk and gain the resources needed to address them, we do not win. It is only when we have awareness and acceptance that we are capable of action.

SB: We see that boards, investors, insurers, and regulators are increasingly accounting for cyber risk in their investing, underwriting, and oversight activities. Cyber risk has historically been opaque for them and they are now demanding more transparency and quantification of the risks. Security ratings combined with Cyber Risk Quantification (CRQ), which translates performance into potential financial loss scenarios, will help these groups more efficiently and effectively measure and quantify organizational cyber-performance and the consequential financial impact of that performance.

VG: The perception of security ratings not being an indication of risk is starting to change with next-generation ratings solutions. When you get a risk rating from a trusted provider, the score should accurately represent your susceptibility to a data breach. This is part of risk management – the ability to inform your risk profile with other factors via integrations with other sources is key to defining the most accurate representation of risk. I believe next-generation ratings solutions provide these capabilities and are the future.

This interview has been edited for length and clarity.

About the Contributors:

Stephen Boyer:

Stephen co-founded BitSight in 2011 and serves as the Chief Technology Officer. BitSight is a cybersecurity ratings company that analyzes companies, government agencies, and educational institutions. Prior to founding BitSight, Stephen was President and Co-Founder of Saperix, a company that was acquired by FireMon in 2011.

While at the MIT Lincoln Laboratory, Stephen was a member of the Cyber Systems and Technology Group where he led R&D programs solving large-scale national cybersecurity problems. Before MIT, he worked at Caldera Systems, an early Linux startup.

Stephen holds a Bachelor's degree in Computer Science from Brigham Young University and a Master of Science in Engineering and Management from the Massachusetts Institute of Technology.

Connect with Stephen Boyer
Learn more about BitSight

Victor Gamra:

FortifyData is a cybersecurity ratings and risk management platform provider that helps enterprises assess, identify and manage their cybersecurity posture. Before launching FortifyData, a cyber risk management solution, Victor Gamra was the Head of Information Security for a credit reporting agency in Atlanta. It was during this time that Victor was confronted with a problem. He was unable to effectively quantify the complete cyber risk exposure of his own company, let alone those of his third-party vendors. Existing GRC and security rating products were insufficient and inaccurate due to misattributions and a plethora of false positives.

Today, in his role as the CEO, Victor continues to focus on building the company. The vision is to help companies of all sizes effectively assess cybersecurity risks and guide business leaders to make better-informed decisions to protect their resources from cyberattacks.

Connect with Victor Gamra
Learn more about FortifyData

Mike Wilkes:

Mike Wilkes is the Chief Information Security Officer (CISO) at SecurityScorecard, an information security company that rates cybersecurity postures of corporate entities through completing scored analysis of cyber threat intelligence signals for the purposes of third-party management and IT risk management. Wilkes is responsible for developing enterprise-wide security programs to protect corporate systems as well as growing and extending the SecurityScorecard platform to customers, executives, and boards of directors.

Wilkes is a technology evangelist with experience reaching back to the earliest days of the internet and the birth of e-commerce (he and his team built, launched, and supported starbucks.com in 1998), Mike has been leading the digital transformation of globally renowned brands such as Sony Playstation, Macy's, Nvidia, KLM, and many others. Before joining SecurityScorecard, he was the VP, Information Security at ASCAP and the Director of Information Security, Enterprise Architecture, and DevOps teams for Marvel Entertainment.

Connect with Mike Wilkes
Learn more about SecurityScorecard

SPOTLIGHT

The Importance of Revisiting Business Continuity Plans

Maureen Kiefer-Goldenberg
Chief Compliance Officer at The Mather Group, LLC

Maureen Kiefer-Goldenberg is the Chief Compliance Officer at The Mather Group, LLC, an investment advisory firm in Chicago that is regulated by the Securities and Exchange Commission (SEC).

What are the top priorities for improving Business Continuity that organizations should be considering in 2022?

Because of the pandemic, everyone, across all industries is revisiting their plans and making adjustments. Having a BCP is a best practice and you do not want to be the firm that doesn't have one. Besides that, it is just good business. For 2022 and beyond, I believe the focus will be on the following:

- Considering effective practices to help improve preparedness for large--scale climate events.
- Safeguarding client accounts and the ability to service them should an event occur.
- Ensuring you have the right resources in place to handle large scale events.
- Insurance considerations.
- Enhancing support for remote personnel.
- Evaluating operational risks for remote associates.
- Evaluating succession plans/key persons.
- Conducting ongoing assessment of vulnerabilities.
- Documentation of data breaches and keeping incident response logs.
- Conducting training for staff.
- Testing, testing and more testing.

Of course, this list could go on and on, especially as we have some seen some events happen firsthand. For us, we had the ice storms in Texas last year. This was definitely new ground for firms headquartered in Texas or with any type of presence there. We had to quickly pivot in our BCP mode and make sure that our associates and clients were taken care of. The point here is do not think it can't happen to you. Of course, you cannot prepare for every situation, but you can learn from the ones that do happen and make your plan even stronger.

How should business continuity plans evolve?

This is about constantly revisiting your BCP plan. It should not be a document that sits on the shelf, and you dust it off every once in a while. It is a living, breathing document, and every time a business decision is made, you should have your BCP in mind. It doesn't matter what the change is in your organization. It should always be a question of "Does this affect my BCP, and do we need updates?" Many times, the answer to this question is "Yes."

How important is visibility and eliminating silos when it comes to BCPs within the organization?

This is the key to a successful plan. In my organization, compliance and operations work hand in hand to ensure the appropriate changes are being made and communicated to the rest of the firm. When we onboard a new associate, we tell them to read the plan and review where it is. We also make sure that our plan has key contacts listed so an associate always knows who to call if something happens.

We have found that even if the elements of the plan do not affect someone today, there is a pretty good chance at some point they will… But also, BCP isn't just about the technical aspect. Backups are very important, but communication is equally so. Always be sure to address this in your plans. Use your website to communicate with clients in the event of a disaster as well. That should be the first place you add a message so your clients are not left wondering.

If you work in an organization with cross-functional teams, you can use this to your advantage. Something that affects or has affected one group may be of benefit to another, so collaboration is key.

The Mather Group, LLC (TMG) is registered under the Investment Advisers Act of 1940 as a Registered Investment Adviser with the Securities and Exchange Commission (SEC). Registration as an investment adviser does not imply a certain level of skill or training. For a detailed discussion of TMG and its investment advisory services and fees, see the firm's Form ADV on file with the SEC at www.adviserinfo.sec.gov. The opinions expressed, and material provided are for general information and should not be considered a solicitation for the purchase or sale of any security.

FEATURE

Integrated Risk & Resilience

Why Butterflies, Swans, and the Pace of Change Demand a New Approach to Managing Risk Across the Extended Enterprise

Kimberley Allen
Chief Marketing Officer
at Aravo

Today organizations operate in a hyper-connected, interdependent business ecosystem. A large part of business strategy depends on the reliance on external third parties (and associated physical and cyber supply chains) for the provision of key infrastructure, services, support for critical processes, and products.

Businesses also operate in a shifting risk landscape. Risks too are interconnected and emerge from diverse areas (e.g., cyber, geopolitical, extreme weather, regulatory, health, climate, financial). They can be location dependent, but they can also defy any geographical or cyber borders. One ostensibly small hazard can ripple into catastrophic outcomes.

A butterfly flaps its wings

A butterfly flaps its wings…could the miniscule flutter of a butterfly wing in the forests of Brazil set off a tornado in Texas?

The "butterfly effect" is a term that chaos scientists have used to describe various related phenomena, but essentially is the concept that one small occurrence can influence a much larger, complex system.

The term "butterfly effect" was coined by meteorologist Edward Lorenz in the 1960's, when he discovered that tiny, rounding error scale changes to the starting point of his computer weather models (synonymous to the flap of a butterfly's wings) resulted in vastly different outcomes. This led to the title of his paper, "Predictability: Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?" The flapping wing doesn't itself cause the tornado, but represents a small change in the initial condition of the system, which cascades to large-scale alterations of events.

While we'll never know with certainty if it was a butterfly's wing that set off the strong winds experienced around Suez on 23 March 2021, we do know it was the force of those winds that buffeted the Ever Given, a 400-metre-long container ship, leading it to become wedged across the Suez Canal. This resulted in it blocking all traffic for six days until it could be freed. And this one condition, in some ways, set off its own 'butterfly effect' – massive global supply chain disruption. The Suez Canal blockage cost roughly 12 per cent of global trade and was holding up trade valued at over $9 billion per

day, according to data from Lloyd's list. This is equivalent to $400 million worth of trade per hour or $6.7 million per minute. Countless retailers around the world — both offline and online — suffered losses due to the blockage as key shipments were delayed.

This example underscores a couple of truths:

The first is that enterprises today are part of highly complex business ecosystems. In order to be successful, they are highly reliant on interdependencies between their internal operations, technology infrastructure, third parties and supply chains. Businesses in all parts of the world were interrupted in this case because key products or product components were delayed.

The second is that these complex enterprises are operating in a dynamic landscape of interconnected risks. Risks that continue to grow in variety, impact, and velocity. In this case a weather hazard triggered heighted operational and business continuity risks amid a risk terrain already heightened by the global pandemic.

Grey swans are coming home to roost

Somewhat ironically, we hear the term "black swan" being bandied about relatively frequently. "Black swan" is a term popularized by author and former Wall Street trader Nassim Nicholas Taleb. Taleb has described a black swan as an entirely unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences.

What's more predictable is the grey swan – events with severe and devastating consequences, that are easier to see coming, but nevertheless often not taken seriously enough in advance.

The last two years illustrates the impact of multiple grey swan-type events occurring in close proximity: a global pandemic, a series of hundred-year weather events, social disruption, and war.

According to analysis by insurance firm WTW:

"While the frequency and concurrence of these events may appear unlikely on the surface, predictive analysis across 10 risk categories calculates a 63% probability of one or more hundred-year events in any given decade, and a 26% chance that multiple such events will occur in the same decade. The likelihood is even higher when events are interdependent."

Ultimately, business interdependencies and the interconnectedness of risk, and the fact that catastrophic events can be more likely than we may think, call for a much more integrated approach to managing risk and resilience across an enterprise.

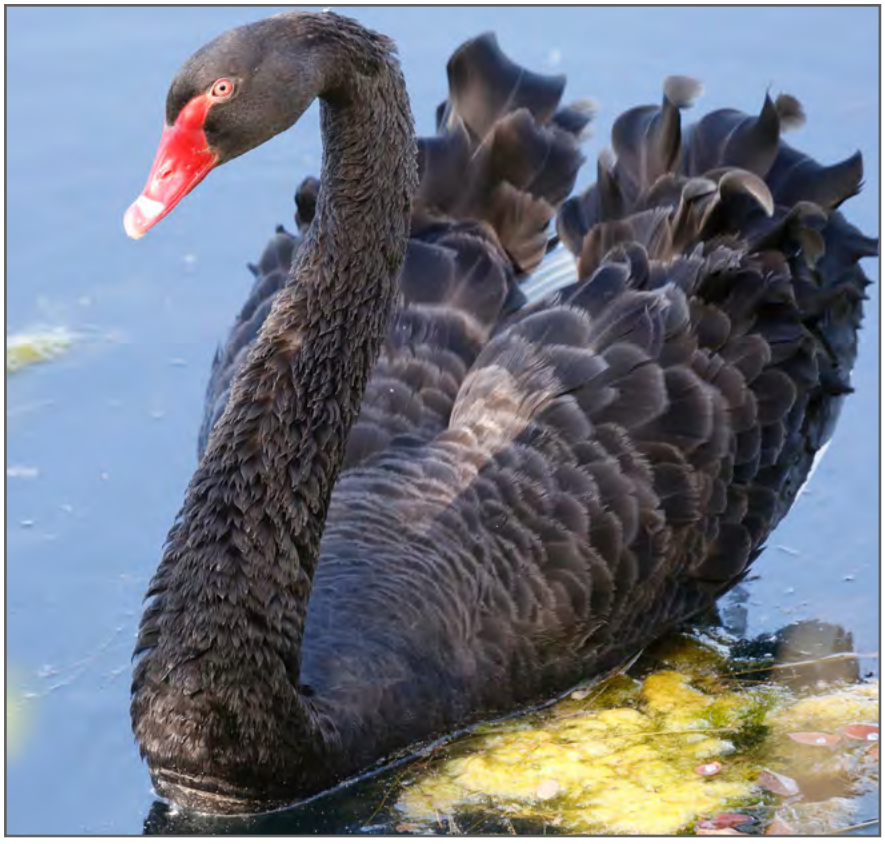
For example, companies often manage different risk types and different program types in silos, rather than taking an integrated view of risks. They also focus attention on managing the types of risks that they encounter most often. But they fail to factor in less frequent shocks that have the potential to inflict much bigger losses and disruption. Like global pandemics. Or large-scale war and sanctions.

Organizations need to have a comprehensive view of risks that could impact their ability to meet their business objectives at the enterprise level. Furthermore, understanding the business impacts of these types of events occurring allows organizations to build in resilience – these might include measures such as building in financial buffers, moving from just-in-time to just-in-case sourcing strategies, diversifying suppliers across different geographical locations, supporting hybrid working models, and so on.

The pace of change

Further complicating risk and resilience management is the pace of change. Globalization, technology, markets, and the ways we work are rapidly shifting. We saw the pandemic throw more fuel on the fire of change, catalyzing even faster changes in the way companies in all sectors and regions do business. According to a survey of executives by leading consultancy firm McKinsey their companies have accelerated the digitization of their customer and supply-chain interactions and of their internal operations by three to four years.

This brings to the foreground the other risk management imperative for businesses – agility. The ability to move effectively at the pace of change.



Disconnect in this environment of interconnectedness

It's clear that organizations need a more unified, fluid, and agile approach to risk and resilience for the extended enterprise.

However, a significant challenge for boards seeking to improve their organization's ability to manage risks and enhance resilience is the current level of disconnect across the enterprise. This disconnect manifests itself in several ways.

- **Disconnect from strategy and objectives:** In many organizations, risk management is not fully integrated with the organization's operations and strategy. Organizations limit their ability to develop effective responses (and build their resilience) when they are unable to anticipate risks or align them with strategies. Connecting risks to long-term strategy helps organizations move from risk to readiness, and mitigate business interruption, reputational damage, financial exposure, and other losses.

- **Disconnected risk and resilience programs:** These are managed in silos across an enterprise, with a lack of connected context, processes, and data. Organizations have often managed operational risk, third party risk, supply chain risk, and business continuity/disaster recovery programs in a highly siloed fashion despite their many intersections and interdependencies.

- **Disconnected data:** Enterprises are managing vast amounts of structured and unstructured data from different systems, processes, and programs in their efforts to manage risk and resilience. Different data models and taxonomies and varying quality of data can create silos and noise, rather than delivering actionable insights for the organization to respond to in a proactive and agile fashion.

- **Disconnected tools:** Many organizations lack a common risk and resilience information and technology architecture across the enterprise. They are relying on a patchwork of technology systems that are often difficult to integrate and built on custom code, making them slow (and expensive) to adapt to the dynamic risk and operating environment. They lack a common connective tissue that connects processes and data in an intelligent and efficient way.

In order to survive and thrive in an interdependent and dynamic environment – enterprises must take a more connected approach to risk and resilience. Strategy, people, programs, processes, and technology must all come together to make this work. The time for integrated risk and resilience is now.

Taking Action: Integrated Risk & Resilience (IRR)

Moving towards an integrated approach to risk and resilience is a journey that involves breaking down many existing silos and supporting better connectivity across strategy, programs, data, and processes. Some of the steps we explored in our infographic that an enterprise can take to begin this journey include:

Connecting risk and resilience to strategy and objectives. A strategic goal of any resilience program will be the ability to continue to deliver critical services and products through disruptions that could be caused by hazards. This means it is important for an enterprise to understand what their critical products and services are and, in turn, what is critical to the organization being able to continue to deliver them. This will include internal operations, infrastructure, and systems, but also third parties, suppliers, and supply chains.

Connecting risk and resilience programs. There will be multiple risk and resilience programs across an enterprise that need to be considered in the context of a unified program. Better connective processes, shared data, and stakeholder collaboration across these is critical:

- **Business Continuity Management:** Business continuity management involves the advanced planning and preparation of an organization to address organizational risks and ensure the business can maintain normal

operations during disruptive events. It involves identifying potential risks, having plans in place to respond to and recover from any threat, testing those procedures, and periodically reviewing the process to make sure that it is up to date and learning and improvements are captured.

- **Crisis Response and Management:** These are processes an organization has to address a major situation or disruption that has the potential to cause harm to the business, the stakeholders, the public, or other entities.

- **Disaster Recovery:** This is an organization's set of policies, tools, and procedures to enable it to respond to and recover from an event that negatively affects business operations (typically those that impact critical systems and IT infrastructure).

- **Supply Chain Risk Management:** This involves the strategic and operational steps a business takes to identify, address, and mitigate risks within their supply chain.

- **Third-Party Risk Management:** This is the process of managing all the third parties (and their engagements) that the organization works with, with a focus on identifying and mitigating the full range of risks that they could expose the organization to over the lifecycle of the relationship.

- **Cybersecurity:** This includes the processes and tools to protect critical systems and information from digital attacks. Within resilience, this includes cybersecurity of vendors and along the supply chain.

- **IT Resilience:** This involves the IT security of systems and infrastructure that supports operations in order to maintain service levels during disruptions.

- **Operational Resilience:** These initiatives expand on business continuity to examine impact and tolerance levels during disruptions that could affect the organization, customers, and other stakeholders.

- **Training and Development:** Organizational resilience training helps build new routines and improvisation techniques so that employees and leaders are prepared to act confidently and quickly during uncertain situations.

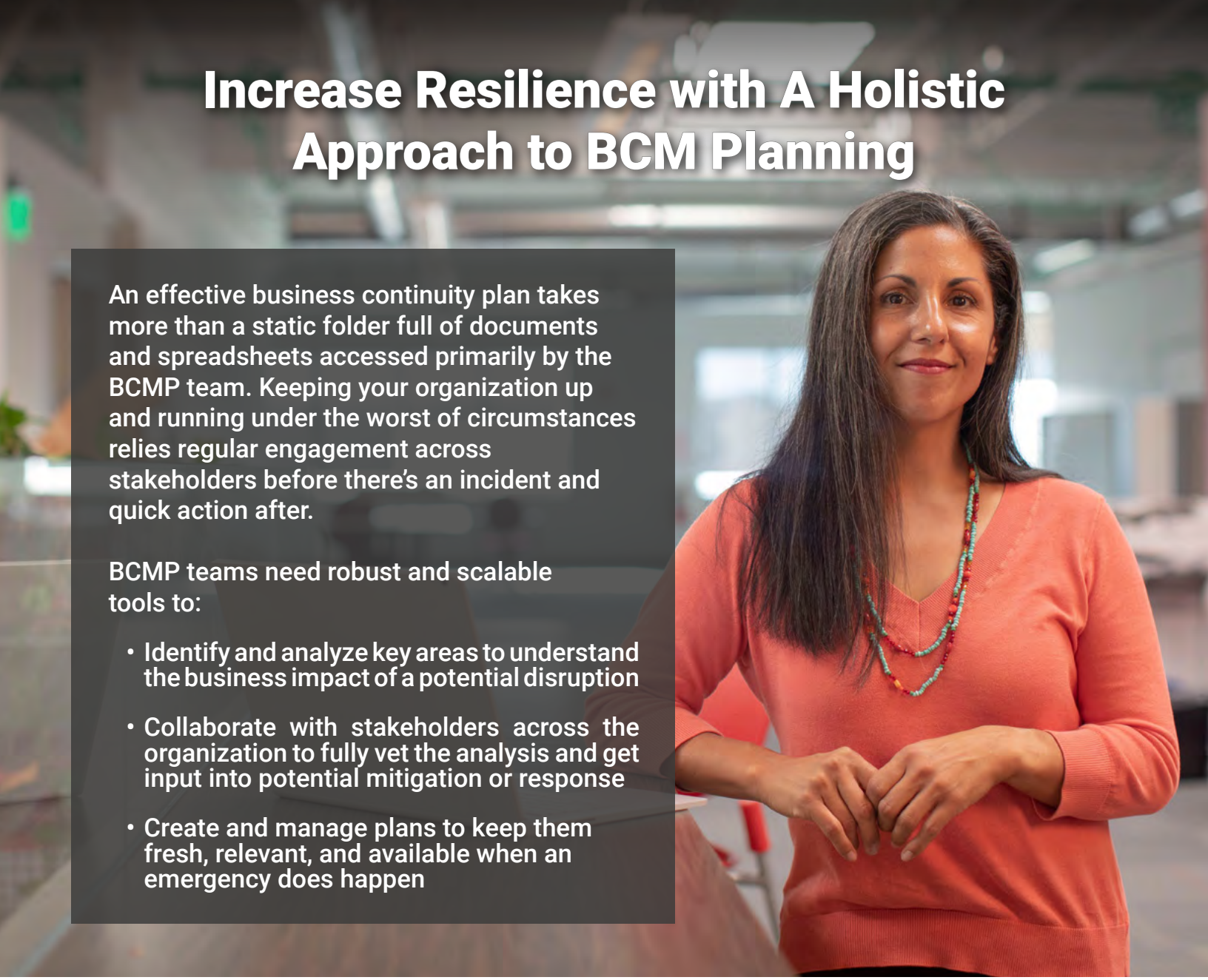
Connecting risk intelligence to action. Organizations need to be able to take real-time hazard monitoring and risk intelligence and be able to overlay this intelligence with their assets across their business ecosystem (which will include their third parties and supply chain). Risk intelligence needs to be broad – covering all types of risks (e.g. cyber, geopolitical, extreme weather, regulatory, health, ESG, financial), and monitoring needs to be ongoing. Comprehensive and actionable real-time intelligence will enable teams to align objectives and approaches across the enterprise, and prioritize and focus mitigation efforts to prevent disruptions, secure supply chains, and achieve better business resilience.

Connective technology. Technologies of the past built on custom code with little interoperability are not going support the agility that the programs of today and tomorrow will require. Platforms will need to be able to pull data from internal systems, enterprise and cloud applications, IT management systems and risk intelligence providers, and trigger the appropriate workflow actions based on that data. Domain expertise and best practice ways of automating organizational routines and embedding simple rules are important, but the ability to adapt and improvise according to context is becoming even more important. Leveraging low-code no-code (LCNC) automation platforms will play an important part in success. Their flexibility will allow organizations to be able to quickly add risk domains to assess and monitor, to quickly add data sources, to quickly add integrations, and to seamlessly build connective processes across their risk and resilience programs.

The final word

As the world reels from seismic changes – including a global pandemic, war, new far-reaching trade sanctions, civil upheaval, and significant new supply chain disruptions – it's not too far into the past we have to reach to understand that shocks such as these are more frequent than we care to imagine. Whether or not it was the flutter of a butterfly's wing that set the 2020's on this path of upheaval, it is clear that enterprises are going to have to become much more resilient in order to weather the storms of change. Integrated risk and resilience is one of the levers that enterprises will need to adopt in order to succeed.

Increase Resilience with A Holistic Approach to BCM Planning



An effective business continuity plan takes more than a static folder full of documents and spreadsheets accessed primarily by the BCMP team. Keeping your organization up and running under the worst of circumstances relies regular engagement across stakeholders before there's an incident and quick action after.

BCMP teams need robust and scalable tools to:

- Identify and analyze key areas to understand the business impact of a potential disruption
- Collaborate with stakeholders across the organization to fully vet the analysis and get input into potential mitigation or response
- Create and manage plans to keep them fresh, relevant, and available when an emergency does happen

Integrated Risk & Resilience

Aravo for Enterprise BCM combines Aravo's 20+ years of experience and standards such as ISO22301 and BCiGPG, transforming your BCMP program with:

- Increased efficiency and collaboration with work-flow automation
- Holistic views of BCM and its connection to risk management throughout the enterprise
- Peace of mind knowing that BCPs are data-driven, up-to-date, and can be activated quickly

For More Information

Visit us at aravo.com

Email us at info@aravo.com

Call us at:
+1 415-835-7600 [US]
+44 (0) 203-743-3099 [EMEA]