11:11 SYSTEMS | BROCHURE

Five IT Pain Points for SLED ORGANIZATIONS

11:11 SLED BROCHURE

RETHINK CONNECTED

There is little room for infrastructure failures.

- Cybersecurity
- Disaster Recovery and Operational Continuity
- Hybrid Cloud Computing
- Infrastructure Modernization
- Budget and Cost Control

If you're a state, local, or education (SLED) organization, you understand the need for a robust, secure, and resilient IT infrastructure. The need to provide reliable, always-on business platforms has fueled the need for cloud computing due to its on-demand functionality.

For essential services, like 911 operations and police and fire departments, downtime is unacceptable. Aging infrastructures are more likely to experience component failures or slow performance, reducing employee productivity and the citizen experience. Security is always at the forefront as well. If a ransomware or malware attack occurs, services could grind to a halt.

CYBERSECURITY

Cybersecurity has been one of the top SLED pain points for years. The 2022 Verizon Data Breach Investigations Report[1] uncovered that ransomware grew 13% in 2021, an increase as large as the last five years combined. This increase is across all sectors, affecting every region of the globe.

The most common route for cybercriminals to gain unauthorized access is through users accidentally clicking malicious links, visiting websites that are not secure, and/or clicking on phishing emails, according to the Veeam 2022 Ransomware Trends Report[2].

Preventing these attacks requires diligence within your internal teams. It's also imperative that you have sound infrastructure that includes encryption—at the hardware, system, application, and network levels—as well as software threat protection and a resilient backup and recovery architecture.

13% **increase in ransomware attacks in the last year alone**

47% **increase in number of attacks for government agencies in 2021**

According to CIOs, cybersecurity remains the biggest IT challenge and area of investment for SLED agencies. The pace of cybersecurity attacks has been accelerating, with a 47% increase in the number of attacks every week for government agencies[3]. The costs associated with breaches and attacks are accelerating as well.

Two examples that are often cited are the City of Atlanta, Georgia and the City of Baltimore, Maryland. The City of Atlanta was a victim of a ransomware attack that took many of the city's services offline for nearly an entire week, wreaking havoc for the city's court system and preventing residents from accessing critical services and paying utility bills. Baltimore also experienced a breach that took its 311 and 911 dispatch systems offline for more than 17 hours. This forced emergency support functions to switch over to manual instead of automated operations.

Cloud security can help combat these threats with a set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance, and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business.

[1] 2022 Verizon Data Breach Investigations Report

[2] Veeam 2022 Ransomware Trends Report

[3] Alarming Cyber Statistics for Mid-year 2022 That You Need to Know

DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

It is essential to have a comprehensive backup and disaster recovery strategy in place to protect against multiple risks while keeping all of your critical data and systems available.

Very few organizations can weather a major data loss event, security breach, or just simple downtime without some detrimental cost. We all hope that worst-case scenarios never happen, but the fact is that they do. When they do, you have to be ready to respond with the degree of speed and efficiency your organization requires. Both cloud backup-as-a-service (BaaS) and disaster recovery-as-a-service (DRaaS) focus on minimizing data loss when a disaster strikes. BaaS and DRaaS can provide the business continuity that your SLED organization needs.

HYBRID CLOUD COMPUTING

Many SLED organizations either have a cloud strategy or plan to implement one in the future. The flexibility to choose the most cost-efficient backup and recovery option is ideal for SLED organizations with smaller data centers, especially when there isn't a lot of budget for a hardware backup and additional offsite co-location costs. The primary benefit of a hybrid cloud is agility.

The need to adapt and change direction quickly is a core principle of any digital organization. In addition, with a cloud solution, you can choose what data you want backed up, providing an extra layer of resiliency while keeping costs low.

INFRASTRUCTURE MODERNIZATION

In the past, organizations that wanted to develop new technologies were required to establish their own on-premises IT infrastructure. That meant leasing a data center, bearing the up-front capital costs of new computer equipment, and developing in-house capabilities to deploy and maintain applications.

For many organizations, the massive technical and financial requirements of building and maintaining IT infrastructure are cost-prohibitive. There is also the desire to eliminate the need for the cumbersome bid process, expensive equipment refreshes, and complicated upgrade scenarios.

Cloud computing has created the opportunity for organizations to access the data storage and computing requirements on an as-needed basis—and with a significantly reduced up-front cost.

The exact benefits will vary according to the type of cloud service being used, but fundamentally, using cloud services means organizations do not have to buy or maintain their own computing infrastructure.

No more buying servers, updating applications or operating systems, incurring power and cooling costs, or decommissioning and disposing of hardware or software when it is out of date. This is all taken care of by the cloud partner.

BUDGET AND COST CONTROL

Funded by taxpayers and limited by annual, fixed—and sometimes extremely tight—budgets, SLED organizations must find ways to get the best infrastructure and performance while limiting costs.

3% **of SLED spending is allocated for information technology**

75% **of IT spending goes toward maintaining aging systems**

In many cases, SLED organizations are more likely to use equipment longer than other organizations or businesses, so it's important to be future-proofed. Only around 3% of all SLED spending goes toward IT[4]. And out of that small amount, the Government Accountability Office estimates that more than 75% of IT spending is allocated to the operation and maintenance of legacy systems that are rapidly aging[4].

Budget constraints are also intensifying talent and skills shortages. In a competitive labor market, public-sector institutions have traditionally been at a disadvantage in attracting and retaining the skilled talent required to drive modernization. They are limited in being able to match private-sector firms that offer highly competitive wages, innovation-oriented cultures, modern tools and technologies, and a wide breadth of opportunities.

This is why the focus for SLED agencies is on maximizing the efficiency of their limited resources. Leveraging cloud services means organizations can move more quickly on projects and test out new concepts without lengthy procurement and massive upfront costs.

Choosing a cloud solution built on industry-standard hardware is one way to dramatically cut costs, improve performance and manageability, and get the scalability required.

[4]U.S. Government Accountability Office

11:11 systems, an industry-leading provider of secure application and data protection cloud services built on proven VMware technology, is helping state, local government, and education customers around the world move to the cloud.

This digital transformation is helping to level the playing field against ransomware attackers, keep data safe, and ensure that operations are up and running. City governments—large and small—are responsible for critical services that materially impact the quality of living as well as the safety of their citizens. But their IT organizations are forced to operate with scarce resources, small budgets, and limited expertise to combat challenges like natural disasters and ransomware attacks.

IT professionals with state and local government agencies are consistently under-resourced when combating challenges like natural disasters and ransomware. At the same time, staff is tasked with literally keeping the lights on and maintaining critical services. 11:11 helps take the weight off their shoulders by protecting their data in the 11:11 Cloud with air-gapped backups and disaster recovery solutions or by migrating their live server workloads into the 11:11 Cloud Platform with enterprise-class support.

11:11 is working with hundreds of state and local governments and schools around the world to help fortify their IT strategies and guard against ransomware attacks through an intelligent migration to cloud-based services for infrastructure, disaster recovery, and data backup. In addition, with help from 11:11, these organizations are able to replace aging equipment on premises with affordable and award-winning, subscription-based cloud services. These services also include built-in security and access to compliance experts who are available around the clock.

DRaaS

Disaster Recovery as a Service

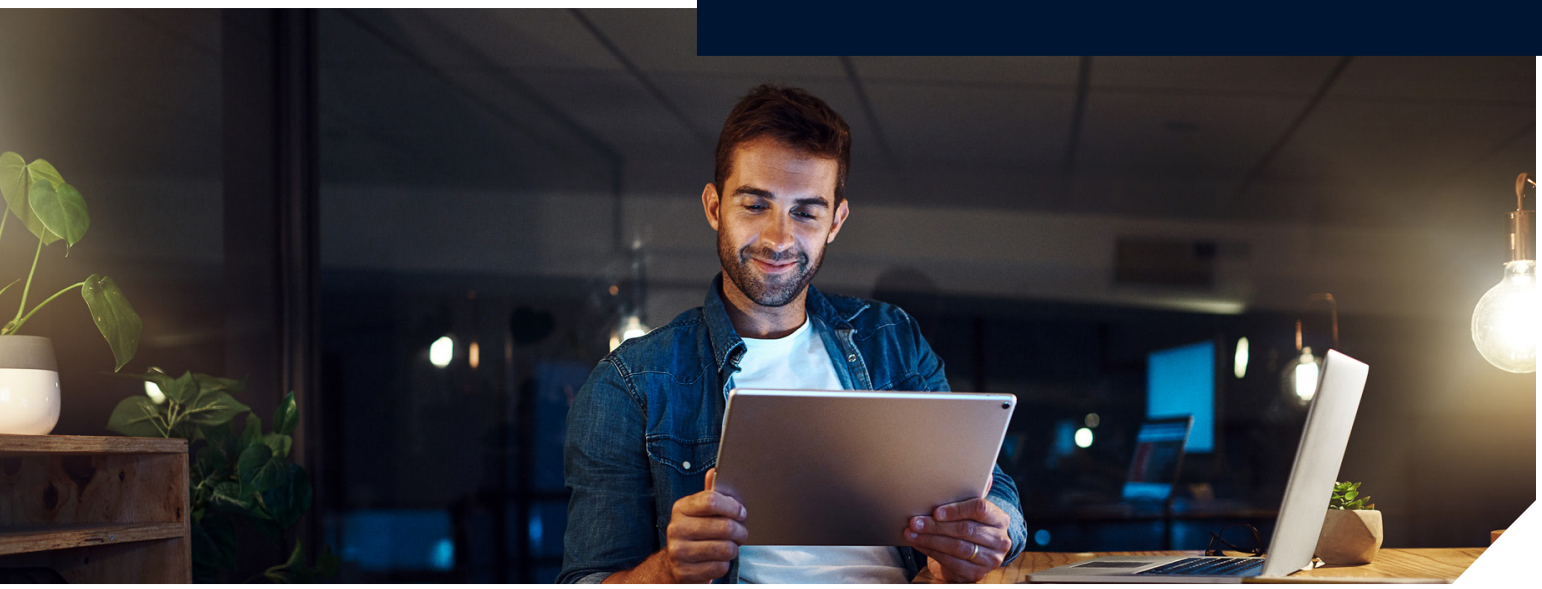
11:11 Disaster Recovery as a Service (DRaaS) and Backup as a Service (BaaS) help protect against ransomware attacks and natural disasters by maintaining multiple copies of data, including optional air-gapped copies of data, offsite in one of 11:11's secure global data centers. 11:11 Managed Security solutions help over-stretched IT staff meet rigorous security requirements with Managed Firewall, Managed Endpoint Detection and Response, Continuous Risk Scanning, and Managed Security Information and Event Management.

11:11 solutions also meet the strict criteria of numerous compliance requirements, including NIST, ITAR, and others. Take, for example, the U.S. Criminal Justice Information System (CJIS), which contains information maintained by federal law enforcement agencies, including the FBI. Local law enforcement agencies access this system for background checks and employment verifications.

BaaS

Cloud Backup

11:11 Systems can help provide the cloud, connectivity, and security services you need to keep government organizations running.



THANK YOU.

About 11:11 Systems

11:11 Systems is a managed infrastructure solutions provider that holistically addresses the challenges of next-generation managed cloud, connectivity and security.

The 11:11 model empowers customers and partners to “Rethink Connected,” which includes fully-integrated, fully-automated services, activities and data powered on a single platform delivering increased performance, optimization and savings.

North America:	+1.800.697.7088
UK:	+44 20.7096.0149
Netherlands:	+31 10.808.0440
Singapore:	+65 3158.8438
Australia:	+61 2.9056.7004

Learn more at **1111SYSTEMS.COM**

11:11 SYSTEMS