NDBT

TEXAS ★ BANKING ★ ORIGINAL

2024 Cybersecurity Event

Heath Stanley

Owner | President | CISO, Curated Cyber

- **Alumni of Texas Tech University, Class of 2006**
- **Over 16 years of dedicated experience across various technology domains – from humble dumpster diving beginnings to the ownership of a cybersecurity consultancy.**
- **Spanning more than a decade as a Chief Information Security Officer, Heath has made significant strides in the realm of data protection.**

Certifications

- **CISSP**
- **Certified Incident Handler**
- **CISA**
- **C|CISO**
- **Certified Regulatory Vendor Management Professional**

Top Cyber Threats and Mitigations

Presented By:

CURATED CYBER
A CISOaaS FIRM

About Me

Heath Stanley

Owner/President/CISO at Curated Cyber

C|CISO, ITIL v3, C|EH, CSAP

Founded in 2022, fractional vCISO since 2015.

Primarily vCISOs for community banks, law firms and consultancies

---

Recognized industry expert in the fields of cybersecurity, risk management, governance, incident response and business continuity. Work closing with community banks, law firms, and software develop shops, FBI, and Cyber Insurance Co's.

I own a business and am raising a 6 year old to be a man.
My golf handicap is going up...but I still love golf.

OVERVIEW

- Cyber Threats & How to Mitigate Them
- Practical Mitigation Techniques
- Funny and Scary Stories
- Minimal Dad Jokes

CURATED CYBER
A CISOaaS FIRM

CIA Triad & Risk Management

- Confidentiality
- Integrity
- Availability

CURATED CYBER
A CISOaaS FIRM

TOP CYBER THREATS

1. Phishing Attacks / Social Engineering
2. Ransomware Attacks
3. Credential Stuffing and Account Takeover (ATO) Attacks
4. Cloud Security Threats
5. Improperly Handled Data Breaches/Events
6. Insider threats / Configuration Mistakes
7. Third-party Vendor Risk
8. Unpatched and Outdated Systems
9. Weak passwords and multi-factor authentication (MFA)
10. IoT Vulnerabilities

CURATED CYBER
A CISOaaS FIRM

Phishing Attacks/Social Engineering

- Phishing (Most common, Email)
- Spear Phishing/Whaling
- SMSishing
- Quishing (QR Code Phishing)

As a small/medium sized entity, there is a 50/50 chance of a breach.
92% chance that breach is email or via email.

CURATED CYBER
A CISOaaS FIRM

Phishing Attacks - Mitigation

- Awareness Training
  - How to Identify
  - Treat every email as if it is a **phishing attempt.**
  - Allow people to ask!!!

- Technical Controls
  - Email Filtering
  - Implement MFA
  - Email Gateway
  - IPS/IDS

- Operational Controls
  - Phishing Campaigns (KnowBe4, PhinSecurity)

CURATED CYBER
A CISOaaS FIRM

Ransomware Attacks

A form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable

CURATED CYBER
A CISOaaS FIRM

Ransomware Attacks - Mitigation

Harden the endpoints	Keep systems up-to-date	Maintain backups – thoughtfully	Implement an IDS/IPS	Network Segmentation
ACLs	Firewall	Cyber Insurance	AV / Anti-malware software	Have an Incident Response Plan
Conduct a Ransomware Roundtable Exercise	SIEM	Monthly ITSC	Schedule regular employee training	External Audit / Penetration Test

CURATED CYBER
A CISOaaS FIRM

Credential Stuffing and Account Takeover (ATO) Attacks

Credential stuffing is a type of cyberattack in which a cybercriminal uses stolen usernames and passwords from one organization (obtained in a breach or purchased off of the dark web) to access user accounts at another organization.

Anatomy of a credential stuffing attack

CURATED CYBER
A CISOaaS FIRM

Credential Stuffing and ATO Attacks - Mitigation

- Multi-Step Login Processes
  - Multi-Factor Authentication
- Use unique passwords for each service
- Limit authentication requests and set up for failed request alerts
- Require Users to Solve a CAPTCHA
- Web Application Firewall (WAF)
  - multiple login requests
  - unfamiliar IP addresses
- Password Vaults

CURATED CYBER
A CISOaaS FIRM

Cloud Security Threats

- As entities move to cloud services for better efficiency and scalability, they face risks related to secure data storage and potential data leakage, along with the security practices of their cloud service providers.
- Security system misconfiguration
- Denial-of-Service (DoS) attacks
- Data loss due to cyberattacks
- Unsecure access control points
- Inadequate threat notifications and alerts

CURATED CYBER
A CISOaaS FIRM

Cloud Security Threats-Mitigation

- Implement Identity & Access Management
- Use a trusted Cloud service
- Encrypt the Data in transit and at rest
- Properly Configure Security Groups
- Implement Cloud Security Monitoring and Logging
- Conduct Security Audit & Penetration Tests
  - AND deploy the findings
- Use an MSSP with a Security Operations Center

CURATED CYBER
A CISOaaS FIRM

Data Breach

A data breach is any security incident that results in unauthorized access to confidential information.

CURATED CYBER
A CISOaaS FIRM

Data Breach-Mitigation

Incident Response Plan

Have a Plan!

- Exercise the Plan
- Train users on their roles and responsibilities
- Timeliness of notification is key!

Contain

- Quarantine systems by turning off wifi/ethernet or intelligent EDR tools
- Change Passwords, potentially for more than the single affected users

Eradicate and Recover

- Wipe, harden, retest affected hardware and software
- Restore data
- Test before redeployment

CURATED CYBER
A CISOaaS FIRM

Data Breach-Mitigation

Incident Response Plan

Document and Enhance

- Follow Chain of Custody
- Follow the plan
- Document Actions
- Hold Lessons Learned meetings and deploy controls
- Educate users on the event

Cyber Insurance

- Know your deductible amounts
- Use insurance approved vendors before claim
- Make a claim and turn it over to professionals

CURATED CYBER
A CISOaaS FIRM

Insider Threats / Configuration Mistakes

- Insider threats are threats that come from within an organization, such as employees or contractors. Insider threats can be intentional or unintentional.

- Intentional
  - Theft or Sabotage
    - Emailing to themselves
    - USB/External Hardrives
    - Open websites
  - Fraud (invoice, micro payments, ‘expenses’

- Unintentional
  - Phishing scam
  - Technical Misconfigurations

CURATED CYBER
A CISOaaS FIRM

Insider Threats / Configuration Mistakes-Mitigation

- Implement Strong Access Controls
- Background Check
- Monitor Employee Activity
- Block filesharing/webemail
- Block USBs/external harddrives
- Have a Plan for responding to Insider Threats
- HR Practices
  - Change/Separation Management
  - Hire Competent Staff
  - Sign Acceptable Use Policies

CURATED CYBER
A CISOaaS FIRM

Third-Party Vendor Risk

- Data Breaches
- Compliance Issues
- Operations Disruptions
- Reputational Damage

CURATED CYBER
A CISOaaS FIRM

Third-Party Vendor Risk - Mitigation

Third-Party Risk Management (TPRM):
the process of identifying, assessing, and mitigating the potential risks posed by third-party vendors.

- Vendor Management Policy
- Vendor Criticality Analysis
- Critical Vendor Annual Risk Review

- Use trusted/vetted vendors
- Have exit plans for high risk vendors
- Incorporate into your incident plans

CURATED CYBER
A CISOaaS FIRM

Unpatched and Outdated Systems

Cybersecurity risks are heightened when businesses operate with outdated software or fail to apply security patches in a timely manner, leaving systems vulnerable to exploitation.

Once Windows server 2012 was unsupported 72+ vulnerabilities were found/announced within 1 day.

CURATED CYBER
A CISOaaS FIRM

Unpatched and Outdated Systems - Mitigation

- Patch Management
  - Patch all systems
  - Autoapply security and critical patches
  - Patch third party tools
    - Adobe, Java, Browsers, etc.
- Vulnerability Scanning
  - Scan Internally/Externally
  - Remediate all critical/high findings

- Proactively plan for End of Life systems
  - Save $$$

CURATED CYBER
A CISOaaS FIRM

Weak passwords & multi-factor authentication (MFA)

Weak passwords are one of the biggest security threats. Many people use easy-to-guess passwords, such as their name, birthday, or common words. This makes it easy for attackers to crack their passwords and gain access to their accounts.

CURATED CYBER
A CISOaaS FIRM

Weak passwords

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

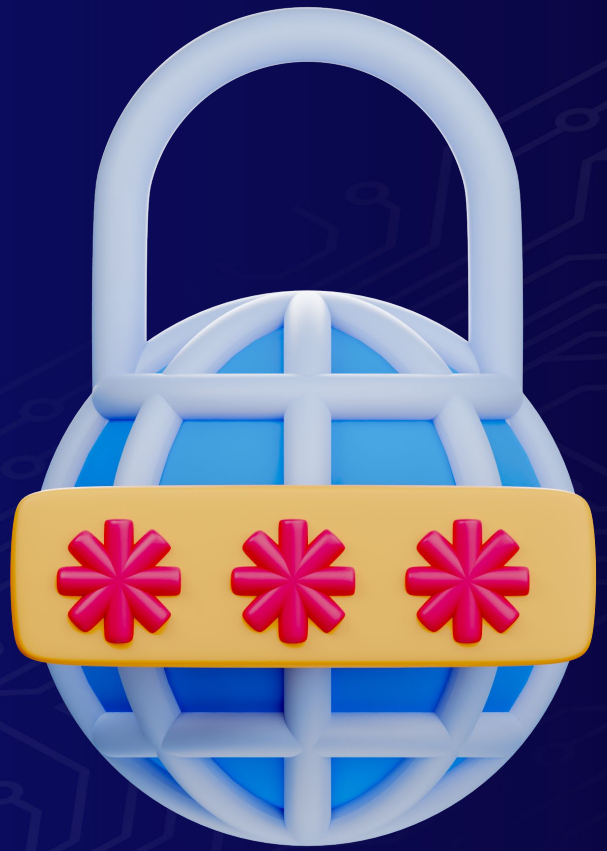
HIVE SYSTEMS

Cybersecurity that's approachable.
Find out more at hivesystems.io

CURATED CYBER
A CISOaaS FIRM

Weak passwords and MFA - Mitigation

- Enforce strong password policies
- Prohibit the use of common passwords
- Avoid password reuse
- Password Managers
- End User Awareness Training
- Authentication App MFA
  - Everywhere you can!



CURATED CYBER
A CISOaaS FIRM

IoT Vulnerabilities

How do you hack a casino through a fishtank?

- Insecure communication protocols
- Outdated firmware
- Lack Security Features
- Default Passwords
- Consumer Grade tools in the business

CURATED CYBER
A CISOaaS FIRM

IoT Vulnerabilities - Mitigation

- Change default passwords
- MFA… Maybe
- Update the firmware regularly
- Network Segmentation
- Enable Encryption

CURATED CYBER
A CISOaaS FIRM

What can we do?

- Plan to Fail Well via Risk Assessments and Audits
- Bridge the gap between business, IT, compliance and governance
- Risk Management (Patch Management, Admin Management, MFA, Passwords, Least Privilege, AV, IDS/IPS) Reporting, and monthly health checks
- Information Security Awareness Training
- Technology Polices
- Vendor Management
- Business Continuity / Disaster Recovery
- Incident Response
- Cyber Insurance

CURATED CYBER
A CISOaaS FIRM

Information Security Awareness Training

- Provide regular security awareness training to all employees
- Make it FUN!!
- Make it Entertaining
- Real World Scenarios
- Demystify cybersecurity… It’s mostly common sense
- Humor and Storytelling
- Rewards & Recognition

CURATED CYBER
A CISOaaS FIRM

Closing Thoughts

G.I. JOE
KNOWING IS HALF THE BATTLE

CURATED CYBER
A CISOaaS FIRM

CURATED CYBER

A CISOaaS FIRM

Simplifying your cybersecurity journey

heath@curatedcyber.com

Connect with us: LinkedIn

NDBT

TREASURY MANAGEMENT

NDBT
TREASURY MANAGEMENT

Fraud Mitigation

Positive Pay

Protects against fraudulent or altered checks

- Enhanced security
- More control
- Peace of mind
- Save money by avoiding or reducing
  - Financial losses
  - Fraud investigation fees
  - Destroying checks from compromised account and re-ordering checks on new account

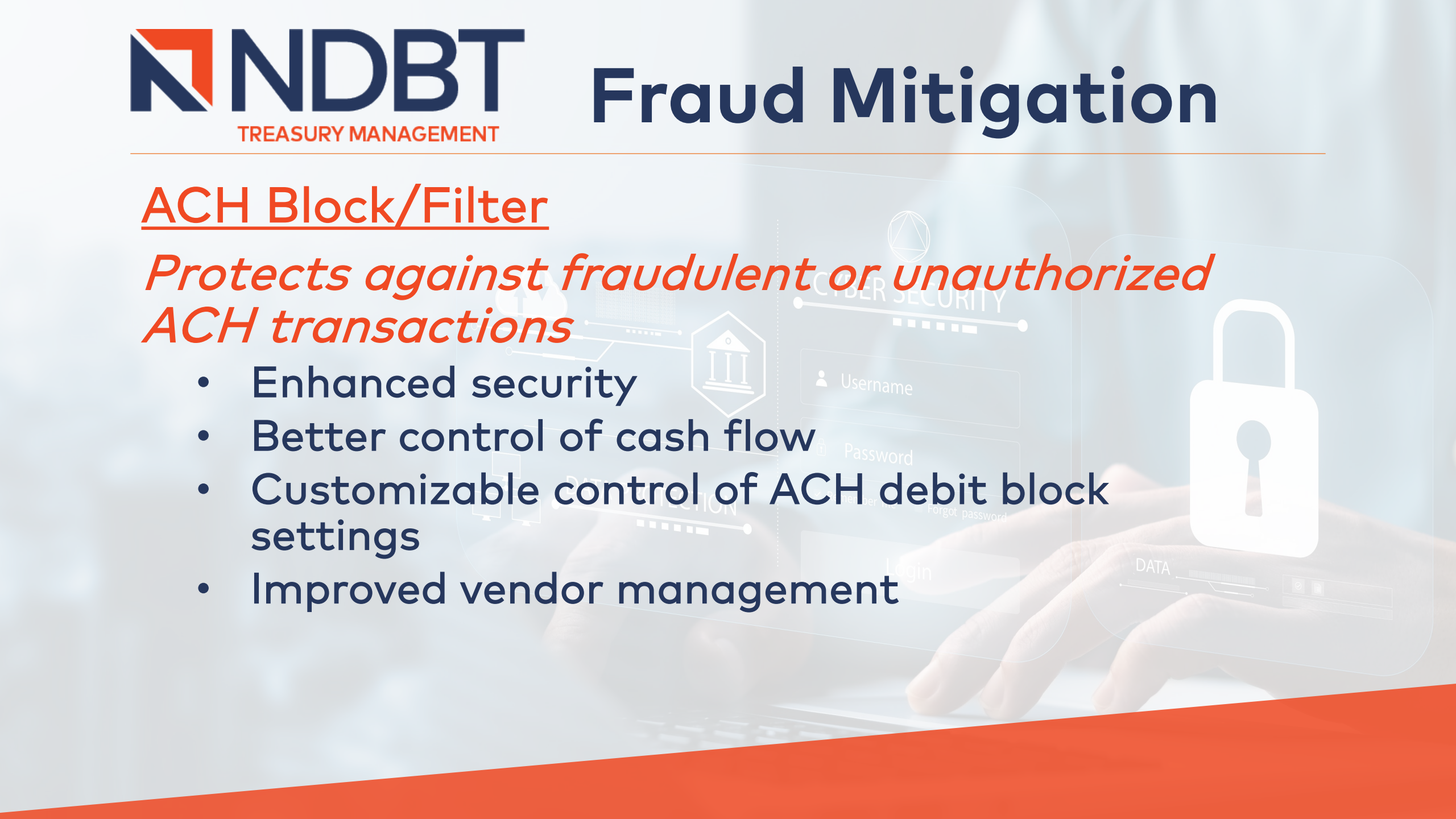
NDBT
TREASURY MANAGEMENT

Fraud Mitigation

ACH Block/Filter

Protects against fraudulent or unauthorized ACH transactions

- Enhanced security
- Better control of cash flow
- Customizable control of ACH debit block settings
- Improved vendor management



Thank you!

NDBT

TEXAS ★ BANKING ★ ORIGINAL