TOP 10 CYBER THREATS & HOW TO MITIGATE THEM

Presented By:

CURATED CYBER
A CISOaaS FIRM

About Me

Brandon Gettert

Founder | CEO Curated Cyber

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

Fractional Information Security Officer

vISO/vCISO/VISO

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.

**My hobbies are Foosball & Listening to 90's Music loud while playing foosball. Nothing else.*

OVERVIEW

- Cyber Threats & How to Mitigate Them
- Practical Mitigation Techniques
- Other Best Practices

CURATED CYBER
A CISOaaS FIRM

TOP 10 CYBER THREATS & HOW TO MITIGATE THEM

1. Phishing Attacks / Social Engineering
2. Ransomware Attacks
3. Credential Stuffing and Account Takeover (ATO) Attacks
4. Cloud Security Threats
5. Data Breach
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 Unpatched and Outdated Systems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

CIA Triad & Risk Management

- Confidentiality
- Integrity
- Availability

CURATED CYBER
A CISOaaS FIRM

Phishing Attacks/Social Engineering

- Phishing (Most common, Email)
- Spear Phishing
- Smishing
- Quishing (QR Code Phishing)
- Vishing
- In Person

CURATED CYBER
A CISOaaS FIRM

Phishing Attacks & Social Engineering-Mitigation

- Awareness Training
  - How to Identify
  - Treat every email as if it is a **phishing attempt.**
  - Tips and Tricks

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

- Operational Controls
  - Phishing Campaigns (KnowBe4, PhinSecurity)
  - Audit

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

CURATED CYBER
A CISOaaS FIRM

Cloud Security Threats

- As banks 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

- Assess and Prioritize Risks
- Implement Identity & Access Management
- Encrypt the Data
- Properly Configure Security Groups
- Implement Cloud Security Monitoring and Logging
- Conduct Security Audit & Penetration Tests
- Establish and Incident Response Plan
- Get an MSSP

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

Prevention:

Implement Strong Access Controls

Regularly Update Software and Systems

Educate Employees on Cyber Awareness

Implement Security Monitoring and Logging

Encrypt Sensitive Data

Detection:

Establish Breach Detection Rules

Implement Security Incident and Event Management (SIEM) Tools

Regularly Review Security Logs and Alerts

Conduct Regular Security Audits and Penetration Tests

Incident Response:

Contain the Breach

Assess the Breach

Notify Affected Individuals

Report the Breach to Authorities

Remediate the Breach

Review and Enhance Security Measures

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

- Unintentional
  - Phishing scam
  - Technical Misconfiguration

CURATED CYBER
A CISOaaS FIRM

Insider Threats / Configuration Mistakes-Mitigation

- Implement Strong Access Controls
- Background Check
- Monitor Employee Activity
- Educate Employees About Insider Threats
- Have a Plan for responding to Insider Threats
- HR Practices
  - Change Management
  - Hire Competent Staff

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

CURATED CYBER
A CISOaaS FIRM

Unpatched and Outdated Systems

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

CURATED CYBER
A CISOaaS FIRM

Unpatched and Outdated Systems - Mitigation

- Patch Management
- Vulnerability Scanning
- Audit

CURATED CYBER
A CISOaaS FIRM

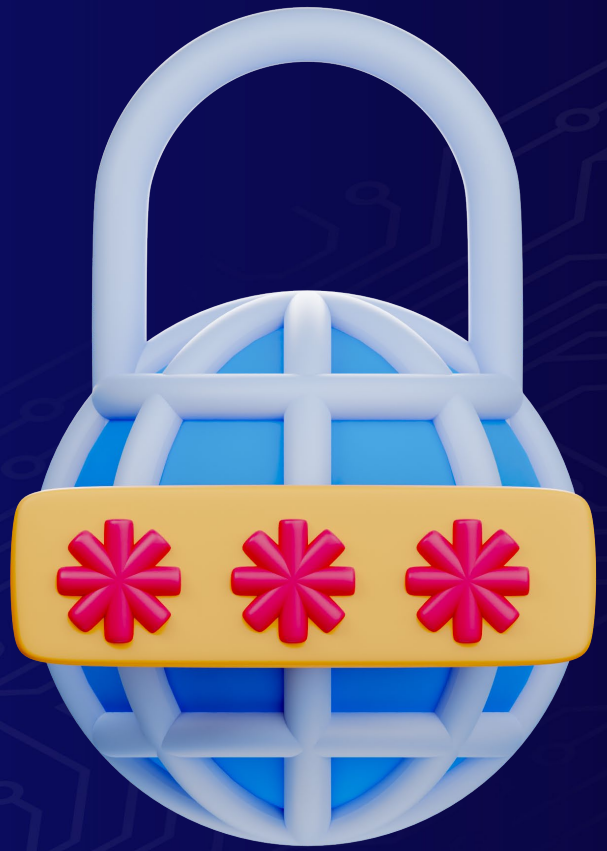
Weak passwords & multi-factor authentication (MFA)

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 and MFA - Mitigation

- Enforce strong password policies
- Prohibit the use of common passwords
- Avoid password reuse
- Password Managers
- End User Awareness Training



CURATED CYBER
A CISOaaS FIRM

IoT Vulnerabilities

- Insecure communication protocols
- Outdated firmware
- Lack Security Features

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 as a business?

- Roll out a governance program
- Plan to Fail Well
- 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
- IT Strategic Planning
- Cyber Polices
- Vendor Management
- Business Continuity / Disaster Recovery
- Incident Response
- Cyber Insurance
- Verizon Data Breach Report - Brandon's take aways
  - 82% of breaches involved a human element.
  - 80% external actors, 20% internal.

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

- Other Threats not discussed: Poor Cyber Hygiene, AI, Malware, Zero Day, etc..
- Let's plan to fail well. Incident Response. Our Systems and Vendors will fail us. Let’s prepare.
- Hire a qualified cybersecurity professional (vCISO). If your bank does not have a dedicated cybersecurity professional, consider hiring one or outsourcing your cybersecurity needs to a managed security service provider (MSP/MSSP).
- Test your cybersecurity defenses regularly. Conduct regular penetration tests and vulnerability assessments to identify and remediate security weaknesses.
- Keep up with the latest cybersecurity threats and trends. Stay informed about the latest cybersecurity threats and trends by reading industry publications and attending conferences.

G.I. JOE

KNOWING IS HALF THE BATTLE

CURATED CYBER
A CISOaaS FIRM

CURATED CYBER

A CISOaaS FIRM

Simplifying your cybersecurity journey

vciso@curatedcyber.com

Connect with us: LinkedIn