How to Manage Your Bank's Cybersecurity Risk With CIS Critical Security Controls

Banks have become prime targets for cybercriminals due to the large amounts of sensitive customer data they hold. To protect this data and remain compliant with strict regulations, banks need better threat reaction times, stronger controls, and better recoverability. These can all be done by implementing CIS Critical Security Controls (CSC).

THE TOP 7 CIS CONTROLS

1 Inventory & Control of Enterprise Assets

Keep track of all assets that connect to your network, including things like security cameras and HVAC systems, because it helps your bank know what needs to be protected and how.

2 Inventory & Control of Software Assets

Keep your software up to date, limit local permission, remove and prevent unauthorized software, and only authorize certain users to access data.

3 Data Protection

Ensure sensitive data is encrypted, understand where it is stored and how it travels, and mitigate the risk of a data breach using Data Leak Protection.

4 Secure Configuration of Enterprise Assets & Software

Implementing a program for regularly patching software and operating systems to mitigate known vulnerabilities is crucial.

5 Account Management

Ensure only authorized users have access to certain data and systems for security such as core systems, data, emails, and accounts.

6 Access Control Management

Manage and monitor user access to data and systems. This includes ensuring that all access is logged, and implementing least privilege principles.

7 Continuous Vulnerability Management

Identify and remediate vulnerabilities in your systems and software including patching software/operating systems and conducting regular penetration tests.

INCORPORATE CIS CONTROLS WITH RESULTS TECHNOLOGY - RESULTS Technology can help you manage and automate many of the tasks associated with each CIS control.

www.resultstechnology.com | (913) 928-8300, *Overland Park KS* | (314) 222-2600, *Chesterfield MO*

RESULTS TECHNOLOGY