Bouncing Back: How Your Agency Can Handle Disruption and Embrace Resilience

govloop

Table of Contents

3 Executive Summary

4 At a Glance: Surveying Public Sector Resilience

6 6 Facts About Federal Resilience

8 6 Facts About State and Local Resilience

11 Making Your Agency's Networks Resilient

12 Resilience Revealed: 4 Areas Worth Considering

13 Learning From Cybersecurity Incidents

17 Strengthening Your Agency's Web Apps

18 Tricks for Workforce Resilience

21 Procuring Your Agency's Secure Digital Displays

22 Refine Workflows for Resilience

25 3 Ways to Secure Your Agency's IT Environment

26 Harden Your Agency With Technology

29 Making Your Identity and Access Management Resilient

30 How Resilience Makes the Defense Logistics Agency Ready for Anything

33 Managing Your Agency's Machine Identities

34 How Connecticut Reinforced Its Resilience

37 How Hybrid Clouds Can Cover Your Agency's Resilience

38 Best Practices for Resilience

41 Approaching Your Agency's Security Holistically

42 Conclusion

Tech Trends Covered in This Guide

- Continuity of Operations (COOP)
- Cloud Computing
- Disaster Response and Recovery
- Preparedness and Risk Management
- Remote Work
- Zero-Trust Cybersecurity

Executive Summary

Any time an agency's operations are disrupted, the public may lose access to valuable – even life-saving – products and services such as food stamps or unemployment benefits. With such high stakes, agencies at every level cannot afford many interruptions.

But recent years have demonstrated that no agency can permanently avoid setbacks. From the COVID-19 pandemic to natural disasters, the list of organizational and personal emergencies employees may face keeps growing. Whatever the crisis, toughness seems like a more important quality for governments than ever.

Enter resilience. Individually or collectively, resilience is the ability to respond to, recover from and continuously operate during disturbances. Whether agencies are encountering cyberattacks, terrorism or other challenges, resilience can mean the difference between mission success and failure. Resilient agencies not only rebound from misfortune faster than their peers, they also return with fewer problems. Even better, resilience can prepare the public sector for any problem, ensuring agencies focus on serving constituents rather than putting out fires.

Yet resilience is not a quality that agencies or individuals can obtain overnight. Resilience requires effort and dedication; it is not an attribute that agencies acquire once and then forget. Federal, state or local, resilient agencies continuously maintain a culture of preparedness built on flexible and strong people, processes and technologies.

If your agency needs to fortify its resilience, this guide can launch its journey toward lasting durability. The anecdotes, wisdom and best practices we share can keep your agency's lights on during internal and external surprises.

Initially, we recap the latest data, news, statistics and soundbites to understand the public sector's overall resilience.

Next, we highlight five areas of resilience worth considering: the pitfalls making resilience necessary, cybersecurity and the people, processes and technologies facilitating resilience.

Then, we share lessons that top federal, state and local thought leaders have learned that can assist your agency's resilience efforts.

Lastly, we explore best practices for maximizing your agency's resilience and constantly staying prepared for the worst.

Agencies cannot predict the future, but that does not mean their employees should enter the future unprepared. Let us dive into ways you and your team can stay prepared for whatever shocks are around the bend for your agency.

At a Glance: Surveying Public-Sector Resilience

7 Resilience Terms to Know

The following terms are critical for understanding and discussing resilience across the public sector.

Continuity of operations (COOP): COOP plans identify an agency's essential functions and then describe the people and resources critical to maintaining those activities. Overall, COOP frameworks detail the processes an agency needs to protect and preserve its assets, operations and personnel during any circumstances. Examples of COOP considerations include determining safekeeping for vital records and databases and deciding how to delegate authority during emergencies.

Disaster response and recovery: Disaster response and recovery plans differ from COOP strategies as they dictate how agencies act before, during and after catastrophes. Disaster response determines how an agency prepares for situations like severe weather; it also defines how that agency reacts during and after such incidents. Disaster recovery, meanwhile, centers on recuperating from these troubles. Together, disaster response and recovery provide agencies with a map for navigating difficult times.

Federal Employee Viewpoint Survey (FEVS): Conducted annually by the Office of Personnel Management (OPM), FEVS measures the engagement of all federal employees. OPM gauges the internal atmosphere of each federal agency, polling employees about how satisfied they are with their office's leadership, policies and programs. Each year, FEVS also probe the federal government's overall resilience.

Individual resilience: Individual resilience refers to the physical, mental and emotional routines each person establishes to feel resilient. For the individual, these practices help them overcome internal and external stress more easily. For agencies, individual resilience can collectively create happier and more flexible workforces.

Preparedness: Preparedness covers the research necessary to take precautions against potential hazards like fires. Typically, preparedness mixes physical preparations — say, emergency supplies — and training to ready agencies for surprises. Ultimately, preparedness assists agencies with accomplishing their goals while avoiding and mitigating negative outcomes such as financial damage.

Risk management: Risk management centers on pinpointing the effect of uncertainty on an agency's goals and then analyzing and prioritizing these potential roadblocks accordingly. At agencies, risk management can monitor misfortunes and minimize and control how likely they are to occur and decrease the impact. Additionally, risk management is about maximizing the opportunities agencies can realize.

Zero-trust cybersecurity: Zero-trust cybersecurity hinges on automatically distrusting all devices, users and other entities on an IT network. Whether these entities are inside or outside the network perimeter, agencies let them access their resources only after verifying their identities. Zero-trust cybersecurity also enables agencies to continuously monitor their IT systems and assets.

6 Facts About Federal Resilience

Federal Network and Critical Infrastructure Security Statistics

The Homeland Security Department (DHS) identifies and manages America's most critical national cybersecurity risks alongside key stakeholders.

More than $1.1 billion

the projected amount of funding for DHS's cybersecurity efforts in fiscal 2021.

Source: The White House

More than 6,500

the projected amount of DHS-led network risk assessments in fiscal 2021, including assessments of state and local electoral systems.

Source: The White House

Federal IT Spending

IT modernization is a component of practicing resilience, so the amount of money federal agencies spends annually on this technology matters.

$90.9 billion

the projected amount of total federal IT spending in fiscal 2021, up from **$65.9 billion** in fiscal 2020.

Source: Federal IT Dashboard

$23.9 billion

the projected amount of the above total that will go toward major IT investments, vs. **$67 billion** that will go toward non-major IT investments.

Source: Federal IT Dashboard

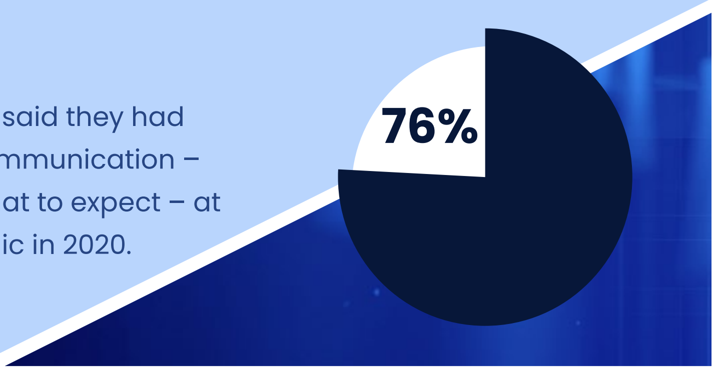
Federal Resilience Amid COVID-19

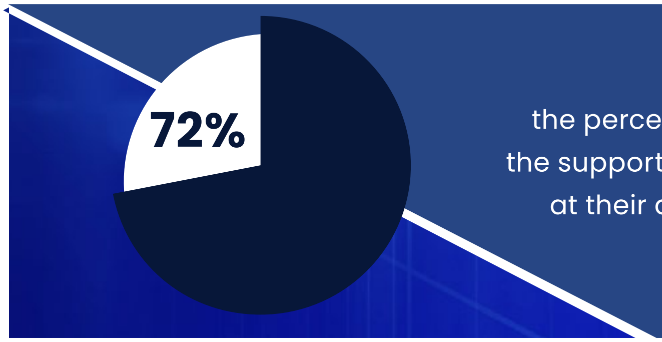
In April 2021, OPM released the results of its 2020 FEVS, which assessed the COVID-19 pandemic's impact on federal agencies and their employees.

76%

the percentage of federal employees who said they had the support they needed for consistent communication – on topics like organizational status and what to expect – at their agency during the COVID-19 pandemic in 2020.

Source: OPM





72%

the percentage of federal employees who said they had the support they needed for expanded collaboration tools at their agency during the COVID-19 pandemic in 2020.

Source: OPM

6 Facts About State and Local Resilience

COVID-19 and State Governments

The COVID-19 pandemic put state agencies under unprecedented strain, particularly with IT, due to the expansion of remote work to promote social distancing.

No. 1

the rank state chief information officers (CIOs) gave application development when asked to rate the top five competencies COVID-19 impacted in 2021.

Source: National Association of State Chief Information Officers (NASCIO)

No. 1

the rank state CIOs placed expanded work-from-home and remote work options when asked which business processes, practices or investments they believed would change post-COVID-19.

Source: NASCIO

State Cybersecurity and IT Modernization Rankings

The Internet Association's (IA) State, Local, Tribal, and Territorial Information Technology Advancing Reform Achievements scorecard ranks states' cybersecurity preparedness and IT modernization plans, which both factor into resilience.

0

the number of states that achieved "exceptional" or "excellent" ratings in either cybersecurity preparedness or IT modernization plans in 2020. The scorecard's other rankings are "very good," "good," "baseline," "getting started" and "needs help."

Source: IA

3

the number of states that scored "very good" on cybersecurity preparedness and IT modernization plans in 2020.

Source: IA

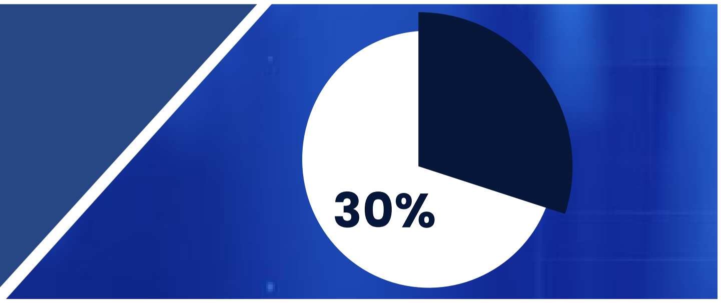
High-Risk Counties

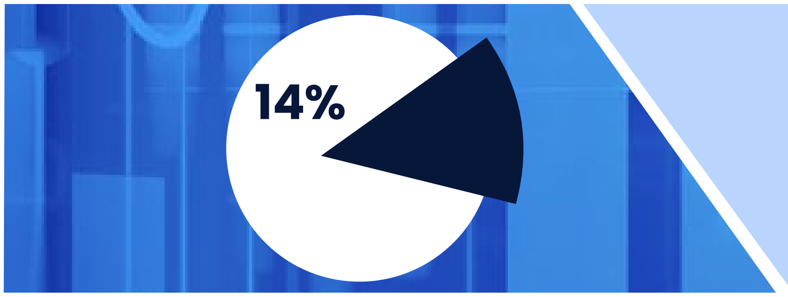
The Census Bureau's Community Resilience Estimates (CREs) measure a community's ability to endure, respond to and recover from the impact of disasters. Diabetes, heart disease and physical crowding are some of the high-risk factors populations may have.

30%

of rural communities were high-risk nationwide in June 2020.

Source: Census





14%

of urban communities were high-risk nationwide in June 2020.

Source: Census

Simple.
Resilient.
Secure.

Industry Perspective

Making Your Agency's Networks Resilient

An interview with Robert Schumann, Federal Solutions Architect, Juniper Networks

Remote work's growing prevalence means government networks need to connect larger numbers of people across wider distances. Despite this, many agencies are discovering that the scope of their missions exceeds their networks' capacity. No matter how far they reach, many agencies' networks do not fully meet the needs of employees or the public.

The situation only grows more complicated when resilience enters the picture. From the federal level down, agencies need networks that work consistently, reliably and securely. Without these attributes, networks may experience service disruptions or even jeopardize sensitive constituent data.

Fortunately, software-defined, wide-area networking (SD-WAN) can put agencies' missions at the forefront of their networking capabilities. WAN enables connectivity across vast distances, while SD-WAN simplifies management and removes hardware dependencies. Using SD-WAN, agencies can function more efficiently with fewer networking interruptions, allowing teams to focus on innovation instead of maintenance.

"It puts the mission first," Robert Schumann, Federal Solutions Architect at Juniper Networks, a networking solutions provider, said of SD-WAN. "Agencies' networks can now understand context about users and applications and how best to connect them across any type of transport."

Schumann discussed three ways that SD-WAN strengthens agencies' networking quality, resilience and security.

1. Boost connectivity

By now, most people have experienced poor connectivity issues like choppy video calls. Application and network problems – such as congested network traffic – cause these complications.

"It's frustrating when citizens can't do certain activities due to problems with agencies' networks and applications," Schumann said.

SD-WAN can prevent connectivity issues by intelligently routing sessions to improve application and network performance. The resulting application experience is more stable for both the public and government employees.

2. Increase innovation

Too often, agencies' networks are not reaching their full potential. To innovate, agencies need networks that can launch products and services quickly, securely and affordably.

"You can create networks that are highly dynamic and agile," Schumann said.

For instance, many agencies have traditionally needed significant time and funding to launch new applications. Embracing SD-WAN's flexibility, however, agencies can adopt applications more easily, delivering quality user experiences (UX) in ways and places that were not possible before.

3. Reveal root causes

Whether it is for security or the UX, agencies need strong visibility into their networks. Using emerging technologies like artificial intelligence (AI), agencies can gain fresh insights about topics such as user activity. AI imitates such human cognitive skills as learning to dramatically elevate agencies' understanding of their networks.

"It all comes down to what and why," Schumann said of how AI assists agencies. "Something is slow – that's the what. Next is the why. AI solutions help automatically surface the why and, in many cases, can simply fix the problem instead of manually tasking it to personnel."

Agencies cannot use degraded networks. But by using SD-WAN solutions such as Juniper Networks' Session Smart SD-WAN, agencies can focus their networks on customer satisfaction and mission wins.

Resilience Revealed: 4 Areas Worth Considering

Government resilience anticipates the unknown. From the federal layer down, agencies face nearly limitless obstacles.

Internally, the shocks can range from power outages to abrupt leadership changes. Externally, everything from flooding to violent crime can jolt agencies out of functioning smoothly. With most of the public sector online, the hiccups are no longer merely physical. Nowadays, cybersecurity mishaps can cause as much upheaval at agencies as traditional stumbling blocks.

But anticipating the unknown is not the only quality resilient agencies have. Resilient agencies also have people, processes and technology that strengthen their overall durability. Agility and flexibility link these three categories. Agencies with nimbler employees, tools and workflows are more capable of adapting to unforeseen circumstances.

For instance, resilient employees feel empowered to swiftly address any fiasco, even if it means switching gears on their daily duties. Furthermore, these workers are prepared for the circumstances facing them, having brainstormed and practiced the response and recovery steps they take. Crucially, these people do not believe they are weighed down by leadership, technology or workflows when encountering setbacks.

Subsequently, government resilience hinges on imagination and responsiveness. For starters, agencies that cannot envision stunning moments cannot be ready for them; agencies that cannot react rapidly to speedbumps, meanwhile, need more time to resume operations after a stumble.

Below are four areas of resilience worth considering, with four recent developments from each one containing information agencies should know about this topic.

Resilience Area #1

Learning From Cybersecurity Incidents

Examples of Recent Cyberattacks

When it comes to government calamities, cybersecurity is in a league of its own. First, many agencies are still finding their footing when it comes to protecting their employees and operations online. Second, cybersecurity misfortunes can become uniquely embarrassing for agencies. Beyond the bad publicity or financial damage these disturbances can cause, they can also expose sensitive information about the public. When agencies are trusted to handle constituents' delicate data and fail, the result is potential damage to their relationship.

The reality is that cybersecurity is no longer a concern for just agencies' IT shops. Going forward, cybersecurity will need to be a significant priority for every public-sector employee.

1. No one is permanently safe

In March 2021, the FBI cautioned other federal agencies and private-sector companies that cybercriminals were taking advantage of a vulnerability in a widespread computing product. According to the FBI, the gap in computing giant Microsoft's Exchange system left precious personally identifiable information and research and technology data at risk.

Even worse, the FBI assessed the activity to have potentially come from nation-state actors. Citing past moves by Chinese cyber actors, the FBI noted everything from academic institutions to nongovernmental organizations might be in similar danger. The FBI recommended that possible victims watch their advanced technology, business information and research data.

In the coming years, agencies must assume cyberthreats can penetrate products and services from the world's most recognizable companies.

2. Cyberattacks can cause physical harm

A scare in Oldsmar, Florida, hints at what agencies may see from future cyberattackers. In February 2021, the Pinellas County Sheriff's Office was notified of a cyber intrusion affecting computer systems at Oldsmar's water treatment plant. According to detectives, the plant permits remote access to troubleshoot system issues. In this instance, an intruder twice accessed the plant's system remotely before raising the level of sodium hydroxide in Oldsmar's water. Although an operator quickly reversed course, the alteration could have made Oldsmar's water unsafe if left untreated.

Thankfully, authorities eventually concluded the incident did not endanger the public. Nonetheless, the strange moment suggests cybersecurity may cause unexpected consequences for agencies.

3. Pay attention to alerts

In December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive warning that malicious actors were exploiting a common IT software. CISA urged other federal agencies to immediately disconnect or turn off the tool – which came from SolarWinds, a cybersecurity company — to prevent further harm.

Since then, CISA has confirmed attackers compromised victims' software as early as March 2020. A task force constructed to investigate the incident also determined that the strike hit about 18,000 public—and private—sector SolarWinds customers, including 10 federal agencies. The task force additionally suggested the perpetrators may hail from Russia, presenting national security concerns for the United States.

Happenings like these demonstrate that cyberthreats are an increasingly global menace requiring unity and coordination from the public and private sectors.

4. Don't expect mercy from cyberthreats

In October 2020, Virginia's Fairfax County Public Schools (FCPS) fell prey to an increasingly notorious predator: ransomware. Ransomware blocks access to – or threatens to leak – data unless a ransom is paid. In recent years, cybercriminals have used this malicious software to extort huge payouts from public school systems like FCPS.

Adding insult to injury, FCPS was struck while many students and teachers were learning remotely because of the COVID-19 pandemic. Rather than expecting mercy from cyberthreats, agencies like FCPS should increase their vigilance during moments of weakness such as public health emergencies.

Industry Perspective

Strengthening Your Agency's Web Apps

An interview with Ted Rutsch, Federal Account Executive, Invicti Security

The modern world runs on web applications, and governments are no exception. But at every level, these apps are growing at a rate that is overwhelming agencies' security teams. To ensure security of these web apps, it is vital that new processes be introduced to help maintain a strong IT security risk posture.

Traditionally, agencies have used manual penetration testing to identify web app security vulnerabilities or scanners prone to false positives that then require manual verification before acting. Not only is this process costly and slow, but it raises the potential for human error exponentially.

Fortunately, the right mix of strategies and tools can keep agencies safe from resilience-damaging security incidents. By automating processes in DevSecOps and leveraging Dynamic Application Security Testing (DAST), agencies can plug every gap in their web apps.

"Fifteen years ago, there were 50 million websites in the IT marketplace," said Ted Rutsch, Federal Account Executive at Invicti Security, a web application security solutions provider. "Now there are nearly 2 billion. Application security automation has become paramount."

Rutsch provided three tips to agencies looking to secure their web apps for stronger resilience.

1. Dive into DevSecOps

DevSecOps combines software development, security and IT operations into one methodology. Shortening the development life cycle helps agencies continuously provide higher-quality software; making security integral to the development process, meanwhile, assists agencies with avoiding harmful security incidents.

"The life cycle to put out a secure website was eight to nine months," Rutsch said of the time before DevSecOps. "Today, agencies are doing that in a matter of weeks."

Furthermore, although DevSecOps begins with people, combining modern security processes with automation can streamline an agency's path to a strong risk posture.

2. Adopt automation

By introducing security automation into web apps' software development life cycle. Agencies can intelligently navigate their apps and find exploitable vulnerabilities - without false positives. Integrations directly into the development environment allow for the automation of workflow assignments and can fix retesting to make issue remediation as efficient as possible. Agencies without automation are trying to patch vulnerabilities reactively, Rutsch said.

Additionally, automation can rapidly align agencies with their federal, state, local and global security compliance requirements. Directives like The National Institute of Standards and Technology (NIST) 800.53 and the Federal Risk and Authorization Management Program (FedRAMP), which authorizes cloud services to hold federal data, can now be met, enabling agencies to securely move apps to the cloud.

3. Dynamically test app security

Modern DAST tools identify potential security flaws in web apps by communicating with the front end of these programs. Rather than reviewing static source code, DAST tools detect security gaps by simulating attacks and automatically confirming exploitable vulnerabilities. Ultimately, DAST tools like those Invicti Security provides reduce the time and energy agencies spend to deliver secure web apps.

"You can imagine how overwhelmed some of these application testing teams are keeping up with the release of new and updated apps," Rutsch said.

By combining automation and DAST processes, agencies can now improve their DevSecOps for better resilience, compliance and stronger web apps.

Tricks for Workforce Resilience

Resilience Area #2

Examples of Resilient People

Government employees anchor every agency's resilience. After all, public-sector workers' dedication helps agencies pivot around distractions and triumph over adversity.

Yet big or small, no agency can embrace resilience without cultivating a steadfast workforce first. Above all else, resilient workers feel psychologically safe, or comfortable sharing their criticisms, ideas and thoughts without fearing judgment or negative consequences. Furthermore, resilient workers also possess the adaptability and speed necessary for any scenario. Rather than getting caught unaware, resilient employees know the barriers keeping their agency from mission wins.

Mixing psychological safety, agility, speed and preparedness, resilient workers can stand with their agencies through thick and thin.

1. Start surge hiring

Surge hiring fills a massive amount of jobs in a short time, making it useful for improving agencies' resilience. Through surge hiring, agencies can gain the workforce necessary to solve any complication.

For proof, see the Biden administration's national strategy for responding to COVID-19. Released in January 2021, the strategy repeatedly utilizes surge hiring to combat the coronavirus.

Picture the state and local agencies that, pre-COVID-19, had antiquated data systems incapable of connecting testing laboratories and public health agencies. Biden's strategy promised federal surge hiring will correct this issue by assisting agencies with near-term manual processes such as tracking laboratory results.

2. Establish workforce sprints

Workforce sprints are short-term projects that focus on the most pressing matters as swiftly as possible. Via sprints, agencies can briskly educate their employees about subjects such as resilience.

In March 2021, Secretary Alejandro Mayorkas announced that DHS would conduct six 60-day sprints. The first three sprints will discuss ransomware prevention, bettering the cybersecurity workforce and industrial control system resilience, Mayorkas said. Future installments will cover protecting transportation systems, safeguarding election systems and advancing international capacity-building.

By teaching vital lessons in record time, agencies such as DHS can make their employees smarter about concepts like resilience.

3. Think outside the box

At times, resilience requires agencies to pursue their missions in unorthodox ways. Innovative workforces are not only more receptive to novel ideas – they are also better equipped for disruptions.

Look at the Jacksonville, Florida Transit Authority (JTA). Like many transportation agencies, COVID-19 presented JTA with extra constraints providing safe transit to passengers. Rather than reduce operations, however, JTA applied its workers to new ventures.

In March 2021, JTA announced it would help bring COVID-19 vaccines to seniors and at-risk citizens throughout Jacksonville. Using two retrofitted buses for vaccine deliveries, JTA depicts how agencies can raise communal resilience by giving employees new roles.

4. Get informed

Resilience requires agencies to grasp the dilemmas they face. Consequently, agencies that train their employees about headaches like cyberthreats are prepared for such ailments.

The National Cybersecurity Center (NCC), a cybersecurity awareness and innovation nonprofit, offers agencies a glimpse of the opportunities available to their employees. In March 2021, NCC began a nationwide push to train state lawmakers and their staff about best practices in cybersecurity. In all 50 states, NCC hosted live virtual forums and interactive, on-demand workshops exploring common cyberattacks, cybersecurity best practices and other curriculums.

Employee training is not limited to cybersecurity, however. Over time, more informed personnel can make their organizations more resilient.

The White House has made cybersecurity the #1 priority for 2021.

While agencies have established tight security standards for tablets, laptops, networks, and servers, there is no overarching standard for large-format displays. Download our FREE guide to discover the cybersecurity essentials for large-format displays in Federal Government environments.

Find out how Samsung can help you integrate this newest layer of technology into your agency infrastructure—and further safeguard your security. **Download the guide today.**

Tips include:

- Avoid features that open up vulnerabilities.
- Take a multi-layer security approach.
- Create secure options for remote work.
- Implement a well-structured security detection chain.
- Develop a clear response plan.

Industry Perspective

Procuring Your Agency’s Secure Digital Displays

An interview with Mike Bahniuk, Director of Federal, Samsung

Most people understand that when devices connect to networks, they can become a security risk.

But think about the large digital displays many agencies use to direct visitors and share information with employees. While not traditional devices, these displays must still be protected when they connect to networks.

“Anything with an IP address is suspect,” said Mike Bahniuk, Director of Federal at Samsung, an electronics and IT solutions provider. “Security is paramount at all different levels.”

Bahniuk outlined three ways agencies can procure secure digital displays that meet all their communication and collaboration needs.

1. Reduce risks

For better or worse, modern devices are more connected than ever. Digital displays are no exception, and many contemporary models boast everything from Bluetooth to Wi-Fi connectivity.

For agencies, these capabilities can become a double-edged sword. While letting workers broadcast their presentations in conference rooms can be valuable, it can also leave their agencies vulnerable to cyberthreats. Attackers can reach agencies’ networks through digital displays and cause trouble.

“The security piece outweighs the convenience from connectivity,” Bahniuk said.

Before procuring digital displays, agencies should determine which connectivity capabilities may put them at risk. Ultimately, these decisions will help agencies avoid displays that endanger their resilience.

2. Protect data

Agencies considering digital displays should also carefully consider how these machines retain their data. After all, no agency can risk digital displays accidentally showing their sensitive information too long.

To avoid this problem, agencies should factor data screen retention and memory volatility into their digital display procurements. Digital screen retention happens when screens retain data or images for longer than necessary. Memory volatility, meanwhile, features the display’s memory – or the memory of another connected device – storing information for problematic amounts of time.

“Now, as soon as they’re off, all that memory and data retention is gone,” Bahniuk said of newer digital displays.

3. Focus on compliance

Currently, agencies must comply with global, federal, state and local rules about everything from data privacy to supply chain origins. Digital displays are not immune to these regulations, so buying the right one can help agencies meet their compliance requirements more easily.

Take the Trade Agreements Act of 1979 (TAA), which governs trading pacts between the United States and other nations. TAA can forbid federal contracts from procuring noncompliant products and services; for digital displays, the legislation’s stamp of approval designates which ones come from TAA-friendly countries.

Overall, companies like Samsung can connect agencies with digital displays that boost their resilience by avoiding security incidents. Whether military bases, post offices or other government locations use these displays, no agency wants their mission disrupted.

“It really has a lot to do with the government use case,” Bahniuk said of each agency’s needs. “We are helping them with their mission and their citizen experience.”

Refine Workflows for Resilience

Resilience Area #3

Examples of Resilient Processes

For true resilience, the processes agencies practice must match their current state. Imagine an agency that has radioactive offices. Although this agency typically meets in person, continually doing so might sicken its employees. This agency must work remotely or cease functioning.

Processes are foundational, then, to building the path agencies follow toward mission success. These workflows must align with agencies' goals while producing tangible progress. More importantly, these operations must react to shifting developments effortlessly.

Resilience is thus about dynamism. Public needs are not static, and agency processes that cannot evolve with them may fall short of mission victory.

1. Centralize responsibilities

Centralization can fuel resilience by breaking down the silos between governments and their partners. Once freed to communicate and collaborate effectively, the sky's the limit for how resilient agencies can become.

Examine North Dakota's Information Technology Department (NDIT). In January 2021, NDIT announced it was centralizing the installation process for a statewide anti-malware software program. Beforehand, 45,000 computing devices used by K-12 students statewide needed these cyberdefenses manually installed. Now, school districts can implement and manage the software more easily.

Actions like NDIT's soothe pain from malware and centralize cyberdefenses, increasing agencies' resilience exponentially.

2. Perform pilots

Pilot programs are small experiments that gauge how well large-scale projects might work at organizations. These initiatives let agencies test resilience boosters without serious consequences or investments.

In April 2021, the Defense Department (DoD) announced such a trial. Titled the Defense Industrial Base Vulnerability Disclosure Program, the 12-month event will run out of DoD's Cyber Crime Center (DC3) component. The pilot will let defense industrial base companies responsible for producing military equipment voluntarily disclose cybersecurity vulnerabilities. DC3 will then provide these businesses guidance about eliminating their flaws, refining the resilience of everyone involved. Pilots are not limited to cybersecurity, so agencies can use them to try out any resilience modification.

3. Cooperate across agencies

Strength exists in numbers, and agencies are no exception. Working together, agencies not only share information and assets – they also toughen up to face internal and external woes.

Rather than struggle separately, Missouri's agencies banded together during the COVID-19 pandemic. In September 2020, the cross-governmental COVID-19 Fusion Cell released expanded dashboards dealing with the virus. These portals collected COVID-19 data from more than four Missouri agencies, providing a clearer portrait of the pandemic statewide.

Knowledge is power, and Missouri's COVID-19 Fusion Cell models how agencies' collective wisdom can benefit one another. The more agencies rely on their colleagues, the less resilient they need to be alone.

4. Prioritize critical tasks

Like it or not, agencies must often pick and choose between their desires. The choices agencies make can influence their resilience, so their leaders must carefully select their priorities.

Fortunately, programs like the Internal Revenue Service's Pilot IRS program can make a difference. Pilot IRS permits the agency to demo new technologies faster due to its processes. The tools that do not meet the IRS's expectations do not reach the next funding level, ensuring the agency does not spend extra time on them. IRS can then focus on the most promising options.

Prioritization can clear distractions, letting agencies focus on items that are critical to their missions and resilience.

Industry Perspective

3 Ways to Secure Your Agency's IT Environment

An interview with Tim Brown, Chief Information Security Officer and Vice President, Security, SolarWinds

Today's agencies have more sprawling IT environments to defend than ever. In the past, cyberdefense meant securing agencies' network perimeters. However, modern agencies must think beyond their office walls and protect modern networks ranging from cloud computing to remote work systems.

Even worse, the more agencies' attack surfaces grow, the faster the rate of sprawl seems to increase. Changes like these once took years or months but now take weeks or days. With IT environments ballooning at unprecedented speeds, staying in the loop about the latest cyberthreats, software and vulnerabilities can overwhelm any agency.

Vendors are dealing with the same challenges. Going forward, the public and private sectors will need to defend their IT environments together if they are to stand a chance against the latest cyberthreats.

"It is critical we cooperate better," said Tim Brown, Chief Information Security Officer and Vice President, Security at SolarWinds, an IT operations management software provider. "Cybersecurity has to be a factor in everything the government does."

Brown shared three ways agencies can work with private-sector businesses to improve both parties resilience.

1. Designate crown jewels

An agency's crown jewels are the assets critical to its mission. Whether these resources are data, people or something else, crown jewels anchor organizational resilience. If their crown jewels are compromised, agencies cannot function, let alone serve constituents.

"When you're designing security for an environment, it's important you can treat someone like an administrator as special," Brown said as an example. "It's okay to treat some individuals or applications as special."

After identifying their crown jewels, agencies can create plans for preventing, detecting and recovering from attacks against these valuable components.

2. Form public/private partnerships

Currently, most agencies leverage a mix of public- and private-sector products and services. At every level, these agencies need to pick vendors that will meet their unique needs for concerns such as cyberthreat detection.

Take intelligence agencies. They may handle data with national security implications, so they may need stronger cyberdefenses than civilian agencies. When picking vendors, these agencies will want partnerships with only the most reputable cybersecurity companies.

"Collaboration is critical for us as a community to move forward," Brown said. "We need to be open about how software is developed and we believe the recent Executive Order on Federal Cybersecurity and the recent nominations for critical cybersecurity leadership positions are important steps towards achieving a collective and collaborative defense posture."

3. Build baselines

Baselines are patterns of normal behavior that can help agencies determine unusual, even malicious, activity. Using software tools from providers like SolarWinds, agencies can establish routines for their entire IT environments.

Presently, agencies must govern everything from databases to application performance. Without tools to measure the resilience of these areas, agencies may miss potential disruptions.

"A well-managed environment becomes a secure environment," Brown said. "Without management, you can never, ever be secure."

Harden Your Agency With Technology

Resilience Area #4

Examples of Resilient Technology

Technology can seem like the cornerstone of public-sector resilience. Tools like cloud computing can make agencies more agile, reliable and scalable than before. Even more exciting? Today's emerging technologies may become tomorrow's most fulfilling solutions. Once realized, inventions like AI may revolutionize resilience. AI imitates learning and other cognitive human behaviors, so it could generate fantastic benefits for agencies.

Despite this, resilience is not some technology agencies buy, install and forget. The fact is no technology fortifies an agency's resilience if its workers do not comprehend it. Having backup plans is also necessary. Should agencies depend on one tool that fails, their operations, products and services may falter.

There is no denying that technology is pivotal to resilience, however. Thanks to technology, agencies can adjust to meet any conundrum head-on.

1. Reduce hardware

All agencies have hardware. But few agencies have hardware like the National Oceanic and Atmospheric Administration (NOAA). At NOAA's Joint Polar Satellite System (JPSS) component, the hardware processes data to predict severe weather and monitor the environment.

In March 2021, JPSS replaced scores of computer racks in Suitland, Maryland, by transferring part of this system to the cloud. Between Suitland and JPSS's backup facility in West Virginia, this alteration shrank the agency's hardware footprint by 40%.

Downsizing hardware makes agencies like JPSS less dependent on tools susceptible to physical destruction. Cloud adoption sweetens the pot by augmenting agencies' adaptability, constancy and rapidity.

2. Leverage use cases

When possible, agencies installing resilient technology should imitate their successful peers. Established in 2007, the federal government's Trusted Internet Connections (TIC) program explains how agencies can securely connect to external federal networks.

Recall the TIC Branch Office Use Case CISA released in April 2021. This use case details how agencies can directly network with cloud-based resources or other trusted external zones. Previously, TIC directed agencies to route internet traffic through their headquarters or a TIC access point. With more agencies working remotely or migrating their data to cloud, these evolutions keep TIC relevant.

All told, the public sector is overflowing with specimens like TIC's Branch Office Use Case that can make agencies' technology sturdier.

3. Embrace zero-trust cybersecurity

Resilience and security are permanently linked – neither concept can exist without the other. Agencies looking for both qualities should ponder zero-trust cybersecurity. By automatically distrusting all users and systems, zero-trust cybersecurity can spare agencies from cyberattacks.

New York City Cyber Command (NYC3) governs the cyberdefenses New York City uses to protect its assets, employees and residents. In December 2020, NYC3 published a request for information about constructing a zero-trust environment for New York City's entire municipal digital infrastructure.

By baking zero-trust cybersecurity into their IT, agencies such as NYC3 can make their communities more resilient and secure.

4. Assign workloads to chatbots

Chatbots are software applications that conduct text conversations with people online. During spikes in activity, chatbots can shoulder some of the workload agencies' human employees carry.

In April 2020, the Texas Workforce Commission (TWC) fielded millions of calls within a week. With TWC's record call volume before COVID-19 reaching about 60,000 daily calls, the agency created a chatbot to answer some common questions. Once launched, "Larry the Chat Bot" started answering questions about the unemployment insurance process.

Chatbots like Larry are not just cutting-edge – these digital assistants boost resilience by keeping humans from getting overwhelmed.

SecurID™

FOUR POINTS TECHNOLOGY

A Service Disabled Veteran Owned Small Business

Intelligence-Driven Security Solution for Government

GSA

SEWP

For More Information on SecurID and Four Points Technology's partnership visit

https://www.4points.com/it-solutions-partners/securid/

Four Points Technology, LLC
14900 Conference Center Dr, Ste 100
Chantilly, VA 20151
703-657-6100 | sales@4points.com

www.4points.com

NITAAC
OMB Authorized GWACs for IT Acquisition
CIO-CS
COMMODITIES/SOLUTIONS

Industry Perspective

Making Your Identity and Access Management Resilient

An interview with Steve Schmalz, Field Chief Technology Officer, RSA Federal

No government can afford the wrong people accessing their information. After all, constituents expect that the sensitive data they give to agencies will remain private. When cybercriminals steal that data, the trust between agencies and their constituents erodes.

Unfortunately, remote work has made cyberdefense more difficult for agencies. Traditionally, governments have protected their data by constructing network perimeters around it. But as the distance networks cover grows, so do the chances of a cybersecurity incident disrupting agencies' resilience.

Cloud-based identity and access management (IAM) can free agencies from this predicament. IAM covers the framework of policies and technologies ensuring the right users access the right resources appropriately. When combined with cloud computing, IAM can dramatically improve public-sector resilience.

"You want a deployment model that's flexible enough to protect your workforce no matter where they do their work," Steve Schmalz, Field Chief Technology Officer (CTO) at RSA Federal, a computer and network security provider said of the cloud.

Schmalz discussed three methods for increasing agencies' resilience with cloud-based IAM.

1. Turn to zero trust

Perimeter-based security has a major flaw: it makes perimeters the only place agencies can enforce security. If cyberthreats breach this perimeter, agencies' resilience may be at risk as the only way to shut out cybercriminals is to shut out everyone.

Enter zero-trust security. Zero-trust security treats all devices and users as untrustworthy until their identity has been verified. This model prevents bad actors from obtaining valuable assets by deploying multiple policy enforcement points as close to the assets as possible. If a breach happens at one of these assets, it must be shut down.

2. Add authentication options

Today, agencies have an unprecedented number of identity authentication services. Whether it is authentication tokens, cell phones or other options, agencies can leverage the most convenient and secure solutions for their workers. Even better, cloud can help agencies implement these solutions with more speed and security than before.

Biometrics can add another security layer to cell phones by making users verify their identity using bodily characteristics such as fingerprints.

3. Unify user experiences

Too often, agencies cannot provide the same UX for tools like IAM when they are on-premise or cloud-based. With a hybrid approach that effectively integrates their on-premise and cloud-based IAM services, agencies can ensure their users' login experience is the same no matter what services they are accessing.

Cloud-based IAM like RSA Federal provides can give agencies the cloud's flexibility and scalability without sacrificing security. The result is more resilient agencies worrying less about implementing secure IAM.

Additionally, Schmalz encouraged agencies interested in learning more about RSA Federal's solutions to contact Four Points Technology, an IT solutions provider. Four Points Technology is RSA Federal's Platinum partner, offering RSA Federal's solutions on federal contracts and presales engineers who can evaluate customers' needs.

How Resilience Makes the Defense Logistics Agency Ready for Anything

The Defense Logistics Agency (DLA) supports the U.S. military's combat logistics worldwide, so it cannot have many delays. The explanation is simple: When it comes to war, lags can mean the difference between life and death. Preserving agencywide resilience, then, ranks as one of DLA's highest concerns.

This dichotomy has made resilience part of DLA's DNA, said Vice Director Brad Bunn. With about 26,000 employees operating in most states and 28 countries overseas, the agency currently provides more than $42 billion in goods and services annually. This translates into roughly 86% of the military's spare parts and nearly 100% of its fuel and troop support consumables, making DLA's resilience indispensable to how America's armed forces live, work and fight.

GovLoop spoke with Bunn about how resilience propels the agency's mission at home and abroad.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: How can people create a culture of preparedness making their agency more resilient?

BUNN: It goes to the focus we put into understanding what makes our workforce tick and what drives our culture and climate in the agency. We've had a robust culture climate program for many years. It gets to things in our organizational culture we can diagnose, pinpoint and act on. Are we preparing our workforce to be adaptable and agile? There is a portion of our culture model that deals with being able to adapt to change and change management. As a combat support agency, we're constantly adapting to what our customers want and what our leadership and DoD are driving toward. We must be a dynamic and innovative organization. Hopefully, we're not just meeting our requirements, but exceeding them.

We've built that into our leadership training and development. We've built that into what we call our culture climate action plans. Those are heavy with communication with the workforce, some amount of training and development that builds that competency within our workforce and then certainly in our actual mission plan.

These are things that any organization, any institution, ought to focus on. Because of our reach, these things become especially important to accelerate our ability to adapt. There is constant looking in the mirror and seeing where we need to add focus.

How can improving your agency's processes boost DLA's resiliency?

There's good news and bad news with our processes. I won't call them rigid, but they are very structured and repeatable. We are a heavily process-oriented organization. Those processes are reflected in our IT systems and financial processes.

The good news is those processes can be executed in 100 different ways regardless of whether we're in the office or 100% virtual, if that IT is operational. It's not just how the system works. It's why the system works the way it works. If we do have a disruption, we can still perform those operations even if it is in a different way.

We have standardization across most of our business units. Whether it is IT or something else, if we need another business unit to pick up some workload, we can move that workload to that unit and the same processes still exist. Process management is important for several things. It also ensures we are auditable and accountable and our customers understand how we do our business.

What are some best practices for resilience you'd recommend to other agencies?

In a military sense, resiliency is usually focused on the individual and ensuring they have resources at their disposal to deal with not just crises in their personal or professional lives, but the things that add stress.

The best way to prepare for something is to practice how you'd respond if it happened. We try to do that at DLA. When you practice that, people become more comfortable with adapting to a quick change in their environment. They're not so unaccustomed to having to work in a different way.

We were able to move quickly to telework because we had practiced it for so long. Not every future natural disaster or other type of crisis will cause the same thing. It could be we don't send everyone home to work. We may need to relocate some folks to another place. The DLA practices both kinds of COOP exercises.

There's not much more important work out there than supporting our military and what they do. What I've seen over the past year with our people, even though they've dealt with stress – and, in some cases, tragedy in their personal lives – what keeps them focused is the mission. Having a purpose and being part of something bigger than themselves is a great motivator. That's one area where we have an advantage over the private sector. It's easy to get really attached and invested in the mission we perform for our nation. That's what drives our people to go above and beyond.

Industry Perspective

Managing Your Agency's Machine Identities

An interview with Diane Garey, Product Marketing Manager, Venafi

Government security teams already have their hands full trying to manage the identities of the people accessing their agencies' networks. Meanwhile, a new identity challenge is growing. Beyond authenticating humans, these teams now realize they must also manage the identities of countless machines like systems, applications, devices and other non-human entities on these networks.

In many cases, these digital services do not involve humans at all. Instead, they cover machine-to-machine communications. Fortunately, such systems use unique certificates and keys that can verify their identities before they access data or other network resources. Tracking all this information, however, is hard work.

"As there are more machines doing more things, managing machine identities can't be the domain of small certificate service teams anymore," said Diane Garey, Product Marketing Manager at Venafi, a machine identity management solutions provider. "There are too many machines to track them all."

Thankfully, automation can help agencies manage and secure machine identities more easily. Automation involves machines performing processes with little to no human input, saving people energy and time on things like requesting, approving, monitoring and renewing machine identities.

Garey explained three ways agencies can become more resilient by streamlining their machine identity management and security.

1. Avoid certificate outages

Certificate-based outages occur when the unique certificate verifying a machine's identity expires. These outages not only disrupt agencies – they also give cybercriminals an opportunity to slip onto agencies' networks using vulnerable machines.

"We want to make sure bad actors can't get on to the network and get to sensitive data," Garey said.

Automating certificate renewal not only reduces outages, it assists humans with managing and securing machine identities agencywide. Preventing cybersecurity disruptions, meanwhile, strengthens agencies' resilience.

2. Lighten workloads

For better or worse, authenticating machine identity certificates can become a lengthy process. For example, Garey cited a federal agency that manages 500 certificates annually. Each year, a contractor physically checks and approves these certificates at a location separate from the agency. Since 2020, the COVID-19 pandemic has only complicated this workflow.

"If I'm responsible for a big volume of certificates, if I must update them once a year instead of once every two or three years, that is a huge increase in workload," Garey said.

Fortunately, automation can reduce the burden by ensuring these machine identity certificates are renewed without human intervention.

3. Speed software development

Nowadays, software is often a crucial component of the products and services agencies deliver to citizens. Besides the other benefits, automating machine identity management can also speed up software development and strengthen cybersecurity.

"You don't want developers to be working on an application and have to pause for an hour or day to get what they need from machine certificate services," Garey said.

Management platforms like those Venafi provides can automate security for the machine identities on government networks. The result is more resilient federal, state and local agencies whose employees are not looking over their shoulders for cyberthreats.

How Connecticut Reinforced its Resilience

With resilience, simpler is sometimes better. The fewer people, processes and technologies agencies have, the less energy it takes pleasing the public. Gradually, the more streamlined agencies grow, the more resilient they become too.

Reflect on Connecticut's recent step to consolidate all its IT into one agency. In March 2021, Gov. Ned Lamont proclaimed that Connecticut would spend one year merging the state's IT capabilities into its Department of Administrative Services (DAS). Once streamlined, Connecticut's IT will be more reactive, sustainable and secure.

GovLoop spoke with CIO Mark Raymond about how Connecticut's IT merger breaks new ground for his state's resilience.

The interview below has been lightly edited for brevity and clarity.

GOVLOOP: What is resilience, and how would you like Connecticut to become more resilient?

RAYMOND: To me, resilience is our ability to continue to meet our constituents' needs in a changing environment. And "changing environment" is a loaded word, right? We have changing environments and changing legal, regulatory and political frameworks. Our physical world changes around us. How do we continue to meet the needs that we have and emerging needs in a consistent way? Lots of that comes with flexibility in how we deliver, the ability to adapt and to recognize what is happening around us, and what changes we need to put in place for that. It is one of the reasons why we're changing how we are structured around technology. We have so many different silos of agencies and technologies that prevent that flexibility in applying technology and applying skills. We know that we can become more resilient if we can more flexibly apply the deep skills that we do have to the challenges that we face.

How can IT consolidation make Connecticut more resilient?

First, having the ability to flexibly deploy deep skills across agencies as needed would make us more resilient. We have great skills in our workforce, but it is just happening in pockets, so they are not as broadly applied as we need them. It is like cloud architectures, right? To be able to deploy those as needed and be flexible in how we do that generates greater commonality of use and faster times to embrace some of these new technologies.

I think greater automation in the things we do also helps us become more resilient. When you talk about scale – like a 30,000-person organization like we have in the state – automation allows you to do things at mass much more quickly. If you must touch each individual device, you can't change as quickly. Automation helps that quite a bit. It is not a natural skill to a lot of our technicians – it must be taught. To have everyone together where we can teach and apply these skills and grow our people to think this way and put them in place, it helps us to become more resilient and create more value.

Today, if someone wants to grow in their career, many times they need to leave their agency and go get a promotion someplace else. They leave the knowledge, the background and the agency they know and love behind. By having our IT people within an organization where we are serving all of them, we create some greater career pathing and growth without having them give up on that service and knowledge that they have with a business unit. We view that as creating a more resilient and responsive IT workforce.

What best practices for resilience do you recommend?

Don't put all your eggs in one basket. Have options and consider failure. Technology is so important to our delivery. If you only rely on it, understand how you would operate without it for COOP, planning and discipline. I think some folks may have gotten away from that. In Connecticut, we have not.

Continue to plan and practice before it becomes something urgent. I would love for people to seek out their emergency operations teams and ask them to run through some best practices around cyber and around failure of critical systems.

Thinking about redundancy cannot be underestimated, right? Many times, people use technology to reduce costs. They reduce them so much they forget about needing to add redundancy into the process. Whether it is with multiple areas of the cloud, multiple data centers or different kinds of network connections, with the proliferation of ransomware, you must have alternative processing and options in the event some are constrained or unavailable, so you can continue your operations.

What do you hope is readers' main takeaway about resilience?

People rely on government services more than you know. In many instances, it is life and death. It is important to understand where your failures are and know that you can continue to operate. Technology will fail, right? That is the guarantee. It will be inaccessible at some point in time. So, how have you planned for what that looks like? Knowing that you are asking yourselves these important questions is what I hope people take away.

Industry Perspective

How Hybrid Clouds Can Cover Your Agency's Resilience

An interview with Brad Bowers, Director, Enterprise Cybersecurity, SHI

Most agencies realize their legacy IT is way past its expiration date. Despite this, many federal, state and local governments are hesitant to adopt cloud computing. After all, deciding whether their sensitive citizen data should reside in public or private clouds can intimidate agencies.

Thankfully, hybrid clouds can cover almost any need agencies have. Hybrid clouds mix public and private cloud environments, giving agencies benefits from both deployment models.

For example, hybrid clouds can keep agencies' on-premise resources private while letting them access publicly available cloud services. This format boosts agencies' resilience by choosing the cloud setup that is best for their operations and data.

"Utilizing a hybrid cloud environment can be a highly effective and cost-effective way to get things done," said Brad Bowers, Director, Enterprise Cybersecurity at SHI, a software provider that offers hybrid cloud solutions.

Bowers detailed three ways hybrid clouds can improve agencies' resilience – and everything else.

1. Increase resilience

Resilience revolves around shrugging off disruptions. Using hybrid clouds, agencies can adjust their IT capabilities according to their needs. For instance, agencies can increase their website bandwidth during political elections for surges in user traffic.

Even better, hybrid clouds can become multi-clouds. Multi-clouds leverage products and services from several public clouds, letting governments choose the options that fit their demands the best. Relying on multiple clouds also gives agencies a safety net if one cloud struggles.

"We're making sure that if one part of something goes down, it doesn't bring the entire agency or organization down," Bowers said.

2. Increase agility

Agencies do not always have the agility they need for disruptions like severe weather, which can interrupt power and threaten safety. Without agility, government employees cannot react to fluid circumstances quickly and efficiently. Even worse, these workers may not be able to assist constituents in need.

Yet hybrid clouds can make agencies nimble enough to overcome these problems. Thanks to hybrid cloud's flexibility, agencies can mold their products and services to whatever a situation demands.

"Agencies can focus on making applications and products that do what they want them to do," Bowers said of hybrid clouds' elasticity.

3. Increase security

Recently, agencies have embraced more remote work than ever. While convenient, remote work expands the perimeter agencies have typically defended, making cybersecurity increasingly difficult.

Enter zero trust cybersecurity. Zero trust cybersecurity assumes all users and devices on agencies' networks are untrustworthy until proven otherwise. Hybrid clouds enable agencies to rapidly implement and enforce zero trust cybersecurity by making agencywide governance easier and more manageable.

"A zero-trust strategy can focus on who the users are and what access they need," Bowers said.

When it comes to public and private cloud services, hybrid clouds offer the agencies the best of both worlds. Thanks to hybrid cloud vendors like SHI, agencies can also make their resilience more robust.

Best Practices for Resilience

For every agency, the best time to bulk up resilience is before calamity strikes. Even when that is not possible, constituents often depend on the products and services they receive from their governments. Services like unemployment benefits can save lives, so there is scant time to waste while providing them.

The good news is there are many small but significant steps agencies can take to make their people, processes and technology tougher.

Here are eight tips for making agencies more resilient, inspired by the federal, state and local thought leaders featured throughout this guide.

1. Expect stress

Agencies may crave resilience, but that does not mean they enjoy the conditions that make resilience necessary. Like it or not, turmoil is a given no matter agencies' size or scope.

Anticipating anxiety, then, eases the hardships agencies encounter while dealing with it. While covering bases is important, no agency can get them all. Because of this, government employees should prepare for every shock they can and take deep, steady breaths for every shock they cannot. The chances are that expecting pressure will help agencies survive it more confidently.

2. Remain optimistic

Public-sector employees are not immune to negativity. After a while, any workforce can be discouraged by adversity, failure and disappointment.

For leaders, this means carefully monitoring their agency's collective mood and promoting positive messages to keep employees focused on their mission. For workers, maintaining a glass-half-full mentality and networking with peers who support them can keep spirits high. And no matter where they rank, every employee should remember resilience begins with hope.

3. Regroup quickly

Resilience is like basketball – games are won and lost by the team that rebounds the best. Amid chaos, the faster agencies can resume their routines, the faster they can reconnect with constituents.

Envision agencies like engines – the most resilient ones run no matter what gets under the hood. To get on the right foot, resilient agencies map how they behave under ideal parameters. Next, these agencies plot how quickly they can regain these abilities after they come under fire. Most of all, such governments then design alternatives for when their original plans do not work.

4. Emphasize education

Employees contributing to their agency's resilience should consider the many options available to them. Whether it is coaching, mentoring or learning courses, workers have many avenues for nurturing personal resilience.

First, critical-thinking classes can teach employees procedures for making better decisions. Some courses also boost awareness of potential trouble spots, while others discuss resilience through teamwork.

Coaching, meanwhile, can personalize resilience for participants. The problem-solving approaches many instructors provide can benefit agencies down the road.

5. Exercise resilience

Like muscles, resilience will weaken if it is not flexed regularly.

Playing out worst-case scenarios, then, can be advantageous for agencies. These exercises let agencies approach real crises in safe settings; the same training can also heighten internal morale before setbacks occur.

Drawing from expertise about threats like ransomware, agencies can walk through how to respond during security incidents without truly suffering one. Rather than leaving people untested, courses like these prepare them.

6. Plot a way out

Without exits, agencies may find themselves stuck with the disturbances assailing them. Afflicted by something like a snowstorm, no agency wants to remain on the sidelines, away from the public.

To that end, agencies should consider failure a necessary evil. They should not expect one person, process or technology to save them heartache. No solution works if it cannot deal with the problem.

Generally, the agencies that rely too heavily on one answer to disruption may find themselves surprised by different questions. Conversely, broad toolkits can ensure that agencies bring the right solution to respond.

7. Foster friendships

Agencies do not need to go it alone. No matter their size, agencies can count on their peers when the road gets rocky. If that does not work, there are many private-sector businesses, academic institutions and nonprofits willing to lend a hand.

What can allies provide agencies? From data to expertise, funding to human capital, agencies do not know if they do not ask. The icing on the cake? Organizations propping one another up serves the greater good and makes society more resilient overall.

8. Play the long game

Patience is a virtue, and nowhere does this maxim ring truer than resilience. Recognizing this, agencies should commit themselves to resilience long-term. By continuously pursuing resilience, agencies can protect their operations, products and services better. As a bonus, the public can rest easy knowing their governments are ready for everything on the horizon.

Industry Perspective

Approaching Your Agency's Security Holistically

An interview with Mike Stolp, Director-Security Practice, Cask

Public-sector security and resilience are two pieces of the same puzzle. After all, agencies cannot operate continuously when their workforces are constantly fending off security threats.

Yet many agencies are discovering that seeing their security posture agencywide is harder than ever. For starters, these agencies cannot easily picture the security threats and vulnerabilities facing them. Even worse, budget, manpower and regulatory constraints are making it tougher for agencies to prioritize the problems they can find. The resulting mix is potentially ripe for disaster.

Fortunately, automation can save the day for agencies. Automation involves machines performing manual processes with little to no human input. Using automation, agencies can reduce the strain security places on their employees. Even better, automation can make holistic security – and, in turn, resilience – easier to govern than before.

"Agencies should be able to manage their security environment in a way that they understand the threats they are facing," said Mike Stolp, Director-Security Practice at Cask, a security solutions provider. "Automation allows you a single point of view from end-to-end."

Stolp outlined three ways agencies can strengthen their resilience by automating their security agencywide.

1. Reduce human error

To err is human, and people can produce scores of security mishaps for agencies. For instance, the more employees check IT systems for potential vulnerabilities, the more likely they are to miss these gaps.

"People are much more easily corruptible than systems are," Stolp said. "You can scan systems, but you can't scan a person."

Whether it is curbing human error or eliminating potential insider threats, automation can make agencies' overall security healthier.

2. Increase security testing

Stolp recommended agencies frequently measure their security. One option is penetration testing, which simulates cyberattacks to gauge a system's potential shortcomings. Tabletop exercises, meanwhile, imitate real-world disruptions like hacking to prepare people for them.

When it comes to tests such as these, automation assists agencies with conducting them faster and more often. Over time, this improves agencies' ability to find, fix and prevent trouble.

"Automation helps validate things faster whether they are working or not," Stolp said. "If you have a system that is highly automated from end-to-end, you can detect security lapses as they occur."

3. Standardize security routines

Regrettably, some agencies do not consider security when designing and implementing new products and services. Automation, however, can quickly and easily standardize security into any process agencies wish.

"Security is a cycle, not an event," Stolp said. "Treat security as a core part of your operational levers."

Gradually, automated security solutions like those Cask provides can help agencies see their whole security posture clearly. When agencies are no longer in the dark about today's threat landscape, the result is a renewed focus on citizens and mission wins.

Conclusion

Just because there are potholes does not mean there should not be roads. Rather than driving around inconveniences, resilience can permit agencies to plow through them instead.

This approach might be messy, but it beats giving up. The public relies on agencies, and meeting constituents' needs gives public servants their careers. Satisfying the public often nets agencies mission victories too.

No agency wants to be a cautionary tale. Rather than becoming a warning to their peers, resilience can give agencies the flexibility, responsiveness and speed their employees need to thrive.

About GovLoop

GovLoop's mission is 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 the public sector.

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

govloop.com | @govloop

Thank You

Thank you to Cask, Four Points Technology, Invicti Security, Juniper Networks, Samsung, SHI, Solarwinds and Venafi for their support of this valuable resource for public sector professionals.

Authors

Mark Hensch, Senior Staff Writer

Designers

Nicole Cox, Jr. Graphic Designer

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

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

www.govloop.com
@GovLoop