GovSense

Cybersecurity Threats are Moving at the Speed of Light

You need to move just as fast to avoid being the next victim

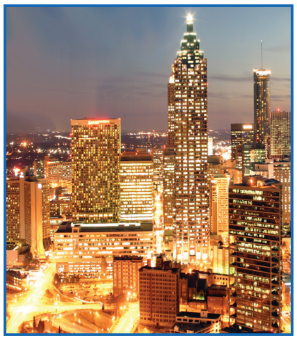
We all now know that cybersecurity issues are a global problem and not merely a local problem. Even for the smallest and most remote of government jurisdictions, however, we're past the need to follow the standard outline of the usual white papers about cybersecurity. We're not going to bother giving you the latest and greatest definitions of terms like "ransomware" and "phishing." Everyone is well aware of what these menacing terms mean. Rather, we'll get right to the point.

You can not afford to wait one more minute to take the most aggressive steps possible to protect your jurisdiction's data . . . move to a comprehensive true-cloud software solution.

We got right to the point in this article because that's the speed at which you also need to be acting to secure your data. While we understand the need to responsibly and transparently utilize your constituents' tax dollars, you can not let your outdated, lumbering procurement process slow down your ability to protect the business and personal data of all your stakeholders. How do you think your citizens will react at the next "town hall", open-public meeting if you have to tell them their data was compromised because you were operating at a 1960s-era work pace? **Business as usual is no longer an accepted excuse.**

.

The Sense of Urgency Hits Hard When It Happens in Your Own Neighborhood



At the time we're writing this white paper, the City of Atlanta has been hit with a much publicized ransomware attack that shut down many government functions. Luckily the 911 system was not affected, yet even police officers were forced to take reports with pen and paper. GovSense headquarters is located in a North Atlanta suburb in the area commonly referred to as the "technology corridor" known for its plethora and still growing population of high-tech companies. So, this serious data breach happened right in our own neighborhood, which was a sharp reality-check for us as to how vulnerable most of the jurisdictions we talk to each day really are.

Some of these local governments even admit to having experienced a cyber attack themselves with serious and long-term adversity that they will need to manage for years. It's a constant strain on already stretched budgets to add a hefty line item each year for data security. Those dollars add up fast and, in so many cases, the security expenditures leave them no better protected than they were before. This diversion of tax dollars from other much needed improvements like infrastructure, education and economic development makes it even more difficult for jurisdictions to continue to enhance and improve the lives of their citizenry. It's a "necessary evil," they say, but there is a superior and cost-effective way to defend against illicit attacks on your government's data and the personal data of your constituents.

The State-of-the-Art Security and Technical Resources Provided by True-Cloud Data Centers are at a Level No Local Jurisdiction Can Afford

Cybersecurity issues are a global problem . . .
. . . and not merely a local problem.

Let "The True-Cloud" do the work for you. Even the basic process of backing up data is more affordable in the cloud and gives you data redundancy for recovery purposes. These security costs are spread across a number of cloud customers. While we are proud to state that GovSense is the first unified, true-cloud software system designed specifically for local government, we also know that along with some bragging rights comes the responsibility to educate and make sure our customers, potential customers and our own systems are protected.

Let's look at a few of the specifics of how the **GovSense software solution provides enterprise-class data management, security and availability that helps ensure your jurisdiction is resilient to security breaches.** GovSense provides the cloud infrastructure so that you can run all your necessary applications in the cloud with complete confidence.

GovSense

Cybersecurity Threats are Moving at the Speed of Light

You need to move just as fast to avoid being the next victim

Crisis Management — All production data is stored immediately to redundant locations. “Hot backups” can restore your data rapidly and reliably. Extensive disaster recovery documents ensure crisis management is handled promptly and without fanfare.

Application Security — Advanced functionality secures the application including role-based access, strong encryption, robust password policies and more.

Operational Security — Stringent round-the-clock monitoring tools, controls and policies and a dedicated tenured security team ensure the strongest security for customers.

Data Management — Data management policies and infrastructure provide you with the peace of mind of knowing that your data is completely replicated, backed up and available whenever you need it. You enjoy reduced risk with enterprise-class data management processes and policies. Multiple levels of redundancy ensure you get continuous access to your data, and replication and synchronization across data centers provide you with the utmost disaster recovery confidence.

Availability — GovSense's redundant infrastructure enables it to provide world-class uptime, including during upgrades, averaging 99.96%.

Additional Information Sources Worth Reading:

https://www.ready.gov/cybersecurity
Department of Homeland Security

https://www.us-cert.gov/
United States Computer Emergency Readiness Team

Here’s a Reality Check for You . . .
You Can Not and Never Will be Able to Keep Up with Hackers

A reluctance on the part of affected jurisdictions to talk about the extent of their attacks prevents us from knowing the whole story and, thus, uncovering the true source and conduit for the incidents. One thing is certain, however. These data raids are coming at the speed of light and from every corner of the globe. We can’t overemphasize the sense of urgency you and everyone at your jurisdiction, no matter their role, should have to move your systems to the true-cloud to mitigate the impact a cyber attack will have on your data.

All the resources — both staff hours and budget dollars — that your jurisdiction has invested in on-premise or fake-cloud software will be wasted with just one instance of an illicit hack of your computer systems. You originally made technology investments to operate faster, provide automated services to your citizens, enhance inter-departmental collaboration and improve financial accuracy. One data security strike will bring all of this to a screeching halt. And you’ll have your constituents to answer to.

GovSense staff have years of experience with cloud technology and, in addition to the overall land and financial management benefits of the solution, we can be a ready source of expert information for understanding your vulnerabilities to cyber attack.

Please think of us as your Cybersecurity Hotline!
Call 888.824.1293 or email info@govsense.com.

Run Your Jurisdiction At the Speed of Light
How to Avoid FAKE-Cloud Systems

Use this checklist to avoid purchasing a system that is not truly in the cloud.
If the vendor’s answer is NO to any of these questions, scrap the launch and look for a True-Cloud Solution.

- **Do you host, maintain and manage your own solution?**
- **Are ALL of your current customers using the same version of your software?**
- **Are software upgrades free of charge?**
- **Is it true that consulting or implementation services are not required for software upgrades?**
- **Do you provide solutions with an open API?**
- **Can customers execute their own customizations within the system without direct database access?**