

# Country Credit Union

Jasleen Kaur  
Max Kramer  
Anthony Price  
Zach Wilson

# Country Credit Union CCU

*Country Credit Union(CCU) is a small credit union located in the hills of Southern Ohio*

- 35 Employees
- Founded in 2018
- Founded by Jonathan A. Banker

Objective:

Cyber security firm providing services to predict, prevent, and protect cyber attacks

# Access Cyber Security Firm

*Cybersecurity firm with infosec experts delivering protection through strategic collaboration for a wide range of clientele specializing within the financial sector.*

## Project Control Applications:

- Hardware Inventory & Control
  - Security Awareness & Training Program
  - Use of Administrative Privileges
  - Data Recovery Capabilities
-

# Asset Protection:

- Customer Basic Contact Info
- Financial profiles
- Trade, Selling, and Investment Information
- Access to Financial Products, Commodities, and Currency

## CIS Control 4: Controlled Use of Administrative Privileges

### Planning:

Consider the level of difficulty of password requirements and other authentication systems especially for large portfolio clients, inventors, and traditional customers

### Risk Assessment:

High volume communication with vendors, consumers, investors, and financial stakeholder allows for a blindspot to be when a privileged user may open a malicious email attachment.

Privileged administrator also are at risk when opening a file from a malicious website, rousing their browser for financial updates or other browser usage and the website hosting attacker content that can automatically exploit browsers several steps from being able to access administrative passwords and client sensitive financial data.

# CIS Control 4: Controlled Use of Administrative Privileges

## Implementation:

Nine Step comprehensive password creation

Requirement, authentication, safeguard practice for all administrators, and active users

## Benefit:

Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities

Protect the integrity, contact information, financial portfolio, and access to large quantities of funds

# CIS Control: Hardware Inventory & Control

## Planning

- *Simple to implement*
- *Low cost*
- *Minimal additional staff*
- *Very effective*

## Implementation

- *Network Scan*
- *Maintain detailed control of assets on environment*
- *Configure Automatic Network Scanning*

# CIS Control: Hardware Inventory & Control

## Benefit

- Allows an organization to monitor all devices on network
- Control access to networks
- Makes network management easier



# CIS Control 17 Implement Security Awareness and Training Program

## Planning:

Identify the specific KSA's needed to protect the enterprise

Develop security training that is congruent with the roles and responsibilities of different employees

Identify the security protocols that are currently in place and prioritize additional security protocols accordingly

Conduct a Risk Assessment to identify the most prominent vulnerabilities that can be resolved with proper security measures and protocols

## Risk Assessment:

- CIS Risk Assessment Method
- Skills Gap Analysis
- Tiered Training

## **CIS Control 17** Implement Security Awareness and Training Program

### **Implementation:**

Deliver educational training to fill skills gap identified during the Skills Gap Analysis

Engaging and informative trainings that stresses the importance of the security protocols taught

Trainings should be updated regularly as new threats are identified as well as any relevant business or legal standards

Employees should feel discouraged from engaging in any “shortcuts” relative to security procedures by stressing the importance of security controls

### **Benefit:**

Introducing the necessary knowledge required for maintaining a robust cyber defense posture is crucial in mitigating identified risks and vulnerabilities

Employees educated in proper security protocols will reduce the likelihood of threat actors gaining access to any sensitive data

# CIS Control 10: Data Recovery Capabilities

## Planning:

- Why?
- Where?
- How often?

## Risk Assessment:

- Not “if” but “when”
- Changes from attackers range from obvious to subtle
- Protect critical data and save time on recovery

# CIS Control 10: Data Recovery Capabilities

## Implementation:

- All data backed up at regular intervals
- Test integrity of backup data
- Backup data protected
- At least one offline backup

## Benefit:

- Safety net
- Time saved
- Be sure all traces of attack are removed from system

# Expected Outcome

- Robust security defense posture
- Well trained workforce capable of identifying and mitigating risk by increasing awareness surrounding social engineering tactics and cyber attack trends
- Incident Response and Recovery capabilities

# Reference Page

Secure Set (n.d) Sca Hunt 300-2 CIS Back 10 PDF, Retrieved March 2021

CIS. (n.d). The 20 CIS Controls & Resources. Retrieved March 22,2021, from <https://www.cisecurity.org/controls/cis-controls-list/>

