HOW-TO GUIDE

10 steps to keeping public sector data secure

Data security is one of the most persistent issues facing federal, state, and local governments—and often one of the most alarming. A data hack immediately becomes the one, all-encompassing priority that overtakes everything else. The severity of cybersecurity threats, combined with the **stunning growth** in data volumes, underscores the urgency to protect cloud data through a comprehensive certification like the Federal Risk Assessment and Management Program (FedRAMP®). **Gartner research** shows that 88% of boards regard cybersecurity as a business risk rather than solely a technical IT problem. Thirteen percent of boards have responded to this by instituting cybersecurity-specific board committees overseen by a dedicated director.

Cybersecurity is a functional need to always keep in sight. Here are get your agency on the right track. Here are several major considerations.

1. Accept that small organizations face big risks

The first step to building a cybersecure organization is to realize you're at risk. For several years now, it's been a rule of thumb among data security specialists that if you think your organization is impervious to attack—that's the first indication that you're vulnerable.

The Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem. Five key takeaways from the report include: By 2026, at least 50% of C-Level executives will have performance requirements related to cybersecurity risk built into their employment contracts.

By 2025, 60% of organizations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements.

By 2025, 50% of cybersecurity leaders will have tried, unsuccessfully, to use cyber risk quantification to drive enterprise decision-making.

By 2026, 30% of large organizations will have publicly shared environmental, social and governance (ESG) goals focused on cybersecurity, up from less than 2% in 2021.

By 2025, 40% of programs will deploy socio-behavioral principles (such as nudge techniques) to influence security culture across the organization, up from less than 5% in 2021.

2. Realize you're not alone

The list of the top 10 data breaches hitting US state and local governments shows that hackers aren't the only problem. "Some of the biggest and most significant government data breaches come down to human error: from lost hard drives, misconfigured databases, and physical device theft to simple mistakes that lead to millions upon millions of leaked Social Security numbers, names, addresses, voting affiliations, and other sensitive data," Research from **CompareTech** showed that in 2020, 79 ransomware attacks were executed against U.S. government organizations, totaling an estimated $18.88 billion in downtime and recovery costs and illustrating the severe risks that state and local governments face when it comes to cyberattacks.

The report from CompareTech how credentials continues to be compromised and pose a risk—"Lookout's Government Threat Report found more than 70 percent of phishing attacks against government organizations sought to steal login credentials, a 67 percent increase from 2019. The same report found that in 2020, one in 15 federal, state and local employees were exposed to a phishing attempt."

With remote work likely to continue, considering historically overlooked mobile devices is essential. Apps on personal and work-related mobile and other network-connected Internet of Things (IoT) devices constantly communicate with.

Something as simple as sharing a document with a compromised machine or malicious individual can lead to an opening for cybercriminals to infiltrate the network. Once on the network, a bad actor can easily move laterally and undetected through the enterprise's technology infrastructure.

Isolated, on-premises tools are no longer enough to tackle ever-evolving cyberthreats. To truly ensure secure networks, agencies must practice good cyber hygiene while investing in integrated platforms and solutions that can secure data at all access points.

Progressing into 2022, it's clear agencies must be prepared to proactively protect themselves against cyberattackers by using comprehensive security solutions capable of providing protection from endpoint devices to the cloud.

This list leaves out commercial data breaches like the well-publicized **4 Steps to Government Security** that helped bring cybersecurity to the attention of managers everywhere. And it reveals two important points: Data loss has been going on for a long time, and it affects respected, established organizations that were credible in their own right, before and after their breaches. The response is not to single them out, but to address an issue that affects every government agency at every level—because even the best organizations are being targeted.

3. Modernize your software to keep up with today's cybersecurity needs

Postponing cybersecurity planning is a mistake, but it's easy to understand how it happens. It costs money and changing something as fundamental as the way your organization protects its IT systems soaks up valuable time. But it costs far more to keep operating vulnerable legacy systems. There may be many reasons for your agency to upgrade its enterprise resource planning (ERP) and associated systems—and as those reasons accumulate into an irresistible need, enhanced security is one of the most important gains to expect from modernizing your software.

In order to maximize efficiency and reduce costs, many public agencies have stretched their financial and program management systems to the limit. At the same time, supply chains are becoming more complex. Enhanced data security is one of the best reasons to break away from old, obsolete systems that have been in place for far too long and can't meet the latest compliance standards, making cybersecurity one of many compelling reasons to upgrade.

4. Apply the same security tools across your supply chain

Today's cybersecurity challenges extend beyond in-house systems. Your system is only as strong as its weakest link, and if any part of your extended supply chain is vulnerable—you are, too. One enduring lesson from the 2013 Target data breach was that it originated with a vendor so small that it almost certainly wasn't on the security team's radar—until a small company's vulnerability became an entry point to a retail giant's business. In an era of unprecedented complexity, your supply chains likely originate 80% of the data you rely on to deliver on your mandate for public service. Securing your own systems is just the essential first step: The next challenge is to extend that protective umbrella to every piece of external data that enters your system.

5. Take advantage of cloud-based data security tools

The good news is that it isn't all about threats and potential loss. Enhanced cybersecurity is just one of the advantages you tap into when you move operations into the cloud. The emergence of smart city strategies is opening the door to wider collaboration, coordination, and optimization across service areas, agencies, and levels of government. Internet of Things (IoT) technology offers a wealth of sensor data to optimize operations and capture the most granular updates on equipment performance and material flows.

Additionally, cloud-based asset management systems help maximize the performance and extend the operating life of expensive, often specialized capital equipment and property. Across every aspect of your business, cloud computing offers greater access and efficiency, with routine, seamless updates that can keep operations more current than an on-premises system.

6. Leverage modern user experiences to keep your workforce engaged

The benefits of modern IT infrastructure are just one upgrade away and the need is acute: CFOs and CIOs regularly cite legacy systems that fall short of organizational objectives, are often out of date, and frequently hamper efficient operations.

Outdated systems can eat away at your organization's effectiveness, blocking performance improvement, limiting your access to best practices, isolating you from emerging technologies, and failing to deliver the ease of use that the next generation of millennial employees expects on the job. Modern, cloud-based solutions can deliver consumer-grade experiences that millennial users have come to expect from enterprise systems, while also staying current with upgrades to ensure that security protections are in place.

7. Meet data safety and security needs with FedRAMP authorization

FedRAMP is a one-stop resource for governments at all levels that are intent on keeping their data safe and secure. Its primary mission is to keep federal data and US citizens safe in an environment of ever-escalating threats. But the program is also open to state and local governments and commercial enterprises that are prepared to leverage its stringent authorization process to increase security, confidence, and innovation in their own cloud strategies.

Artificial intelligence (AI), machine learning (ML), and IoT have the potential to transform agency missions and drive business success—but cloud migration is a necessary first move. By choosing software solutions that provide FedRAMP authorization, you can ensure that every layer of an organization's IT structure—from the operating system to industry-specific applications to data analytics—is continuously monitored and assessed, and that new innovations are quickly integrated into a secure architecture.

8. Build an integrated framework for vendors, partners, and contractors

The Department of Defense is working to protect controlled unclassified information within supply chain and contractor networks. Expected to begin appearing as a requirement in 2020, the **Cybersecurity Maturity Model Certification** establishes five levels of progressively more rigorous security controls that operate across 14 different control families based on standards such as NIST SP 800-171, NIST SP 800-53, and ISO 27001. **According to Regulatory Comparison: CMMC vs. FedRAMP**, a FedRAMP authorization may satisfy many of the CMMC requirements. Both programs have similar control families from access control to awareness and training, from security assessment to system and information integrity. Building a deliberate, integrated framework will ensure that your vendors and partners are onboard as you embark on your cybersecurity journey.

9. Act swiftly on FedRAMP certification to avoid long-term risks

The other great reason to embrace a more cyber-secure architecture is that your clients, customers, and stakeholders are demanding it. In 2018, a survey of 374 Infor® customers across multiple industries listed innovation, security and compliance, performance and scalability, user experience and adoption, and total cost of ownership as the five top reasons to move to the cloud. The majority of the arguments against the transition had to do with system security—which is precisely where FedRAMP comes in. The certification is so complete and comprehensive that an organizations' data is probably more at risk in an internal, on-premises system than in a state-of-the-art cloud environment. The longer you delay the transition, the more serious that risk becomes.

10. Audit new controls with a 3PAO to ensure compliance

If you're thinking of FedRAMP authorization for your own operations, the first thing to understand is that you won't be out there on your own. Experienced, third-party cybersecurity advisors are available to guide the process. Once the system is in place, a Third Party Assessment Organization (3PAO) conducts an independent audit to ensure that your security controls meet FedRAMP requirements, while assisting with document development and providing ad hoc engineering support as needed. Both of these highly trained professionals are paid by the cloud services provider you select to house your data.

With online threats multiplying and changing daily, the first rule of practice for any cybersecurity professional is that no system is guaranteed foolproof. That's why Infor has invested more than $14 million to obtain FedRAMP authorization for Infor CloudSuite™ solutions, and achieved it in record time in July, 2018. Infor FedRAMP Program Executive Joe Arthur called it: "A major step towards providing our government and regulated customers the security they require without sacrificing product features and functionality." With FedRAMP authorization in place, Infor CloudSuite can provide the key to maximizing data protection and unlocking all the other advantages and efficiencies of a modern cloud operating environment.

LEARN MORE

Follow us:

641 Avenue of the Americas, New York, NY 10011

INF-2736503-en-US-0622-1