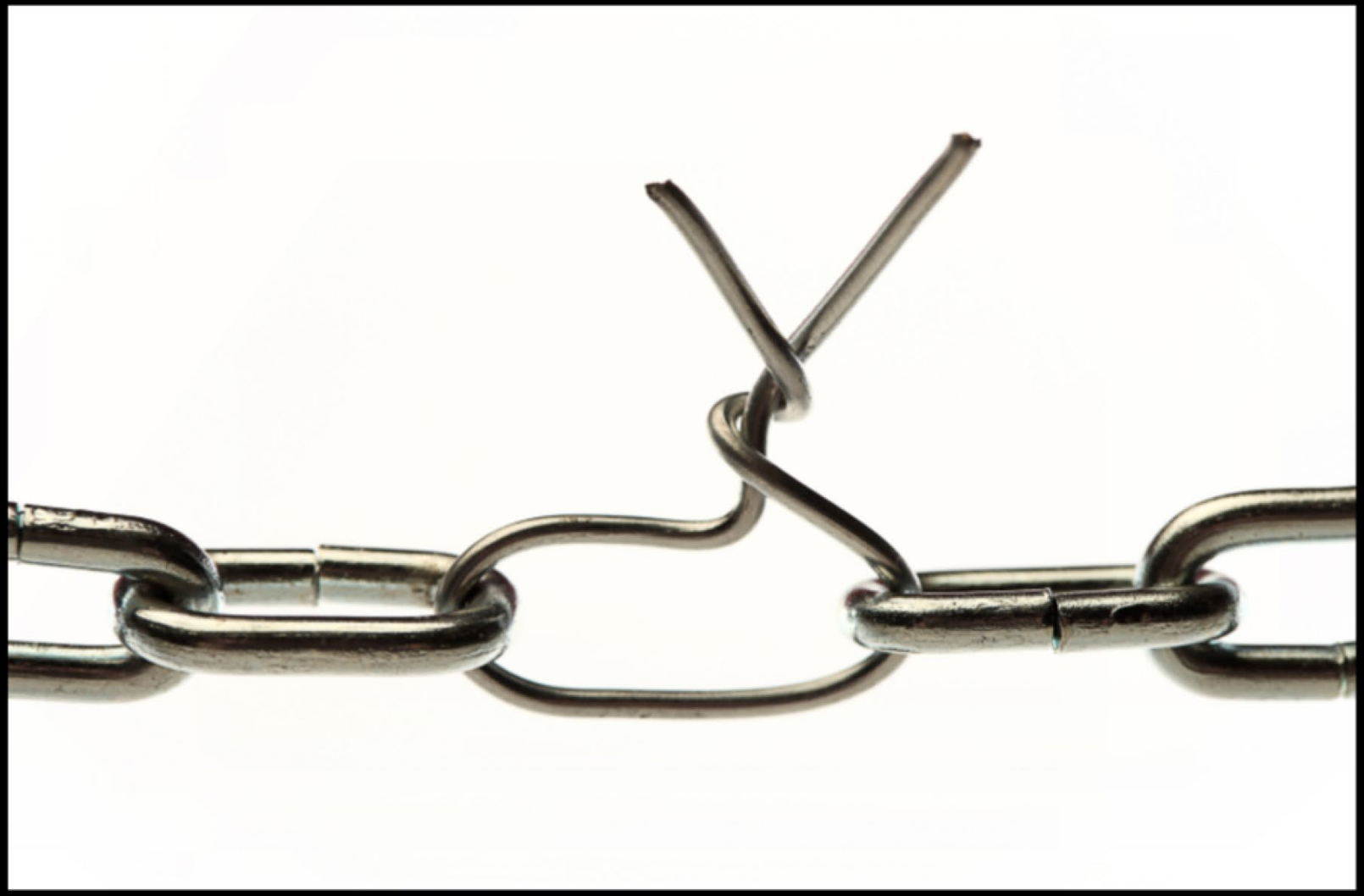
INFORMATION TECHNOLOGY SERVICES

METROPOLITAN STATE UNIVERSITY℠
OF DENVER


THE COURAGE
TO BE VULNERABLE


Vulnerability is the
birthplace of innovation,
creativity and change.
Brené Brown
quotefancy



VULNERABILITY MANAGEMENT

One weakness is all it takes.

Vulnerability Management

- CIS Controls – Version 7.1
- Basic Controls
  1) Inventory & Control of H/W Assets
  2) Inventory & Control of S/W Assets
  3) Continuous Vulnerability Management
  4) Controlled Use of Admin Privileges
  5) Secure H/W & S/W Configuration
  6) Log Maintenance, Monitoring, and Analysis

Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers

- Software updates
- Patches
- Security Advisories
- Threat Bulletins

Continuous VM Sub-Controls

3.1 - Run Automated Vulnerability Scanning Tools

3.2 - Perform Authenticated Vulnerability Scanning

3.3 - Protect Dedicated Assessment Accounts

3.4 - Deploy Automated O/S Patching Tools

3.5 - Deploy Automated S/W Patching Tools

3.6 - Compare Back-to-Back Vulnerability Scans

3.7 - Utilize a Risk-Rating Process

Tools We Use

- Nessus
- InsightVM/Nexpose
- SCCM and Jamf
- UT Austin Dorkbot Service
  - https://security.utexas.edu/dorkbot

Related Tools

- InsightIDR
- PAN Events and Feeds
- DNS Firewall
- Endpoint Alerts
- O365 Alerting
- Security Feeds and Alerts

THANK YOU