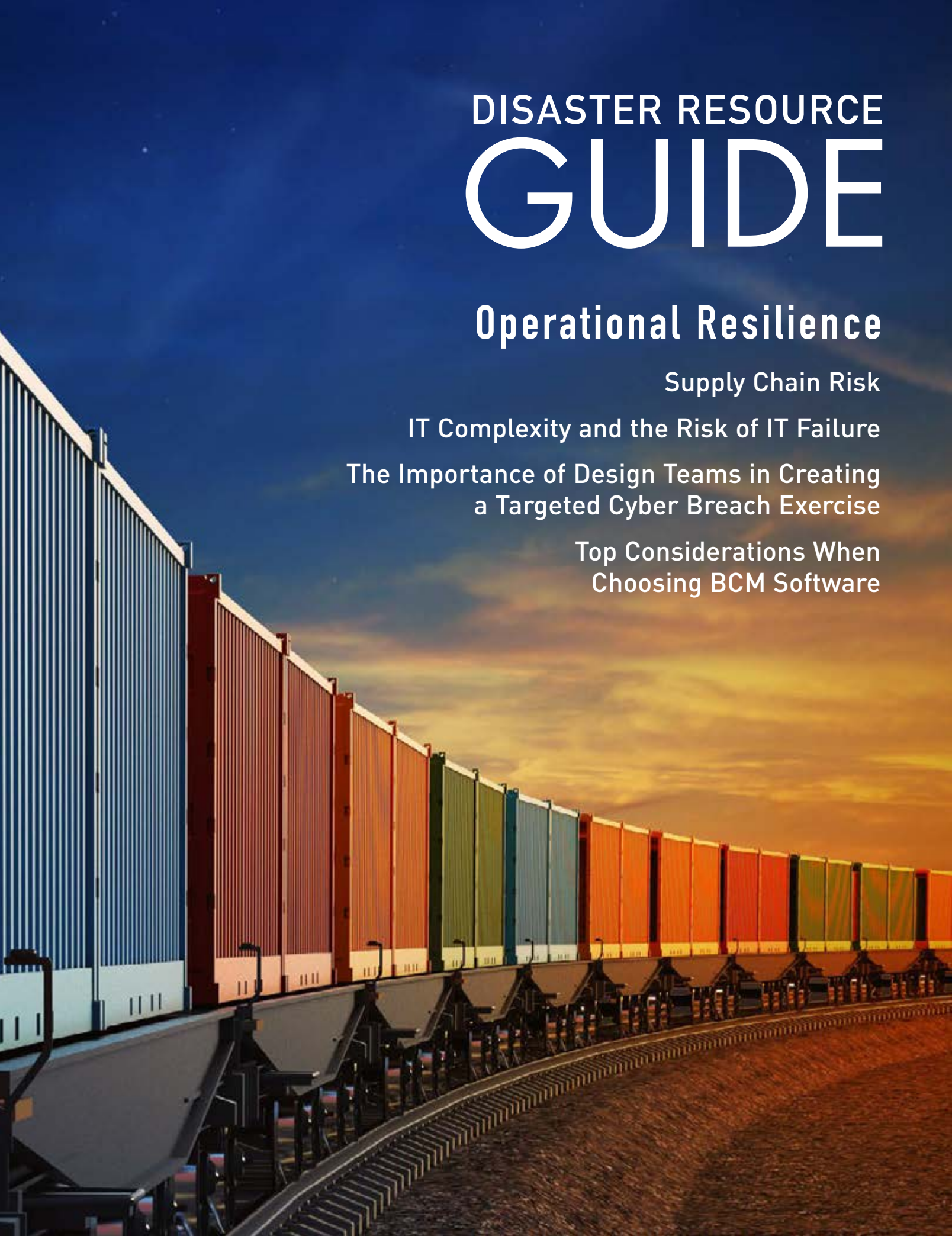


DISASTER RESOURCE GUIDE

Operational Resilience

Supply Chain Risk

IT Complexity and the Risk of IT Failure

The Importance of Design Teams in Creating a Targeted Cyber Breach Exercise

Top Considerations When Choosing BCM Software

A trusted approach to security, risk, and compliance management.

Visit @RSAGRC booth 528
during #gartnersec

RSA

www.rsa.com/grc

Taking Command of Your GRC Journey

THE CRITICALITY OF RISK INTELLIGENCE

The next five years will bring even more pressure and greater shifts in the way governance, risk and compliance (GRC) programs need to operate to succeed. Not only are regulations and risk management needs changing, but the technology used to power businesses is radically shifting. The delineation between digital strategies and business has disappeared, and any differentiation between cyber risk and business risk has vanished. Given that many new business growth strategies rely on technology, organizations must be able to manage cyber risk as part of their risk management strategy. GRC programs must create a unified risk culture and a common language across the enterprise in order to understand risk in the context of the organization's overall objectives. Therefore, effective risk management practices must address cyber risk and business risk in equal measure and provide a consolidated view of risk to executives and practitioners.

Today's business environment is fraught with risk. Technology and eeconomic and market conditions affect organizations on a daily basis. The constantly changing risk landscape is a leading topic in headlines, industry forums, media outlets and Board rooms. We are moving to a world where your risk management approach is not only your defense against known and unknown risks, but a critical component of your competitive advantage.

Rather than avoiding risk, organizations need to effectively position themselves to embrace risk with confidence to successfully seize growth opportunities in the market.Risk management is becoming a core capability that separates the winners from the losers. Organizations that understand and effectively manage risk will prosper, while those that cannot will fail. Success starts with the ability to manage risk in a manner that frees up resources to focus on the company's long term, strategic objectives. Executives need relevant, up-to-date risk information in order to make the right decisions and pursue the right opportunities.

With so much change in the risk landscape, organizations need agile, flexible programs to anticipate and mitigate risk. Without these programs, a wrong decision could be costly to the business and the company's brand reputation. While most organizations have built out risk processes and programs in one section of the company, organization are often left with isolated pockets of risk management, with efforts duplicated or, even worse, skipped entirely, leaving serious gaps. Insight into risk is often incomplete, inaccurate or delayed. These factors make it difficult to ensure accountability and impossible to prioritize where to dedicate resources. Ultimately, the business does not have the risk insights needed to make the right decisions to protect company value and drive growth.

THE ROAD TO MATURITY

No organization can achieve complete visibility into risk. There is no crystal ball that will magically outline opportunity, map risks, and provide a distinct, unobstructed path to success. However, there are specific stages organizations can move through in building Risk Intelligence.

Siloed Stage: Many organizations are stuck in the most elementary risk and compliance approaches that attack individual issues within a stovepipe strategy. This strategy relies on constant fire-fighting mode for the front line and functional employees. Some silos may be mature, but some could be missing or just forming. With the focus typically on compliance and tactical risks, the organization cannot see beyond the immediate issue. Risk managers are hunkered down in the trenches with little movement forward, relying on old fashioned approaches that may get the job done but will never keep pace in today's market.

These organizations need to take this "compliance crush" off the table and start solving regulatory and industry needs in the most efficient and effective manner. This requires automating compliance and building a cohesive strategy to deal with the compliance "table stakes" of doing business. Compliance obligations need to be tackled but with an eye towards the future. Building more silos at this point is futile. Risk and compliance functions need to focus on where data and processes can be leveraged, reused and shared and limitations of niche, operational tools can be overcome. By "Transforming Compliance," companies will pave the way to the next stage in their journey.

Managed Stage: Companies in this stage have solved or are well on their way to solving the compliance conundrum and are poised to harness risk. Transforming Compliance has resulted in common policies, standards and controls, an effective control infrastructure, and efficient methods to measure, monitor and report compliance state.

Companies in this stage need to become aware of the various risks they are juggling and put plans in place to manage these risks within the context of a broader strategy. A key factor in this evolution is addressing both cyber/technical risk and business risk with a combined strategy. The business needs to understand the risks in its technology landscape, and technologists must be active participants in addressing business risk. The risk program should be focused on giving the business the insight to navigate major issues. This progress is being fueled more and more by metrics and analytical capabilities that provide visibility into risk.

Companies in the Managed stage begin building the bigger picture, shoring up strong competencies, and bringing weaker elements up to a stable state. As the GRC program matures, effort begins shifting from compliance as the key driver to more focus on risk. The organization eventually reaches a point where the Opportunity Landscape starts taking shape and the company is then poised to move to the next stage – Advantaged.

Advantaged Stage: When the organization has mapped out and conquered the Risk Landscape, they can begin exploring the "Opportunity Landscape" The organization is now ready to realize the competitive advantages of harnessing risk – beating competitors to market, launching new products and services with calculated efficiencies, and avoiding major issues that affect reputation and the bottom line. They have turned the corner from managing "Unrewarded Risk" to benefitting from "Rewarded Risk."

Organizations in this stage focus on speaking "business language" rather than "risk language." They are able to identify and respond to emerging risks ahead of the curve, using common taxonomies, common approaches, well-oiled decision-making processes, and, most importantly, data to support their decisions. This is where the full power of Risk Intelligence comes to bear, as the organization explores and exploits the Opportunity Landscape.

IT'S MORE THAN TECHNOLOGY

GRC is not a challenge that can be solved simply with technology. It is a business imperative that must be addressed through a shift in focus, priority, and culture within a company that makes risk management an integral and proactive part of how the company thinks and acts. This is the Risk Intelligence that will drive your company's success. By driving better Results and broader Reach, your GRC program can demonstrate significant Value to your organization. This requires a GRC maturity journey to take risk and compliance efforts from Siloed approaches, to consistent Managed processes, to an enterprise class Advantaged program that provides the competitive advantages that come with harnessing risk.

RSA

DISASTER RESOURCE GUIDE

SPECIAL EDITION

7 From the Publisher: Decrease Risk. Increase Resilience
BY KATHY RAINEY

8 Supply Chain Risk
BY LYNDON BIRD

12 IT Complexity and the Risk of IT Failure
BY JON TOIGO

18 The Importance of Design Teams in Creating a Targeted Cyber Breach Exercise
BY REGINA PHELPS

22 Operational Resilience Research Reports

24 Top Considerations When Choosing BCM Software

30 2016 BCM Software Features Matrix

The Disaster Resource GUIDE has been published since 1996 by The Emergency Lifeline Corporation of Santa Ana, CA. Emergency Lifeline was founded in 1985 by Kathy Rainey in response to the devastating Mexico City earthquake, with the mission to help organizations, government agencies and families prepare for earthquakes. The GUIDE is an extension of that mission and provides valuable resources to businesses and other organizations worldwide to help them build resilience.

On the Web Visit the Online GUIDE for more on this subject. **www.disaster-resource.com**
Crisis & Emergency Management • Disaster Recovery • Business Continuity • Homeland Security

MAIL-GARD® to the RESCUE

Printed and mailed communications to your customers are critical to your compliance and your bottom line…

Do you have the right recovery plan in place?

Mail-Gard Can Help!

- We are the nation's leading provider of print-to-mail business continuity and disaster recovery services with an unbeatable 100% recovery success rate.
- A recovery plan with Mail-Gard not only gives you peace of mind in the event of a business disruption, but also when peak production loads wreak havoc on your schedules.
- A continuity and recovery plan with Mail-Gard means your communications are delivered to your customers on time, keeping you in compliance and keeping you in business!

Mail-Gard®
CRITICAL COMMUNICATIONS RECOVERY
A Division of IWCO Direct

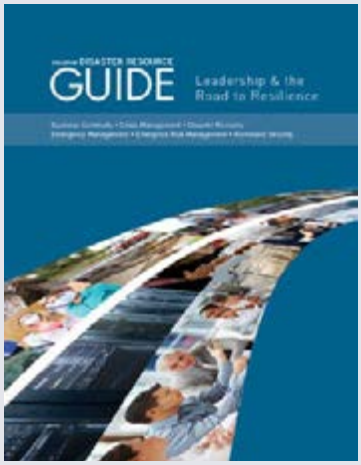
Call 1-800-220-2066 or email us to learn more
mailgardsales@iwco.com • mailgard.com

THE GUIDE ...

Bringing the Whole Industry Together –

Business Continuity • Crisis Management • Disaster Recovery •
Emergency Management • Enterprise Risk Management • Homeland Security

ANNUAL GUIDE | SPECIAL EDITIONS | CONTINUITY EGUIDE



The Disaster Resource GUIDE

Since 1996, the annual GUIDE has brought together the best of the best in one single volume. We go to dozens of conferences where we find products and service solutions for real business needs. All year long, we comb through periodicals, e-newsletters, whitepapers and reports for trends and best practices. We talk to professionals working at the local and national level. And it all comes together each year in the annual GUIDE. By the way, you must sign up every year to get a free copy. Go to www.disaster-resource.com/freeguide

Special Edition DR GUIDEs

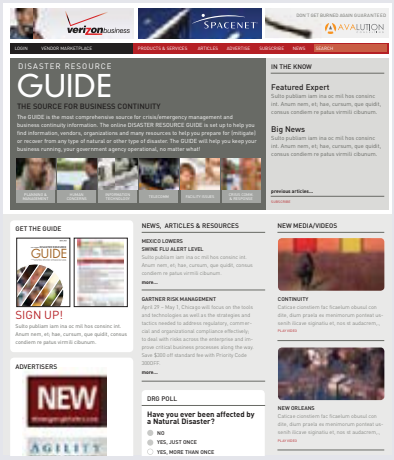
The Disaster Resource GUIDE is growing to meet the changing needs of the Business Continuity, Emergency Management and Homeland Security marketplace. The annual GUIDE covers six content categories and includes an extensive directory of organizations, products and services. Special edition, single-focus DR GUIDEs will be published several times during the year. If your organization would like to sponsor a Special Edition topic, email us at: publisher@disaster-resource.com.

The Continuity eGUIDE

On Wednesdays, the Continuity eGUIDE provides a concise snapshot of the business continuity and emergency management industry from around the world right down to the local level. Based on the philosophy of "working together", the eGUIDE integrates, consolidates and communicates resources from organizations that are leaders in business continuity, risk management, crisis management, emergency response, and disaster recovery. For a free subscription go to www.disaster-resource.com/freeguide

Planning & Management | Human Concerns | Information Availability & Security | Telecom & Satcom | Facility Issues | Crisis Communications & Response

ONLINE 24/7



The Online GUIDE

At your fingertips, you will find links to all the important places. Looking for a product or service? You can search by vendor or by product category. Want to know the best articles published in the past 12 months? We list articles from a dozen periodicals and include links directly to the articles in many cases. Our industry organizations directory includes more than 300 updated groups. On our homepage you will find new articles and press releases which are updated on a regular basis. Come to the online GUIDE – we'll be sure you stay connected! www.disaster-resource.com

◄ Core Content Areas

From the Publisher

DECREASE RISK. INCREASE RESILIENCE.

The devastating 1985 Mexico City earthquake highlighted the need for preparedness and preplanning. Human suffering and business failures could have been significantly reduced if emergency preparedness and business continuity planning had been a pre-earthquake priority.

The event was a career-changer for me. I began to research and aggregate solutions for preparedness, prevention, mitigation, response and recovery. As I uncovered "treasures", I became passionate about communicating these resources to the public and private sectors.

In the early 90s we worked to integrate the disciplines of emergency management and business recovery. 20+ years later we need a larger umbrella to integrate incident management, business continuity, crisis management, enterprise risk, governance and compliance.

Our mission is to consolidate and communicate resources to help decrease risk and increase resilience in every corner of a business and community. This Operational Resilience edition is the first of a series focused on resilience.

I like this definition from Gartner, a leading information technology research and advisory company:

"Operational resilience is a set of techniques that allow people, processes and informational systems to adapt to changing patterns. It is the ability to alter operations in the face of changing business conditions. Operationally resilient enterprises have the organizational competencies to ramp up or slow down operations in a way that provides a competitive edge and enables quick and local process modification".

The Future is Community

Publishing has changed during the past 30 years, with content growing exponentially. Today the GUIDE has unprecedented opportunity to curate and present the best of the best solutions via an online platform where professionals connect and collaborate 24/7. We believe the future growth for our industry will be linked to building a community of BC/DR/EM/RM/GRC professionals who will connect, create and collaborate online.

We are working to create a community called the Risk & Resilience HUB.

Want to know more? Will you join us?

Let me hear from you via email, publisher@disaster-resource.com

Kathy Gannon Rainey
Publisher

SUPPLY CHAIN RISK

BY LYNDON BIRD

The exact nature of Organizational Resilience and how it differs from traditional Business Continuity has generated much heated debate and very few definite conclusions over the past five years. One concept most agree on is that resilience is more than responding to disruptive incidents. It is about being agile and having the embedded capability to adapt to changing circumstances. Whilst it is clearly not possible to be resilient without continuity, a resilient organization achieves that continuity mainly through pro-active cultural change rather than through fixed response plans.

This becomes a very important distinction when looking at Supply Chain risk. While a company may have many vendors, for most companies there are a few very critical ones and probably a significant number of important ones. Beyond that there may be thousands of providers of minor services and routine goods. From a resilience perspective, we need to understand which supply chain interruptions can harm us and which can be handled routinely as part of normal daily operations. A good BCM program will tell us which vendors, bought-in services, raw materials and logistics are critical. We will also know how long we can operate without such services and what we will do to prevent that time period from being exceeded. I would argue that a totally resilient organization would handle all of its supply chain disruptions as "business as usual" without invoking any formal Crisis Management or BC Plan. Few companies could claim to be at this level today and it will probably remain an aspiration rather than a reasonable target for most.

However, the importance of manging Supply Chain risk effectively has wider implications than the success or failure of an individual enterprise. The UK Government publishes a National Security Strategy Report every five years in which it articulates the biggest risks facing the country. In the 2015 version, it identified what it called the four "Tier 1 Threats" to the UK as a whole. These were physical terrorism, cyber (crime, espionage, terrorism), state-based hostile actions and the erosion of rules-based international order. It takes little imagination to realise that the current global supply chain model is massively at risk from all of these threats. This is implicitly recognized in the report with supply chain weaknesses identified as the major vulnerability that could be targeted by any or all of those Tier 1 threats.

Although the UK is particularly open in publishing this type of assessment, it is certain that these views will not be significantly disputed by other governments, given that supply chain risk is a totally interconnected and genuinely global issue. The problem that democratic governments face, however, is that although they have the power to make policy in this field, the actual resources (food, fuel, power, medicine, accommodation, cash) that are needed to implement that policy are mainly in private hands. In any situation short of war or a declared national emergency, elected governments cannot direct the private sector to do anything except that required by law or regulation. There are many examples of private firms delivering impressive levels of support, on a voluntary basis, to the population following major disasters - with Walmart's work after Katrina often being quoted as one of the most inspiring. Realistically, it is perhaps unsurprising to see businesses responding well in such circumstances - but disasters of that scale are fortunately still relatively rare. The level of partnership needed between government and business to tackle global supply chain risk and make an entire country, its citizens and its wider economy more resilient is, unfortunately, greater than most countries are willing to support. The investment required is much less compelling than the response triggered by a high profile incident. Hence it is much harder to maintain the necessary focus and support required from private industry to achieve any significant cultural change at the Board level.

The argument that governments usually make is that supply chain interruption puts the country at serious risk of critical national infrastructure failure, exposes weaknesses in security and emergency services, causes unemployment and social unrest if leading industrial companies fail (not to mention the shortfalls in tax collected) and damages the nation's overall reputation if it is unable to function orderly and effectively.

So why are we in this state? Techniques such as Just-In-Time, Lean Manufacturing and Offshoring have boomed over the past two decades, resulting in cost benefits that are easy to calculate because they are almost entirely quantitative. Generally, the risks of longer and more complex chains are also well recognized. However, since no one can really prove if and when those risks will materialize, the arguments in favour of mitigation strategies that cost money tend to be subjective and easier to ignore. So we need to be clear in our arguments to senior executives; complex chains are difficult to monitor or manage in any meaningful sense, with full transparency across the entire chain impossible to achieve. Cost saving has resulted in more risk acceptance, with service and quality inherently compromised. Globalization is inevitable, but needs to be managed more proactively and with more strategic oversight.

> Typically, the three most important reasons for supply chain disruption are unplanned IT/ telecoms outages, cyber-attacks/ data breaches and adverse weather.

It is becoming fashionable to see globalization as the root cause of the problem and "jobs for our people" is being advocated by some leading politicians in both the US and Europe. However, it is difficult to see that enough political pressure could be exerted on massive global corporations to reverse this trend. Shorter supply chains and localization works well in some niche markets, but it is not the fundamental direction of travel for the world economy.

What cannot be really disputed is that all organizations (commercial, public or charities) have vendors on whom they rely. Even those who are not in the business of moving physical assets around have key vendors like utility suppliers or outsourced operational activities. A number of international surveys have been undertaken over the past few years, all of which show similar results. Typically,

CONTINUED ON PAGE 10

CONTINUED FROM PAGE 9

the three most important reasons for supply chain disruption are unplanned IT/telecoms outages, cyber-attacks/data breaches and adverse weather or "natural" disasters such as earthquakes. Interestingly, of course, this is pretty much the same list that similar organizations quote when asked about risks to their own operational continuity. However, when you look beyond the headline threats, there are often many risks which are particularly driven by the complexity of supply chains. Among these are arbitrary boundary closures due to migration pressure, transportation disruption, outsourcer commercial failure, labor disputes, differing laws and regulations, quality faults causing product recall, business ethics violations and failure to protect intellectual property rights. All of these risks grow rapidly as suppliers become more geographically diverse and less directly controlled by the parent or sponsoring organization. While such risks can be relatively easily managed in a domestic market, globalization provides almost unlimited potential for accidental failures or complex, deliberate criminal activity. Additionally, the scrutiny placed upon all firms today by the ever-present social media creates an ever increasing need to understand what is happening in the wider supply chain. Now a single incident in a tier 4 supplier in the developing world can almost overnight destroy reputations for social responsibility that a firm may have taken many generations to build.

What can we do about it? As individual managers in companies of all sizes and types we are not able to solve this problem alone. Nevertheless, the techniques that we have developed over many years in our business continuity programs act as our best starting point. The five-point plan below might help organizations get a grip on this key issue.

1 Build on your Business Impact Analysis (BIA). Use the same definitions and thresholds to categorise vendors (or specific purchased items) as you use to identify processes or activities in a regular BIA.

2 Classify your vendors on potential operational impact. Measure that impact exactly the way you would for loss of an internal system. Talk to your procurement people about your findings but do not use their vendor classification which will be usually based on spend or some subjective risk assessment.

3 Develop individual collaborative strategies for "show-stoppers". There are probably a very small number of "stop-stoppers". These are most likely to be strategic outsourced operations or a unique component/feedstock needed by manufacturing or process plants. There is no simple way around this; you cannot just rely on contracts or SLA's and you must work individually with such vendors to find joint working methods that guarantee product or service availability. You must genuinely see your supplier as an equal partner – and treat them accordingly at all times. Some partnerships fail, of course, but even then you need to know how you would manage the "divorce".

4 Agree on measurable resilience criteria for important vendors and monitor them. It is not feasible to give this group the same individual attention as above, although you must agree in contracts your expectation from them in all circumstances including disasters to you (additional support perhaps needed) and disasters to them (your importance in their recovery plan). You should look for proof of their reliability and capability to deliver in exceptional circumstances and agree on a monitoring schedule to ensure they continue to meet your expectations on an ongoing basis. Certification against an appropriate standard might help but is not sufficient proof in its own right that they will be able to supply you in all situations. Generally, single source suppliers should be discouraged and if possible a geographically better spread of strategic inventories introduced.

5 Work with procurement to define potential operational impact for new vendors. New vendors need to be assessed against resilience criteria as well as financial criteria. Co-operation between procurement and resilience professionals is essential in setting such criteria. This might prove challenging, as resilience often adds some degree of cost.

The final sentence in point 5 (above) is perhaps the true measure of how resilient an organization really wishes to be and how mature it is in understanding the global problems it faces and the ultimate consequences of not investing in resilience.

ABOUT THE AUTHOR

Lyndon Bird, (Hon) FBCI, has worked exclusively in Business Continuity since 1986. He chairs the Future Vision Committee for New York-based DRI International and edits the quarterly "Journal of Business Continuity and Emergency Planning". He is also well known internationally for his former role as Technical Director of The Business Continuity Institute from 2006 to 2014. He can be reached at lbird@drii.org.

Disaster Recovery Journal

Fall World

Phoenix, Arizona 2016

September 18-21, 2016

New Solutions for Resiliency and Risk Management

Visit DRJ's Premier Industry Events:

DRJ's Fall World 2016 - September 18-21, 2016 - Phoenix, AZ

DRJ's Spring World 2017 - March 26-29, 2017 - Orlando, FL

Also available on your favorite Social Media Sites

www.drj.com

DISASTER RECOVERY JOURNAL

DRJ is a Proud Global Partner of The BCI

IT COMPLEXITY AND THE RISK OF IT FAILURE

BY JON TOIGO

For the past few years, the unabashed enthusiasm around clouds, virtualization and software-defined everything has led to some unfortunate side effects. One is the suspension of disbelief around the vulnerability of all of this "new" architecture to unplanned interruption events. Even today, it is not uncommon to read a trade press article or listen to a conference speaker claiming that disaster recovery is obsolete – replaced by the high availability architecture of the cloud era. Nice if it were true, but it really isn't.

A year or two back, when we were calling cloud-based computing infrastructure "Infrastructure as a Service" or IaaS, the National Institute of Standards and Technology (NIST) did a fair job of taking the hype down a few pegs. They noted that it would be wonderful when servers were all virtualized and when networks and storage were all software-defined, and when administration and orchestration tools had been developed to the point where they could effectively automate many of the functions for provisioning hardware and software resources to workload.

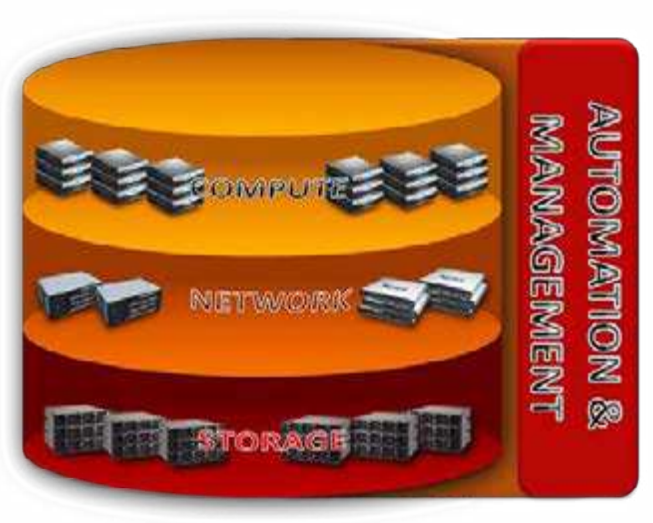


FIGURE 1: NIST model for virtualized/software-defined resource pools.
SOURCE: The Data Management Institute LLC. All Rights Reserved.

They were also careful to describe the reality of the situation. Cloud actually did nothing to change the requirements for operating an enterprise class data center. Doing IaaS, or Platform as a Service (PaaS) or Storage as a Service (SaaS) required a number of layers of operations and management tasks – most of which were familiar to data center operations staff and management.

And, of course, whether the data center was of the "private cloud" variety – servicing the needs of internal or corporate users solely – or a "public cloud" – providing services to numerous subscribers on a multi-tenant basis – there were still a set of overarching business management functions that would need to be attended to. NIST called them a "service delivery layer."

The point that NIST researchers were making was that not all that much had changed from a procedural or process perspective between legacy and cloud-based data centers. Other commentators added that the most significant change was that new technology – mainly software stacks – were being introduced at a breakneck pace. Whenever this happens in IT history, the propensity for unplanned interruption events (aka disasters) generally becomes more likely than less.

Part of the explanation, of course, is the "learning curve" confronting those who must deploy and administer the new technology. Making new technology do what it says it does in the brochure is often a challenge. Absent a pedigree or experiential record on which to base "best practices," and absent any sort of agreed-upon definitions or standards, the IT administrators must work their way through technology by old fashioned trial and error.

Today, after nearly 11 years of trying, server virtualization advocates have

CONTINUED ON PAGE 14

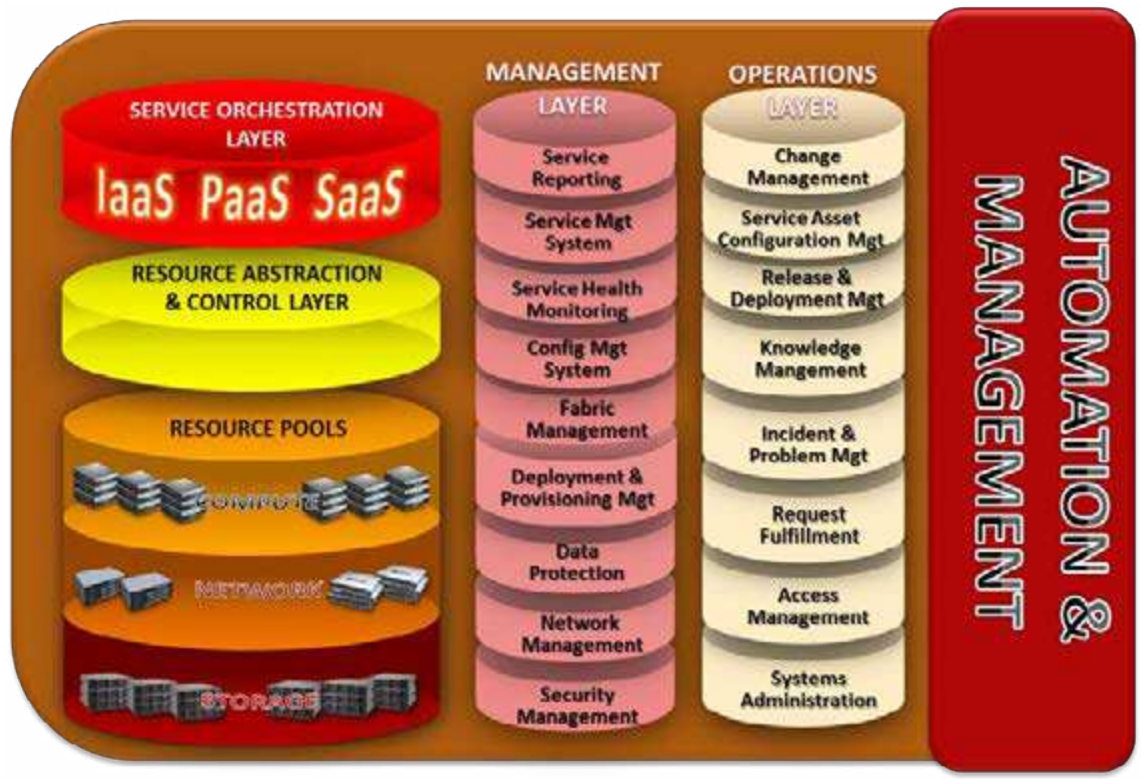


FIGURE 2: Management and Operations tasks also need to be performed in the cloud data center.
SOURCE: The Data Management Institute LLC. All Rights Reserved.

CONTINUED FROM PAGE 13

FIGURE 3: The service delivery layer is also required for cloud-based infrastructure delivery.

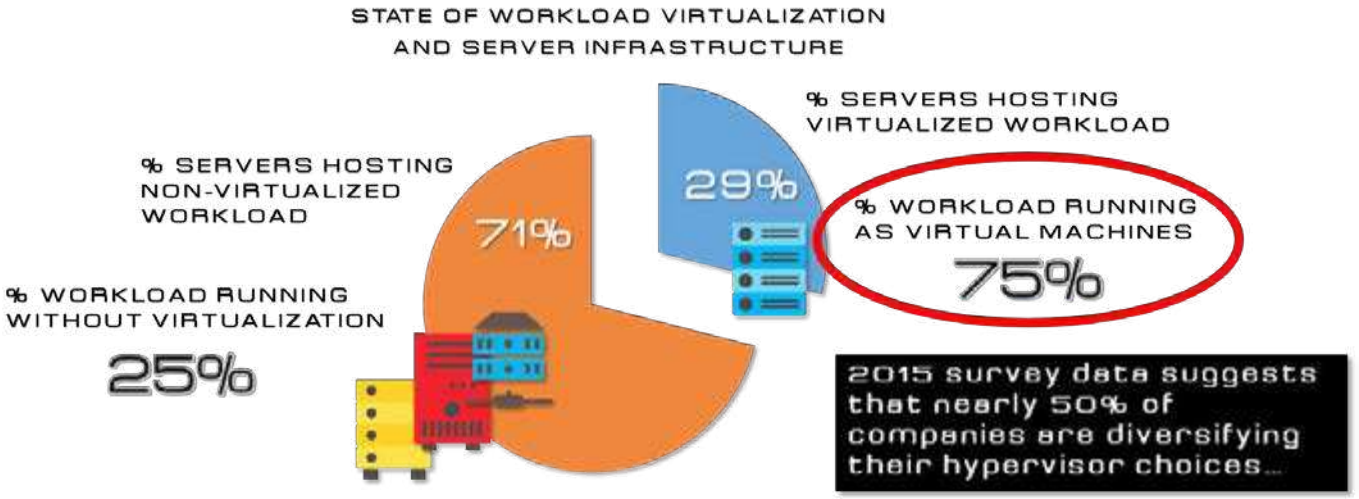


FIGURE 4: Distribution of workload and computing platforms c. 2016 (a composite of several leading industry analysts).

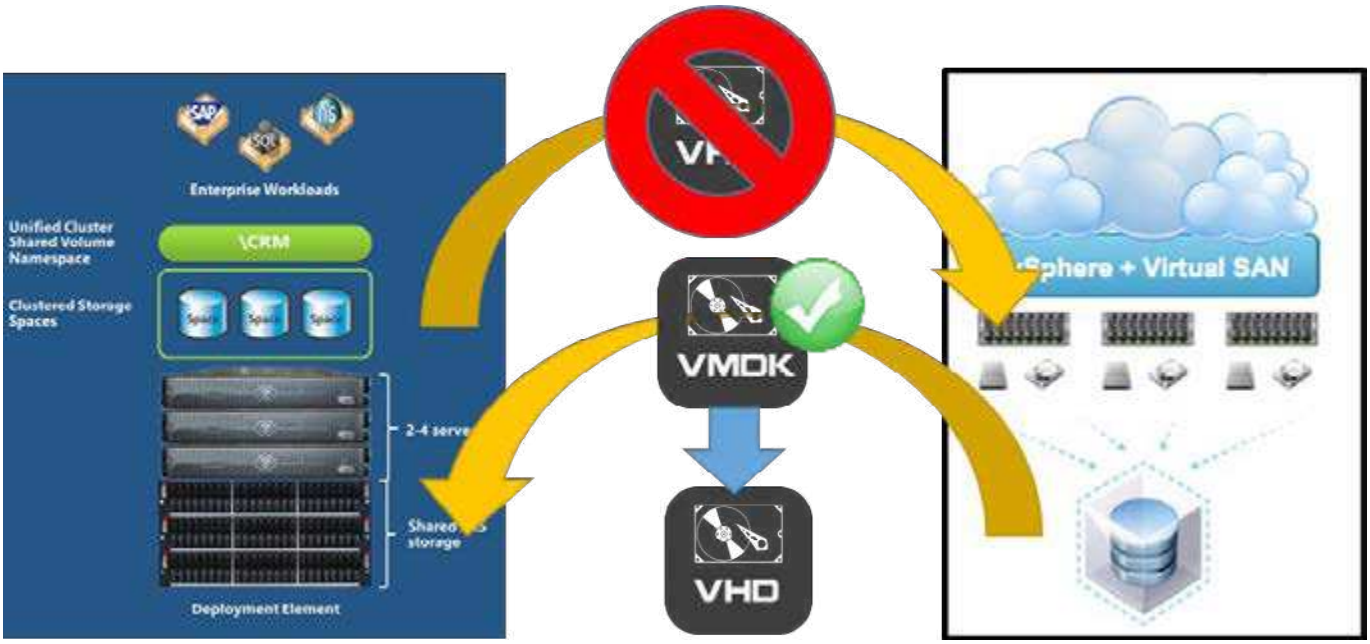


FIGURE 5: Storage sharing challenges in different hypervisor-controlled infrastructure. No sharing VMware VSAN space with Microsoft Hyper-V workload. Hyper-V storage – clustered storage spaces – can be shared, but only if the VMware workload is first converted to Hyper-V format.

realized their vision of placing up to 75% of workload in virtual machines running on hypervisor software using about 29% of data center hosting hardware. Non-virtualized workload, mainly transaction-oriented systems, continue to run on the other 71% of hardware, creating at least two distinctly separate targets for data protection and disaster recovery planning.

The "gotcha" in this picture is the 75% of virtualized workload. The latest surveys conducted by media firms suggest that companies are abandoning the single sourcing of hypervisor software technology. They are diversifying their hypervisor software and using different hypervisors for different workloads. The result is the creation of yet more "siloes" of hardware and software technology, especially when each hypervisor vendor has a preferred and proprietary stack of software-defined networking and software-defined storage beneath its hypervisor software "head."

So, rather than reducing the complexity of infrastructure, new technologies for cloud-ification and software-defined are actually adding to complexity – with potentially hazardous results. A simple example is in the inability to share software-defined storage created with the technology of one hypervisor vendor with the data from the workload hosted by a different hypervisor technology. We seem to have returned to many of the issues we had when Sun Microsystems and Microsoft could not share data (pre-SAMBA): VMware will not allow data from Microsoft Hyper-V workload to be stored on VMware-controlled "Virtual SAN," their flavor of software-defined storage. By contrast, Microsoft says that their "clustered storage spaces" can store data from a VMware host, provided it (the VMware VMDK workload file) is first transformed via a software utility into a native Hyper-V workload file (a VHD).

Clearly, the technology silo-ing that is accompanying the march toward clouds is also adding complexity. Within a single vendor's software-defined storage technology, there tends to be a requirement for multiple nodes of storage (for high availability data replication) and also a requirement for "identicality" between nodes and between clustered server hosting environments. Identicality is the hob goblin of efficient recovery planning and a huge cost accelerator for business continuity.

For example, a hypervisor provides a software-defined storage (SDS) definition and software stack that is proprietary to the hypervisor vendor. Not only can data not be replicated from the storage on this kit to the storage on a rival hypervisor vendor's kit, it may also be difficult to replicate data between the storage nodes controlled by the same hypervisor… if all components of each node are not identical. This was traditionally a problem with monolithic legacy storage arrays, in which synchronous mirroring or asynchronous replication software functionality delivered on the array controller required an identical controller, running identical software, on identical storage media, in order to operate. We are seeing the same thing with the SDS storage nodes defined by VMware, Microsoft, et al. Only DataCore Software, and perhaps IBM with its SAN Volume Controller (if this is ever part of their SDS product offering) are currently hardware agnostic.

CONTINUED ON PAGE 16

CONTINUED FROM PAGE 15

Another by-product of proprietary SDS, by the way, is dramatically accelerating rates of annualized storage capacity demand and cost. In 2011, IDC said there were roughly 21.2 exabytes of external storage deployed worldwide and that capacity demand would grow by about 42% per year through 2016. In 2014, the analyst said that the rate of capacity demand in highly virtualized environments was closer to 300% per year – owing in part to the preference among hypervisor vendors for an SDS topology requiring three identical storage nodes (minimum), each with identical components for local data replication and protection. Gartner revised this estimate to 650% annual capacity demand growth, acknowledging that companies would field two or more identical platforms of three storage nodes each to achieve high availability.

The point is that placing a redundant facility within 80 km of the primary data center does not necessarily provide much protection against a milieu level disaster event.

Lack of technology pedigree and best practices, plus technology silo-ing, and identicality requirements are joined by one more factor that is increasing the complexity of IaaS environments – and by extension the risk of downtime. The fourth problem is network dependency.

Truth be told, most public cloud services are well within the 80 kilometer radius believed by experienced disaster recovery planners to be the absolute minimum safe distance that a recovery site or off-premise backup facility should be from the primary data center or original data storage facility. The reason is simple. To obtain a 1 Gb per second link speed that most experts regard as minimally acceptable for delivering a "good user experience" of cloud-hosted applications, companies typically utilize high speed metropolitan area network facilities to connect their data center or user work areas to cloud service providers. Network facilities like MPLS are available in most NFL cities and can deliver the networking bandwidth required at a reasonable cost. To get 1 Gb/s speeds on a WAN, you need much more expensive facilities, like OC-192.

Why MPLS or OC-192? Simple. To move 10 TB of data across one of these facilities will require about 2.25 hours. Moving the same quantity of data across a T-1/DS-1 facility like those typically used for Internet connectivity would require over 400 days.

The problem is that, even with the availability of MPLS, the separation distance between the primary data center and the cloud is usually inadequate to protect against a disaster with a broad geographical footprint. Hurricane Sandy pummeled Manhattan and forced many firms to abandon their data centers because of flooding and power outages. The same storm caused water to encroach on a hot site facility (a commercial disaster recovery facility) in Philadelphia – 94 miles (or 151 kilometers) away. Nervous high availability advocates observed that a storm with such a footprint was a once in 200 year event, and reassured customers that most disasters – those that cause the most annual downtime – were logical and localized, not large-scaled CNN-style events. That might be true, but it came as no consolation to the Manhattan firms that received another massive weather disaster roughly nine months after the first 1-in-200-year event.

The point is that placing a redundant facility within 80 km of the primary data center does not necessarily provide much protection against a milieu level disaster event. Yet, many companies go this route to save money and to keep distance-induced latency to a minimum. The problem is that there is so much traffic today that network pipes are being saturated. Even short haul networks are being swamped by serialization, queuing and buffering that are collectively referred to as "jitter" – even over short distance connections. So even with a MAN, companies are finding that challenges about to failing over a hosting system with interdependent applications. Invariably, the mirrored systems at the remote site or public cloud are lagging behind the primaries – by several transactions in the case of on-line transaction processing databases. IBM and Duke University are doing some very public testing of this situation in an effort to surmount it.

Bottom line: the issues raised in this article are only a high level summary of four of the leading issues that are adding complexity and risk in the cloud computing era. Planners need to be aware of them and to develop workarounds as best they can. Remember that virtualization, software-defined and cloud technologies are all in their comparative infancy, operating in a standards-free environment with vendors appearing on (and disappearing from) the horizon on a monthly basis. Companies are taking a risk in adopting many of these technologies before they have been thoroughly vetted in the marketplace, so they need to maintain a clear-headed perspective of their exposures and take more (not less) steps to prevent avoidable disasters and to prepare strategies for coping with the vulnerabilities they cannot eliminate.

ABOUT THE AUTHOR

Jon Toigo is CEO of Toigo Partners International and a consultant who has aided over 100 companies in the development of their continuity programs. Feel free to contact him at jtoigo@toigopartners.com.


Introducing the new Virtual Corporation.
virtual corporation
www.virtual-corp.com

THE IMPORTANCE OF DESIGN TEAMS IN CREATING A TARGETED CYBER BREACH EXERCISE

BY REGINA PHELPS

Businesses and organizations defend against unending attempts to steal their computer data or damage their systems. Few, however, have serious plans for how they will respond to the impact of an actual breach. And even fewer stress-test those plans. Exercising a cyber-breach scenario forces real-time decision-making and actions. Creating an exercise with a cyber-incident scenario is infinitely more complicated than creating one with a "normal" emergency scenario, and requires special care in design.

Where to Begin?

Let's say you are tasked with creating a cyber-breach exercise. You're probably not quite sure how to go about it. What you need to make this exercise "spot on" is a highly-tailored narrative and highly-specific injects built around a set of pre-defined technology and information security incidents. You can't do that alone; you need help. And you don't need just any help, you need the right help. What you need are TWO Design Teams.

Why You Need Two Design Teams

You need two Design Teams because you need two very distinct and different sets of skills. First, you need a Technology Design Team that is very technical, detailed, and deeply in the weeds of the scenario. You should spend a lot of time picking the right narrative and then dissecting it. The Technology Design Team's main focus should be to identify all the different affected systems and their interdependencies and connection points.

You will also still need a Business Unit Design Team, but the Technology Design Team needs to do their work first, because you can't create the overall exercise injects until you know the technology issues and failures. Think of it like a Christmas tree

– the technology issues, failures, and problems are the trunk and branches; they provide the solid foundation for the story. The business unit injects are the reaction to those issues – like ornaments hanging on the tree. You can't hang the ornaments without the trunk and branches, and you can't design the business unit injects until you know the IT failures.

This author's firm, EMSS, always establishes the technology design first, followed by the business design. We then circle back with the technology team to review the business unit injects to make sure they align with the stated technology issues.

Technology Design Team

For a cyber-based scenario, there are often five to eight members on the Technology Design Team. (Because of their experience in the company, some members can cover multiple topics.) You'll likely need subject matter experts in the following areas:

- Information Security
- Infrastructure
- Application Development & Support
- Network
- Database
- Network Operations Center
- Help Desk
- Storage

Business Unit Design Team

Your Business Unit Design Team has one primary goal – to develop the exercise injects that play off the cyber-breach story, see Table 1. (As mentioned, the Business Unit Design Team shouldn't hold meetings until the Technology Design Team has completed its work.) The type of members needed for your Business Unit team will depend on the overall cyber-breach narrative. If you have a physical impact in the story as well as a cyber impact, you will also need to include facilities and security on your Business Unit team.

A top-notch Business Unit Design Team member will have several qualities; they should have:

- A good basic knowledge of the overall business.
- At least a year or more with the company in order to know some of the ins and outs of the place.
- Subject matter expertise in an area you will likely be touching on in the narrative.

> "If everyone is moving forward together, then success takes care of itself."
>
> – Henry Ford

A typical Design Team will include members from the following departments:

- Representatives from all of the key lines of business (to help you develop highly specific business injects).
- Facilities.

CONTINUED ON PAGE 20

Call #	Time	Design Team Member (Simulator)	Routing	Caller's name, title, dept	Call Script
1				←Caller name, title, dept→	We have issues printing ←name of→ reports. Sometimes it prints and other times it does not. Can someone help us?
2				←Caller name, title, dept→	We posted our transactions into the Billing system, however the data did not transfer to SAP, therefore, we can't balance our end-of-day.
3				←Caller name, title, dept→	We try to insert the ←name of→ reports into Sharepoint but cannot because we are unable to access ←app name→. Is there an issue with Sharepoint?
4				←Caller name, title, dept→	I cannot open the ←name of→ spreadsheet. I can't update my cash flows.
5				←Caller name, title, dept→	My workstation was identified as one of the ones that are compromised. Do I have to use another workstation? Where can I go to work?

Table 1, Sample Injects

CONTINUED FROM PAGE 19

- Physical Security.
- Human Resources.
- Communications.
- Investor Relations.

Note that the departments listed above are typical of Design Teams. Your organization may benefit from having team members representing a different 'slice' of your business.

The "Other" Role for Your Design Team Members to Play

Design Team members usually make great Simulation Team members. Because they have been involved in exercise design and inject creation, they know the exercise intimately and are already a cohesive team. (They can help on the Simulation Team, but would not be players in the exercise because of their knowledge of the injects. The author's book reviews this in greater detail. See below for a link to the book.) If you plan to ask them to be Simulators in addition to their design job, in the interest of fair disclosure regarding the time commitment for the project, be sure to include that task when you ask for their participation at the beginning of the process. Besides the time commitment needed as a Business Unit Design Team member (see next section), here is the additional time your Designer-turned-Simulator needs to carve out (times are approximate):

- Simulation Team orientation: Ninety minutes to two hours (usually occurring a few days before the exercise).
- Exercise day: However long you have scheduled the exercise.

> "Alone we can do so little, together we can do so much."
>
> – Helen Keller

Design Team Meetings

In our experience, most Design Team meetings last between 90 minutes and two hours. They work equally well when held face-to-face or as a conference call. However, you might wish to do the first meeting face-to-face to make sure everyone is on point. EMSS routinely holds Design Team meetings by conference call, and find them to be a highly efficient and effective use of everyone's time.

How Many Meetings and How Often to Have Them

For an "average" cyber exercise, EMSS usually holds around four meetings with each team, for a total of eight meetings (four technology, four business). However, for a large Functional or Full-scale exercise, it's entirely possible to need between six and eight meetings for each team. It all depends on the scenario complexity, the length of the exercise, the sophistication of the team, and the team's familiarity with the exercise design process itself.

Design Team meetings are usually held every other week. You don't want to lose the team's momentum by waiting too long between meetings. Conversely, the team needs time to do their homework (e.g., doing their 'trench coat' research or writing injects).

Who Does What?

The Technology Design Team has two major tasks: To develop the cyber-breach narrative, and to develop the cyber-breach injects. The Business Unit team develops the injects that reflect the impact of the technology situation on the business side of the organization. (And, as mentioned before, hopefully, both sets of team members will act as Simulators on the day of the exercise.)

Summary

Both Design Teams are critical to a successful cyber exercise. Selecting the right team members will make your exercise credible, exact, and challenging. It will also engage more people in your program and help to build a culture of awareness and support for your program.

This author's book, "Emergency Management Exercises: From Response to Recovery, Everything You Need to Know to Design a Great Exercise" focuses on Advanced Tabletop, Functional, and Full-scale exercises, and covers everything from broad strategies to minute-to-minute decision-making. It also provides very specific, step-by-step instructions – starting from the earliest planning to after-action reports. Find it on Amazon at http://tinyurl.com/j6skbh8.

ABOUT THE AUTHOR

Regina Phelps is an internationally recognized expert in the field of crisis management and contingency planning. She is the founder of Emergency Management & Safety Solutions (EMSS), founded in 1982. Services include crisis management team development, pandemic planning, exercise design and facilitation, and business continuity plan development and audits. She can be reached at: Regina@ems-solutionsinc.com and www.ems-solutionsinc.com.

The Perfect Marriage

BCM Software & Mobile App

RPX™ AND **HELP** Home Enterprise Live Planning

Depth, flexibility & scope for a Planner, yet simple enough for the casual User

- ***BCM, DR & COOP***
- ***Risk Assessments***
- ***Business Impact Analysis (BIA)***
- ***Crisis / Incident Mgmt*** *w/notification*
- ***Exercise / Testing***
- ***Compliance***

A recognized leader since 1999

Business & Home Preparedness & Continuity . . . in One Mobile App

Show your employees you care while taking care of business

RECOVERY PLANNER .COM

Go to RecoveryPlanner.com for a demo

(877) 455-9990 ◆ +1 (203) 455-9990 ◆ www.RecoveryPlanner.com ◆ @ RP_BCM

HQ-USA ◆ Toronto ◆ London ◆ Nairobi ◆ Sao Paulo ◆ Sydney ◆ Santo Domingo ◆ Mexico City ◆ Moscow ◆ Lisbon ◆ Middle East

OPERATIONAL RESILIENCE RESEARCH REPORTS

BUSINESS CONTINUITY INSTITUTE (BCI) HORIZON SCAN REPORT FOR 2016

The Business Continuity Institute has released its 2016 Horizon Scan Report featuring a wealth of information related to risks and resilience worldwide. The report is based on 568 organizations responding from 74 countries, and presents Top 10 Threats, Top 5 Trends, and statistics on business continuity budgets.

The top 3 threats were related to data and included Cyber Attack, Data Breach and Unplanned IT & Telecom Outages. The top trend relates to IT as well, followed by Social Media Influence.

The report also highlights the increasing acceptance of ISO 22301, with 51% of organizations indicating adoption of the ISO standard as a framework for business continuity management.

Significant increases in business continuity investment are anticipated, with much smaller percentages of organizations anticipating a reduction.

The full report is available to the public, at no cost, for download after a simple registration. Click here for the download page.

MANAGING OPERATIONAL RESILIENCE

A thorough and well written article, Managing Operational Resilience, is available from the Cyber Security and Information Systems Information Analysis Center. The report was written by three authors associated with the Software Engineering Institute (SEI) at Carnegie Mellon University.

The report, after an overview and definition of operational resilience, begins with an analysis of why operational resilience is difficult to build and manage. It then details recommended practices to address these challenges within an organization. Those practices include governance program management, staff deployment, communications, risk management, incident management, service continuity, and more. The authors then offer suggestions for deriving more benefit from these efforts.

The full report is available at this link.

WHAT ROLE DOES THE PRIVATE SECTOR HAVE IN SUPPORTING DISASTER RECOVERY, AND WHAT CHALLENGES DOES IT FACE IN DOING SO?

The changing scope and scale of disasters, both natural and technological, have altered the ways in which disaster management and financing are addressed and the roles of private-sector organizations specifically. Businesses and nonprofit organizations are increasingly central to the process, offering critical support in immediate disaster response but also contributing necessary redevelopment funding that supports community recovery. Although these new expectations position the private sector as a key leader in community resilience, these responsibilities have not been fully met with established guidance or clear metrics for how and when these organizations should participate in disaster recovery and financing.

The Rand Corporation report, available at the link below, examines key issues confronting the private sector in disaster recovery financing, what roles private-sector entities have played, and where there has been successful integration or leadership of these organizations. The report also briefly explores challenges that the private sector faces, with particular attention to issues of information use and application, coordination in response and recovery, and timing of funding. Given continued data gaps in this field, the authors offer opportunities for research and policy analysis.

The report is available at this link.

FROM STANFORD BUSINESS: "IT'S HOW YOU GET THERE"

After growing up in a small town in Eastern Pennsylvania, David Cooper joined the U.S. Navy SEALs in 1986 to see the world. He was planning to retire from the military in 2001 to sign up for medical school when the World Trade Center was destroyed by terrorists on September 11, 2001. He stayed in the SEALs and spent the next 10 years in various war zones fulfilling what he sees as both an obligation and a privilege. Now he is cofounder and president of Karakoram Group, a consultancy in Virginia Beach, Virginia that specializes in solving complex risk management problems. An interview is posted on the Stanford Business website.

He comments in the interview: "People are really concerned about security — both cyber security and physical security. The demand signal is that people see the news. Wars are going down; murders are going down. But the use of terror tactics is going up; mass shootings are going up. People are concerned about Islamic terrorism, but that's media spin. Homegrown criminals and terrorists are copying those tactics. We have seen when an employee is mad at another employee, they might use terror tactics."

He offers additional, unique perspectives in the full interview, available here.

The *KOOL Kit*$_{tm}$

By Emergency Lifeline

The *KOOL Kit* has key benefits for families, friends and colleagues – and you!

72-hour* Support for 1 person:

Long-Shelf Life – most items have 5-year or unlimited shelf life

Economical – costs less than you could assemble on your own AND saves time.

And…the ***KOOL Kit*** is packed in a bag that can be used to keep things ***KOOL***!

Here's What You'll Find in a ***KOOL Kit*** …

- 1 Emergency Foodbar, 3600 Calories
- 6 Emergency Water Pouches, 4.22 ounces each
- 1 Mylar-Type Emergency Blanket
- 3 Adhesive Bandages, 1" x 3", sterile
- 2 Gauze Sponges, 4"x 4", sterile, (1 twin-pack)
- 4 Benzalkonium Chloride Antiseptic Wipes
- 2 Antibiotic Ointment, 0.5 g packets
- 1 Tenderskin Tape, 1/2" x 10 yards
- 1 12-Hour Green Lightstick
- 1 Whistle
- 3 Infectious Waste Bags with Ties
- 1 Personal Tissue Pack
- 12 Premoistened Towelettes
- 1 Toothbrush & Paste Set

*PREPAREDNESS TIP: Water Storage

The KOOL Kit includes minimum water amounts for passive and resting conditions. We suggest you supplement your preparedness with additional water storage. HOW MUCH? Ready.gov recommends that you store at least one gallon of water per person per day. Visit www.ready.gov/water to learn more about water storage.

Contact Emergency Lifeline for numerous ways you can economically store water in bulk storage for up to 5 years.

Get Your *KOOL Kit* Today! VISIT EMERGENCYLIFELINE.COM

To order in bulk at a discount, contact Emergency Lifeline at 800-826-2201 x801, sales@emergencylifeline.com

Emergency Lifeline Corporation, founded in 1985, is the publisher of the acclaimed Disaster Resource GUIDE, the One-stop Resource for Emergency Preparedness and Business Continuity.

SPOTLIGHT ON

BUSINESS CONTINUITY MANAGEMENT SOFTWARE

Top Considerations When Choosing BCM Software

BY TOMMY RAINEY

catalyst

RECOVERY PLANNER .com

virtual corporation

fairchild.app

PUBLISHER'S FORWARD

We appreciate the contributions of four BCM software vendors who helped us create this Spotlight. Their insights have illuminated vital aspects of business continuity management (BCM) software which ought to be considered when evaluating options. The executives in these companies are not just builders of powerful solutions. They are also industry thought leaders dedicated to operational resilience.

We intend the BCM Spotlight to equip our readers with questions to ask during an evaluation process. We are not ranking solutions nor are we vetting vendors. What is good for one organization might not fit another. We hope the following analysis will help you in your commitment to continuity and resilience.

A special thanks goes to Linda Hanwacker, The LSH Group. Her research on BCM Software formed the basis for our BCM Matrix.

As always, we welcome feedback. Email us at: publisher@disaster-resource.com

Plates are never big enough when you go through a holiday brunch line! We must make choices and leave some good stuff behind. In 2016, the options and features of BCM software are both tempting and overwhelming, but you don't necessarily need it all. And the right software for your organization can add tremendous value to your company's BC program. But how do you choose?

This article, accompanied by an extensive matrix (pages 30-38), will offer the following:

- Helpful insights whether you have or do not have BCM software
- What BCM software will not do
- When is BCM software appropriate
- Suggestions for the evaluation process
- Important features and benefits for consideration

Why This Spotlight is For You.

This article, and much of the BCM Software Spotlight, will be tailored for the organization considering a new implementation of a BCM software solution. However, if you already have a solution in place, before concluding this Spotlight won't benefit you, consider the following situations:

1. WE ARE HAPPY WITH OUR BCM SOFTWARE!

If you are pleased with your existing solution, the features and analysis in this Spotlight could reveal new functionality that would benefit your organization. These new features could be included in your existing software but not yet implemented. Or these features might address needs you didn't know could be solved with an alternative solution. In the fast-changing tech world of today, yesterday's solution will not necessarily be today's best option.

2. WE ARE NOT HAPPY WITH OUR BCM SOFTWARE!

One key concern for the organization looking to switch solutions would be the risk of trading known shortcomings for unknown ones. It is very tempting to see another vendor's approach to a problem and become enamored with that particular improvement. This could lead you to glide through the comparison process, overlook some key benefits of your existing solution missing from the new, and draw an irrational conclusion that a switch is justified. This Spotlight is intended to touch on a very broad set of considerations as you make your decision. Take advantage of this collection of insights from the leaders in this field as you carefully evaluate the best fit for your organization.

CONTINUED ON PAGE 26

CONTINUED FROM PAGE 25

What BCM Software Will Not Do

DON'T EXPECT A MAGIC BULLET!

The effective implementation of a BCM software solution can do many things for your organization, but first consider what it will NOT do. It will not take a ragged BC program and clean it up and make it good. Evaluating risks, understanding business processes, prioritizing both mitigation and recovery, and much more must all occur with or without software before a BC program can be effective. BCM software can help organize the complexities and it can help in the management and upkeep of your program. It can automate some complex processes such as crisis communications. Having the content digitized and available across many platforms can certainly increase resilience. However, BCM software is not a quick fix for a flawed program, nor will BCM software add value apart from significant effort on your part. Also, it is not a substitute for top management buy-in and widespread support across the management team. Get those in place, and BCM software will likely be a great benefit to your organization.

A painful story was published by one author in CSO:

"I was hired as a Business Continuity Manager for a national healthcare organization and was provided with a software package that I was to implement nationally. The time investment this particular software required was tremendous. In fact, the investment was so great that we scrapped it two years into its development. A significant waste of time, money, and energy for all involved, with my reputation on the line (though I was not even part of its selection)." [1]

When is BCM Software Most Beneficial?

WHICH ORGANIZATIONS WILL BENEFIT THE MOST?

There are two options for a BCM program. Using existing office software such as Word and Excel certainly appears attractive. Immediate costs are essentially zero, as everyone has access to this software and they do not need to be trained. However, this apparent cost saving can quickly be negated. Multi-location organizations will find coordination and input cumbersome. It will be difficult to get consistent plans with updates and modifications likely happening at each location. If your organization has regulatory requirements, reporting can become a critical function, and most office-suite or DIY solutions will not generate reports sufficient to meet regulations.

One industry study[2] suggests the costs of implementing a modern BCM platform could be less than a quarter of the costs of a DIY approach. Maintaining the information that is critical to your continuity program will be significantly greater with the DIY approach when multiple locations or multiple BCM components are saved in various locations.

Most business continuity professionals today would say the DIY approach is only appropriate in smaller organizations with one, or at most a few,

locations, and then only if the organization does not have regulatory reporting requirements. Other organizations would significantly benefit from BCM software. The critical issue is selecting the software which is best for your organization.

Suggestions for the Evaluation Process

EVALUATION PROCESS APART FROM FEATURES...

As you evaluate options, consider the following overall issues when you talk to providers:

1 Can you see demos of the software, or better yet, see an actual live installation? Review training materials and operating instructions?

2 Is your company considering any changes in other software which could impact how it links or works with the BCM software you are considering?

3 Can you get references from the provider? Can you discuss with the references what they find valuable in the software and then compare their priorities to your own to see if their assessments are relevant to you? They may be thrilled with the API to Salesforce, but you may use a completely different, hosted CRM – making that feature irrelevant to you.

4 With the widespread availability of information both on the internet but also through professional organizations, can you locate a user of the software you are considering, not provided as a reference, and find out their opinions?

5 When talking to a user of the software, ask hard questions! What do they wish could be different about the software…something it will not do but they wish it could? Are they happy with the tech support? What about any customizations, and how did they go? Finally, ask about budgets – did implementation cost what they projected and has the cost of maintaining the plan met expectations?

6 Is it possible to find someone who decided against a certain software... whether they actually purchased it and had to abandon it, or just opted to buy elsewhere after their evaluation. What was the problem?

7 Is the software company you are considering financially strong, with a track record? Do they have customers similar in size, and with similar regulatory requirements, to your own?

The Big Picture: Features and Benefits You Need to Consider

FUNCTIONAL CONSIDERATIONS

The next sections of this article will touch on feature considerations. A more complete list of options, as well as detailed descriptions, is available in the Spotlight charts and in links provided in the charts.

EXISTING DATA SOURCES

Getting the various business records into the BCM software is critical dur-

CONTINUED ON PAGE 28

CONTINUED FROM PAGE 27

ing rollout. In addition to a list of applications you will need to access, it would help during the evaluation to have samples of the data that the application stores to compare with the BCM software's database. Will this be a manual process and if so, how many hours will this require? Are there APIs already available from the BCM software vendor to access the applications, or will custom programming be required? And if the latter, can you get firm costs for this work?

POWERFUL. COMPREHENSIVE. EASY. PICK ANY TWO?

This author frankly laments the day Microsoft decided to make Word into a program that can do everything under the sun...don't need it. As you look through a long list of features available, will they really help you? And while they might be nice to have, are you set up to create the inputs and maintain the data necessary? It all takes time. Thus it may serve you to look through the feature sets and prioritize those that would have the most impact on your program. Then evaluate the ease of use for those features and from that derive the effort (time and money) required to implement those. This will undoubtedly be an iterative process requiring input from others on your team, and probably a number of Q&A sessions with vendors. From this process, a list of Must Have's and Really Want's will help narrow your selection, and your likely cost for the program.

SECURITY? AVAILABILITY?

Who will be using the software, where will they be, and on what device? Your company's security requirements may limit some of your choices here. But if remote hosting or SaaS is an option, what security and backup will be provided by your vendor? Many companies were surprised during Sandy when backup locations, too close to the primary office, were impacted by a regional event and unavailable when needed most. What level of redundancy do you consider sufficient, and how can you verify the claims? Are third-party audits being done and are those available for review?

CLEAN DASHBOARD?

During a critical incident, focusing on the critical issues is essential. Given the varied and complex pieces that will be managed during an event, is it possible to get the display or dashboard that YOU want? Can you customize the display of information for the software or will this require vendor programming? What about on-the-fly changes that might be required for unusual incidents…can reporting be adjusted easily? What level of training will be required of users to achieve these capabilities?

COSTS, JUSTIFICATION AND ROI

Be sure and compare options by getting total cost of ownership of each software package, including not only the software but also the initial process

of inputting data, training, and annual upkeep. Can the vendor help you assess not only the software costs, but the costs they expect your company will incur at each step along the way for employee labor or other software modifications? If a DIY program is considered an option against which you are comparing BCM software, have you factored in updates and reporting?

In addition to these specific and measureable (direct) costs, there are other factors which, though difficult to assess, could dwarf these direct costs. Would a software package likely speed recovery or offer other savings in the event of a crisis and can those be included in the ROI? What level of support is offered during rollout? What will the cost be for future support?

UPGRADES?

While it is assumed upgrades during a year which includes maintenance will be included, what about additional changes to any customizations done? How will changes to custom APIs be handled? What about upgrades on the other side…when your company's other applications are upgraded, how will the availability of critical data be affected?

The Best Information is Yet to Come

The BCM Software matrix and comparison in the next 8 pages outlines 14 major categories with 168 criteria. Good news -- the 168 criteria can guide your RFP process or serve as questions for your vendor interview.

We trust the BCM Spotlight will help your organization decrease risk and increase resilience!

FOOTNOTES

[1] Does My Company Need Business Continuity Software? Stieven Weidner, CSO Online.

http://www.csoonline.com/article/2131090/emergency-preparedness/does-my-company-need-business-continuity-software-.html

[2] Calculating the True Costs of Business Continuity Management Plans, 6 Deep-Dive Considerations for Comparing BCM Software Platforms

http://www.sungardas.com/Documents/business-continuity-software-considerations-SFW-EBO-015.pdf

FURTHER READING ON BCM SOFTWARE

Tips from Industry Veteran Paul Kirvan

Kirvan says, "Early disaster recovery planning software came in several forms: fill-in-the-blank templates, checklists or automated systems using a common database structure. But many of these templates and checklists provided little guidance and were difficult to use. Today the content and capabilities of disaster recovery plan development tools have been significantly enhanced. Specialized products designed for complex activities like business impact analyses are also available. Some products boast compliance with industry standards".

From Paul's blog at TechTarget, you can access the following:

- Learn the pros and cons of using business continuity software and how to integrate it
- Tips for implementing business continuity software
- Integrating the software into business continuity management operations

2016 BCM SOFTWARE FEATURES MATRIX

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
CATEGORY 1 General Features				
Which features are included in the solution?				
Includes Program Governance				
Includes Business Impact Analysis				
Includes Risk Assessment				
Includes Plan Development				
Includes Exercising / Testing				
Includes Automated Metrics & Reporting				
Includes Crisis/Incident Management				
Includes Emergency Notification				
Hosting				
Provides a SaaS solution				
Provides a locally installed solution with option to install software behind client firewall				
Provides a browser based solution (no local client software installation requirement)				
Supports prominent browsers: IE, Chrome, Firefox, Safari				
Offers dedicated database				
Offers shared database				
Standards Compliance: Support for industry standard practices in BC, DR, IT & Incident management				
Supports ISO 22301				
Supports NFPA 1600				
Supports FFIEC				
Supports other standards				
Includes evaluation of resilience program maturity				
Includes history logs				
Access & Integration				
Able to access tool from computer				
Able to access tool from tablet				
Able to access tool fom mobile phone				
Software is mobile optimized				
Provides access to mobile app for offline viewing				

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
Offers multi-user application ("unlimited" users with concurrent access)	✓	✓	✓	✓
Offers API access	✓	✓	✓	✓
Able to integrate with 3rd party tools and applications	✓	✓	✓	✓
Allows Single Sign On (SSO)	✓	✓	✓	✓
Import and Export				
Able to import and export data from external sources such as a Microsoft Excel spreadsheet	✓	✓	✓	✓
Able to import data from unlimited number of external file types	✓	✓	✓	✓
Allows access to complete data table schema	✓	✓	✓	✓
Able to easily export any data from the tool	✓	✓	✓	✓
Can import data dynamically from other sources, such as databases	✓	✓	✓	✓
Templates				
Provides templates for policy	✓	✓	✓	✓
Provides templates for BIA	✓	✓	✓	✓
Provides templates for planning	✓	✓	✓	✓
Provides templates for exercising	✓	✓	✓	✓
Able to create new templates, from scratch	✓	✓	✓	✓
Able to duplicate templates	✓	✓	✓	✓
General Features				
Provides easy navigation throughout the tool	✓	✓	✓	✓
Includes multi-language capability	✓	✓	✓	✓
Provides customizable user roles and groups	✓	✓	✓	✓
Allows clients to view and change data table schemas	✓	✓	✓	✓
Provides charts and graphs	✓	✓	✓	✓

CONTINUED ON NEXT PAGE

Click below to learn more about General Features

CATALYST | FAIRCHILDAPP | RPX | SUSTAINABLE

CONTINUED FROM PAGE 31

CATALYST	FAIRCHILDAPP	RPX	SUSTAINABLE
by Avalution Consulting	by Fairchild Consulting	by RecoveryPlanner	by Virtual Corporation

CATEGORY 2 Security such as encryption, login and permissions

Provides lock out feature after a failed number of login attempts

Provides role-based security

Supports encrypted passwords

Includes "Forgot my Password" feature

Allows client to define password strength parameters

Allows data encryption in transit

Allows data encryption in at rest

Click below to learn more about **Security**

Catalyst | FairchildApp | RPX | Sustainable Planner

CATEGORY 3 Risk Assessment/Management provides area to document threats maybe preloaded or part of a Business Impact Analysis

Provides list of key threats and vulnerabilities

Provides strategy options for common risks and documents the recovery strategy

Captures and assesses risks related to business and technology operations

Captures and associates risk responses and controls to risks

Sets the stage for developing business continuity strategies and plans

Includes risk register

Provides technology modeling

Includes operational risk assessment

Includes facilities risk assessment

Automatic analytics

Click below to learn more about **Risk Assessment/Management**

Catalyst | FairchildApp | RPX | Sustainable Planner

CATEGORY 4 Business Impact Analysis that supports survey and/or interview approach

Includes customizable BIA template

Captures critical business functions

Captures recovery time objectives (RTO)

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
Captures recovery point objectives (RPO)	✓	✓	✓	✓
Provides BIA summary report	✓	✓	✓	✓
Includes visual mapping of dependencies	✓	✓	✓	✓
Allows unlimited imports of data from external sources for use in reports and workflow	✓	✓	✓	✓
Includes Gap Analysis	✓	✓	✓	✓
Provides what-if scenarios for impact analysis	✓	✓	✓	✓
Provides RTO/RPO Analysis	✓	✓	✓	✓
Includes multiple impact calculation types	✓	✓	✓	✓
Captures application, facility, supplier, department dependencies	✓	✓	✓	✓
Captures recovery staffing and resource requirements	✓	✓	✓	✓
Provides suggested strategy options for common risks and documents the recovery strategy	✓	✓	✓	✓
Able to set update and approval frequencies that automatically notify BIA owner of the task, and again when completed or overdue	✓	✓	✓	✓
Provides audit trail of changes	✓	✓	✓	✓

Learn more about Business Impact Assessment

CATALYST · FairchildApp · RPX · Sustainable Planner

Plan Creation (Customizable, supports plans and goals of organizational & Maintenance (covers revision history and testing)

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
Able to customize plan templates	✓	✓	✓	✓
Enables the creation of Business Recovery Plans	✓	✓	✓	✓
Enables the creation of Crisis Management Plans	✓	✓	✓	✓
Enables the creation of Crisis Communications Plans	✓	✓	✓	✓
Enables the creation of IT DR Application Recovery Plans	✓	✓	✓	✓
Enables the creation of ITDR Infrastructure Plans	✓	✓	✓	✓
Utilizes data from the BIA and risk assessment	✓	✓	✓	✓
Allows web-based plan development	✓	✓	✓	✓
Able to easily create and edit plans	✓	✓	✓	✓
Captures restoration and recovery information such as processes and checklists based on resource loss type	✓	✓	✓	✓

CONTINUED ON NEXT PAGE

CONTINUED FROM PAGE 33

PLAN CREATION CONTINUED

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
Captures recovery needs and requirements, such as equipment, supplies and vital records	✓	✓	✓	✓
Includes single button plan generation	✓	✓	✓	✓
Documents audit trail of changes	✓	✓	✓	✓
Able to attach multiple file types to plans	✓	✓	✓	✓
Able to test changes to templates, pages, fields before elevating to "active"	✓	✓	✓	✓
Able to set update and approval frequencies that automatically notify plan owner of the task, and admin when completed or overdue	✓	✓	✓	✓

Click below to learn more about **Plan Creation**

Catalyst · FairchildApp · RPX · Sustainable Planner

CATEGORY 6 Incident/Crisis Management & Recovery Site

Provides access to contact and vendor lists	✓	✓	✓	✓
Captures notification/escalation criteria	✓	✓	✓	✓
Enables incident response	✓	✓	✓	✓
Utilizes NIMS-ICS structure for incident management	✓	✓	✓	✓
Able to customize structure and terminology for Incident Management	✓	✓	✓	✓
Includes recovery site layout plan	✓	✓	✓	✓
Includes dynamic incident management	✓	✓	✓	✓
Includes dynamic questions setting/reviews	✓	✓	✓	✓
Includes workflow management with email alerts and reporting	✓	✓	✓	✓
Includes Situation Status dashboards to track impacts, status, assignments	✓	✓	✓	✓
Able to upload multiple file types to event tracking	✓	✓	✓	✓
Provides an online portal to collaborate and manage a disruption	✓	✓	✓	✓
Allows plans to be activated and become working documents for response and recovery personnel	✓	✓	✓	✓
Able to submit issues and questions through an activated plan to raise and document an issue	✓	✓	✓	✓

Click below to learn more about **Incident/Crisis Management & Recovery Site**

Catalyst · FairchildApp · RPX · Sustainable Planner

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
CATEGORY 7 Emergency/Mass Notification				
Able to notify people via phone, email or text message based on various notification lists	✓	✓	✓	
Allows integration with third-party vendors		✓	✓	✓
Includes Emergency Notification that is built-in to the tool	✓		✓	
Can send messages to individual contacts, groups of contacts, or teams from recovery plans	✓	✓	✓	✓
Can record custom voice messages instead of text to speech	✓		✓	
Can send polls and surveys and then view summarized results	✓	✓		✓
Includes pricing model overview	✓	✓	✓	
Click below to learn more about **Emergency/Mass Notification**				
Catalyst · FairchildApp · RPX · Sustainable Planner				
CATEGORY 8 Exercises				
Provides interactive exercise templates	✓	✓	✓	✓
Supports exercise planning - type, objective, participants	✓	✓	✓	✓
Documents results	✓	✓	✓	✓
Documents and assigns action items	✓	✓	✓	✓
Click below to learn more about **Exercises**				
Catalyst · FairchildApp · RPX · Sustainable Planner				
CATEGORY 9 Reporting & Approvals				
Includes multiple formats for output	✓	✓	✓	✓
Able to generate reports quickly	✓	✓	✓	✓
Includes preformatted reports	✓	✓	✓	✓
Allows custom reports to be built	✓	✓	✓	✓
Includes data collection reporting	✓	✓	✓	✓
Allows GIS and Latitude/Longitube mapping	✓	✓	✓	✓
Provides numerous types of charts and graphs	✓	✓	✓	✓
Allows multiple document types to be incorporated in reports	✓	✓	✓	✓
Organize attachments to appear in appropriate section of reports	✓	✓	✓	✓

CONTINUED ON NEXT PAGE

CONTINUED FROM PAGE 35

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation

REPORTING & APPROVALS CONTINUED

Provides automated update and approval reminder process (policy, bias, plans)

Provides automatic program metrics based off of the data entered into the system

Provides automatic gap analysis

Able to visually map directional relationships and dependencies across the organization

Click below to learn more about **Reporting & Approvals**

Catalyst FairchildApp RPX Sustainable Planner

CATEGORY 10 Ease of Use

Includes user friendly interface

Includes filters & search

Allows personal filters

Includes drag & drop feature

Includes single page user guide for simplified user experience

Provides customized dashboard (user-specific)

Provides help text throughout the tool to explain what data is being requested

Includes fully integrated data (data entered in one part of the system is available through the tool – reduced duplication and contradictory data)

Click below to learn more about **Ease of Use**

Catalyst FairchildApp RPX Sustainable Planner

CATEGORY 11 Flexibility & Scalability

Scales to fit the user (different packages are available)

Able to change or add terminology

Allows screen customization

Able to edit folder or tag structure

Able to change/delete fields, questions, pages

Able to "clone" templates with or without prepopulated data

Able to add numerous question types

Able to add custom fields

	CATALYST by Avalution Consulting	FAIRCHILDAPP by Fairchild Consulting	RPX by RecoveryPlanner	SUSTAINABLE by Virtual Corporation
Able to customize default fields	✓	✓	✓	✓
Able to re-order or hide fields	✓	✓	✓	✓
Able to customize help text	✓	✓	✓	✓

Click below to learn more about **Flexibiity & Scalability**

Catalyst FairchildApp RPX Sustainable Planner

CATEGORY 12 Education & Training

Offers on-site training at customer's location	✓	✓	✓	✓
Provides user group meetings	✓	✓	✓	✓
Provides online training	✓	✓	✓	✓
Provides help center	✓	✓	✓	✓
Provides help text throughout tool	✓	✓	✓	✓
Allows Admins to customize the help text throughout tool	✓	✓	✓	✓
Training duration for end users is less than 1 hour	✓	✓	✓	✓
Training duration for end users is 1 - 4 hours	✓	✓	✓	✓
Training duration for end users is more than 8 hours	✓	✓	✓	✓
Training for administrators is less than 8 hours	✓	✓	✓	✓
Training for administrators is 16 - 24 hours	✓	✓	✓	✓
Training for administrators is more than 24 hours	✓	✓	✓	✓
Is there a fee for standard training?	✓	✓	✓	✓

Click below to learn more about **Education & Training**

Catalyst FairchildApp RPX Sustainable Planner

CATEGORY 13 Availability

Includes 99.9 uptime guarantee	✓	✓	✓	✓
Provides redundant system architecture of hosted data centers	✓	✓	✓	✓
Allows daily backup of data	✓	✓	✓	✓

Click below to learn more about **Availability**

Catalyst FairchildApp RPX Sustainable Planner

CATEGORY 14 Other Features

Offers a free trial	✓	✓	✓	✓

Click below to learn more about **Other Features**

Catalyst FairchildApp RPX Sustainable Planner

THANK YOU TO OUR SPONSORS

catalyst

DISASTER RECOVERY JOURNAL

EMERGENCY LIFELINE
Consumer & Corporate Emergency Products

fairchild.app

Mail-Gard
A Division of IWCO Direct

RECOVERY PLANNER .COM

RSA

virtual corporation