Continuity of Operations: The Big Picture

MARKET TRENDS REPORT

govloop RSA FOUR POINTS TECHNOLOGY BlackBerry

Introduction

Government agencies thrust into an alternate universe by the COVID-19 pandemic are thinking more about their continuity of operations plans (COOP) – or lack of them. The particular fallout from the pandemic – including widespread telework, closed offices and virtual meetings and confabs – underscores not just the need to prepare for infectious diseases, but for other disasters. Agencies may not need to expect the unexpected, but they need to be prepared to react swiftly to it. They need holistic COOP plans that position them to maintain continuity during any emergency – what's known as an "all hazards" approach.

A comprehensive COOP plan will allow agencies to be resilient rather than reactive. It takes into account partnerships, people and assets – in some cases, worldwide – along with the IT systems supporting them and the emergency communications tools necessary to react quickly and capably. It can ensure that agencies can continue performing their missions despite disruptions from all the physical and cybersecurity emergencies that can occur in a dynamic world.

Federal, state and local government agencies need to go beyond piecemeal approaches to specific threats and address a wide range of risks while keeping up-to-date with the threat landscape and all overarching regulations.

To learn more about how agencies can plan for a swift response to any crisis, GovLoop teamed up with RSA Archer, BlackBerry AtHoc and Four Points, which have extensive experience in emergency planning, communications and COOP.

BY THE NUMBERS
Evolving COOP Strategies

"Continuity planning is simply the good business practice of ensuring the execution of essential functions and a fundamental duty of public and private entities responsible to their stakeholders."

Source: Federal Emergency Management Agency (FEMA) Continuity of Operations Overview

What kind of functionality is essential for your agency's COOP program?

67% Quickly deploying response plans

61% Centrally managing COOP & disaster recovery

52% Ability to test plans

50% Access business continuity

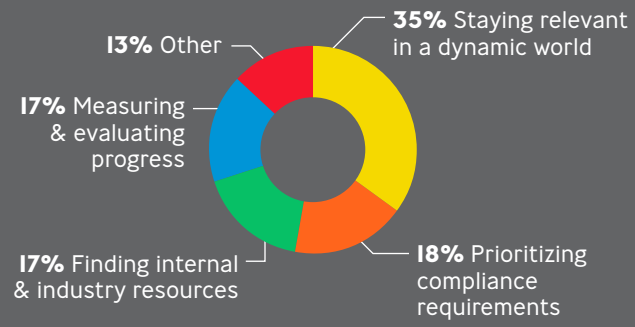
47% Tracking in real time

47% Reporting on vulnerabilities

38% Ability to integrate with mobile devices

34% Perform business impact analysis

What is your top challenge in creating a COOP strategy?



Do you regularly test your COOP plan?

Source: Four Points/RSA

34%

of local governments have no COOP plan

Source: ICMA

46.9%

of local governments have a standalone disaster recovery plan

Source: International City/County Management Association (ICMA)

THE CHALLENGE
Dealing With the Unexpected

Agencies face a series of challenges in establishing COOP plans, starting with the array of threats and potential emergencies that can crop up. They can result from hurricanes, terrorist attacks, government shutdowns, cybersecurity incidents or pandemics.

COVID-19, however, does offer some lessons on the importance of COOP, particularly because its impact and the response it has triggered haven't been seen in modern times.

Pandemic threats have been on the radar of health and intelligence agencies for years, but they weren't a front-of-mind possibility for most government officials or employees. The response the pandemic necessitated was unexpected. It had a huge impact on agencies' full range of operations and entire workforces, and left them with an uncertain timeline for when things might return to normal. In fact, post-COVID "normal" might not be what it was, as some changes could become permanent.

"I think organizations are using their COOP plans," said Patrick Potter, Digital Risk Strategist for RSA. "What was set up as a workaround in an emergency is becoming a longer-term operational procedure in some cases. They're adjusting on the fly. It's an interesting phenomenon."

Meanwhile, agencies face other challenges when developing COOP plans, some of which align with the COVID-19 response. An RSA and Four Points Technology survey of public-sector professionals – taken several years ago but still applicable – found that "staying relevant in a dynamic world" was the top challenge in creating a COOP strategy, cited by 35% of respondents, followed by issues involving compliance requirements (18%), resources (17%) and measuring progress (also 17%). A lack of resources was also the most commonly cited reason (43%) for agencies not testing their COOP plans.

Many agencies are now wondering, "What's the new normal going to look like post-pandemic, and how should COOP plans change while most workforces work from home?" said Jae Kim, Director of Product Management at BlackBerry AtHoc. But the next crisis that threatens critical operations – and the response to it – may also be unexpected.

THE SOLUTION: FOCUS ON RESILIENCE

The answer lies not in being able to predict the next crisis but in being prepared for whatever it may be. And that calls for a COOP plan that addresses a complex threat environment, covering three primary areas:

Physical security, which can be threatened by natural or manmade events that can cause flooding, power outages or structural damage that may close buildings, require telecommuting or working from alternate locations

Cybersecurity attacks, which can come from outside or inside an organization, can disrupt services and freeze access to government systems

Policy and compliance risks that can result from employees inadvertently or deliberately failing to follow directives such as the Federal Acquisition Regulation (FAR), Federal Information Systems Management Act (FISMA) or other federal requirements, many of which have counterparts in state and local governments

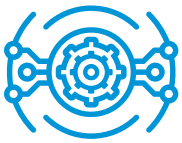
An effective COOP plan accounts for all potential threats, coordinates a COOP response with disaster recovery and crisis management teams and is aligned with policy and compliance mandates.

Technology is essential to every part of the plan. The plan should utilize automated processes and centralized management to swiftly identify and categorize events, determine response and assign and coordinate response teams. It should also make use of unified notification and crisis communications systems that accommodate multiple formats and mobile devices.

And the plan should be designed for continuous improvement, evolving alongside technology to stay current with dynamic threats.

BEST PRACTICES

Key Components of COOP Plans



Automation.

Automated tools are important to preparation and response. Typically, contingency planning teams are small and may be tasked with developing scores of plans for the different moving parts of an organization, Potter said. Part of that process needs to be automated, particularly concerning testing and updating plans, as well as developing new ones for other units. Risk assessments and providing documentation for transactional authorizations are also beneficial. "It doesn't eliminate the human element," Potter said, but it performs work team members don't have time for, and gives them the information they need to make quick, data-driven decisions."

Policy Alignment.

The bottom line for a COOP plan is that it allows an agency to perform its mission under any circumstances, so its policy statement, procedures, testing and business impact analyses of potential disruptions should map to those priorities. It also should adhere to security guidance such as the National Institute of Standards and Technology's (NIST) SP 800-34 and the Department of Homeland Security's (DHS) National Incident Management System (NIMS) framework. Agencies need a top-down approach, starting with leadership, to make effective COOP part of their culture. "You have to start before the COOP plan to build in those resilient steps," Potter said.

Centralized Management.

Coordination is essential to a swift response in any emergency. Centralizing oversight of both disaster recovery and COOP operations ensures consistency throughout an agency while allowing for greater collaboration.

Partnerships.

Response requires coordination not just within an agency but with third parties. They could be other federal or state agencies, but they also could include fire departments and other first responders, medical providers and other outside organizations, Kim said. Agencies need to know the resources they want to provide and what types of organizations they'll work with. Emergency communications systems are an important factor as well. Integrated, IP-enabled messaging and alert systems with automated, web and remote activation capabilities can ensure communications both within and outside the agency, giving responders quick access to recovery strategies and operational procedures.

Continuous Improvement.

There's no such thing as a final COOP plan. In a dynamic threat environment, plans need to adapt to changes in the organization, and be tested and updated regularly. The process for improving a plan must be built into it, which requires commitment from the agency. It will ensure that a plan accounts for recent and emerging threats.

CASE STUDY
The Benefits of COOP

Agencies without comprehensive COOP plans share some disadvantages. They lack visibility into the status of their business continuity capabilities. If they have recovery documentation, it tends to be static and rendered in multiple formats. And they lack communication across the teams responsible for business continuity, disaster recovery and crisis management. With a COOP plan in place, those teams have channels for communication and coordination. What's more, the plan is aligned with an agency's priorities and mission and is designed for continual testing and updates.

An effective COOP plan that's supported throughout an enterprise also can improve operations on a daily, non-crisis basis by reinforcing the commitment to an agency's mission and its employees and partners. For example, the Red Cross recognized the need several years ago for a crisis communications system to help it better respond to emergencies – no two of which are ever alike.

The partnership it developed with BlackBerry AtHoc not only met the Red Cross' needs for assessing damage, working with other response organizations and the public, and helping communities get back on their feet, but it also has become a regular feature of its day-to-day operations. Among other things, the Red Cross uses it with arrival instructions for responders deployed to disaster relief operations and in conducting workforce care surveys with volunteers.

"We use BlackBerry AtHoc for every single deployment, and we do at least 20,000 deployments a year," said Brad Kieserman, the Red Cross' Vice President of Disaster Operations and Logistics.

HOW RSA, BLACKBERRY ATHOC AND FOUR POINTS CAN HELP

RSA, a security, risk and compliance management solutions provider, offers holistic COOP through solutions such as RSA Archer Contingency Planning, which centralizes control of COOP, disaster recovery and crisis management in a single web-based management system. The solution automates the planning, update process and testing, and is designed to comply with NIST security guidance and other federal regulations. The company's proactive approach to COOP emphasizes resilience, ensuring that an organization's response to a crisis includes continuity of operations with established recovery times.

BlackBerry AtHoc provides a software-based crisis communications platform that can operate on premises or in the company's FedRAMP-approved cloud, delivering instant communications via multiple channels and formats. It allows agencies to track messages, accept real-time feedback and quickly account for the whereabouts and condition of staff members during an emergency. AtHoc Cloud Services offers flexible, customizable mass communication tools that comply with federal security and privacy regulations and can integrate with on-premises systems.

Four Points Technology is a CVE-verified Service Disabled Veteran Owned Small Business (SDVOSB) delivering IT solutions to our government customers around the world.

Learn more at www.4points.com.

Conclusion

Disruptions to government operations can come anytime, and from any source. It may be impossible to predict the next crisis, but agencies can prepare for it with a holistic, integrated COOP plan that focuses on maintaining operations and critical functions, establishing solid lines of communication and maintaining compliance with security, privacy and other regulations.

Planning to maintain continuity in the face of disruptions needs to be part of an agency's culture because, as the COVID-19 pandemic has shown, the repercussions can become a way of life throughout an organization. An automated, centrally managed COOP solution can ensure that agencies react quickly not just to mitigate an attack or disruption, but to ensure that mission-critical work can continue, whether the cause is physical or cyber, sudden or ongoing. Agencies need a proactive, resilient COOP strategy that is as dynamic as the constantly morphing threat landscape they face every day.

ABOUT RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

For more information, go to rsa.com/publicsector.

ABOUT BLACKBERRY ATHOC

BlackBerry® AtHoc is a networked crisis communication system trusted by over 2,000 organizations globally to unify their crisis communications. It delivers comprehensive 2-way crisis communication services for personnel and provides leaders with the information they need to make critical safety decisions.

BlackBerry provides intelligent security software and services to enterprises and governments around the world. The company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems.

For more information, visit BlackBerry.com and follow @BlackBerry

ABOUT FOUR POINTS TECHNOLOGY

Four Points Technology is a CVE verified Service Disabled Veteran Owned Small Business (SDVOSB) dedicated to providing IT Products and Professional Services to the Federal Government. Four Points Technology offers solutions that support a wide variety of business initiatives specifically suited for Government organizations. Four Points Technology supplies services and products meeting numerous Cybersecurity, DataCenter, Mobility, and MedicalIT challenges within the Federal customer market. As an RSA Platinum partner, Four Points Technology evaluates customer challenges and helps to bring solutions that solve those problems cost effectively and with exceptional service. Learn more: 4points.com.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop