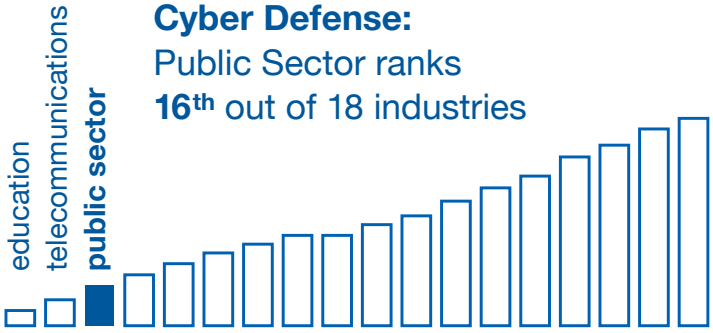
Whether it's at the state, local, or federal level, implementing the latest technology in proactive cybercrime defense can be a tall task.

The facts support an immediate need for government and public institutions to upgrade their cyber security almost more than any other industry.

A recent analysis of 552 local, state and federal agencies across the United States conducted by the risk management firm, Security ScoreCard, found that the **public sector ranked 16 out of 18 industries in terms of cyber defense –** ahead of only education and telecommunications.

It's a shocking statistic, considering the amount of priceless information contained in government databases. Social Security numbers, tax information, and private health data are just a few examples that hackers would love to steal.



Security ScoreCard's report also found that the public sector and government entities tend to struggle with basic cyber defense issues, from password reuse to data exposure and vulnerability on employees' laptops or mobile devices. Between inter-department coordination, bureaucratic red tape, and lengthy approval processes, we understand that government entities face huge logistical challenges in organizing an effective cyber defense.

The good news is that at CyberloQ, we've developed the skills, experience, and expertise geared specifically towards helping any public-sector agency – large or small – develop a proactive, iron-clad cyber defense to keep your critical information safe and secure.

CyberloQ
1.833.292.3757
info@cyberloq.com
www.cyberloq.com

Secure Multi-Factor Authentication

Advanced Credit Technologies' patent-pending CyberloQ™ technology adds a critical and effective tool to any healthcare provider's defense arsenal to guard against unauthorized access of protected resources. Rather than passively responding to a breach, CyberloQ uses Multi-Factor Authentication (MFA) to pro-actively ensure that only authorized users, on approved devices within designated locations can access your protected data.

A Perimeter of Surveillance Around Your Agency

Data protected by CyberloQ can be accessed only by those employees or patients who have been registered with the healthcare provider's secure CyberloQ enabled database. CyberloQ enabled client accounts will always be in an inactive state until the client uses their mobile device (a smartphone, laptop or tablet) and PIN functioning as part of a multi-factor authentication system to access any private or protected data resource. Public sector entities can also use CyberloQ's administrator-defined geofencing capability to ensure that the user/device is within a specified geographical perimeter before access is granted. This location can be as large as a city or, using physical beacons, as small as a room providing the ultimate perimeter surveillance scalability. If a hacker should breach the perimeter of the geofence, the account and all access is automatically disabled. This feature puts our system apart from the rest in a world where public sector data is increasingly accessed via "always-on" active accounts.

Iron Clad Government Security

We're currently developing enhancements to add additional layers of security to CyberloQ's current multi-factor authentication solution by including biometrics for the highest level of access security.

By using CyberloQ's multi-factor protection technology, public sector entities can more effectively meet government security standards, guidelines, and best practices such as those established by the National Institute of Science and Technology (NIST). In the event of a compliance check or audit, essential records are kept and stored securely in a global administrative console that is easily accessible to authorized users at any given time.

Grounded in 30+ years of experience providing domestic and international cybersecurity services for the Government, our patent-pending CyberloQ™ technology is designed specifically to provide a solution for proactive, real-time control of identity governance to protect any government or public-sector entity's private and confidential data.

Global View Console

Featuring comprehensive details and reporting for each information activation across users, devices, and locations.

- **GPS and Location Reports**
- **User Tracking Reports**
- **History Reports**
- **Activation Calendar**
- **Activation Map**

Mobile App Supports GPS and Location Permissions