VIRGINIA
IT AGENCY

Risk Assessment Workshop

VITA Risk Management

Matt Steinbach
matthew.Steinbach@vita.virginia.gov

Today’s Objectives

1 Understand risk and how it is assessed

2 Identify components of risk, including threats, and vulnerabilities

3 Workshop risk designations

4 Understand impacts of social engineering

What is risk and how is it assessed?

What is a Risk?

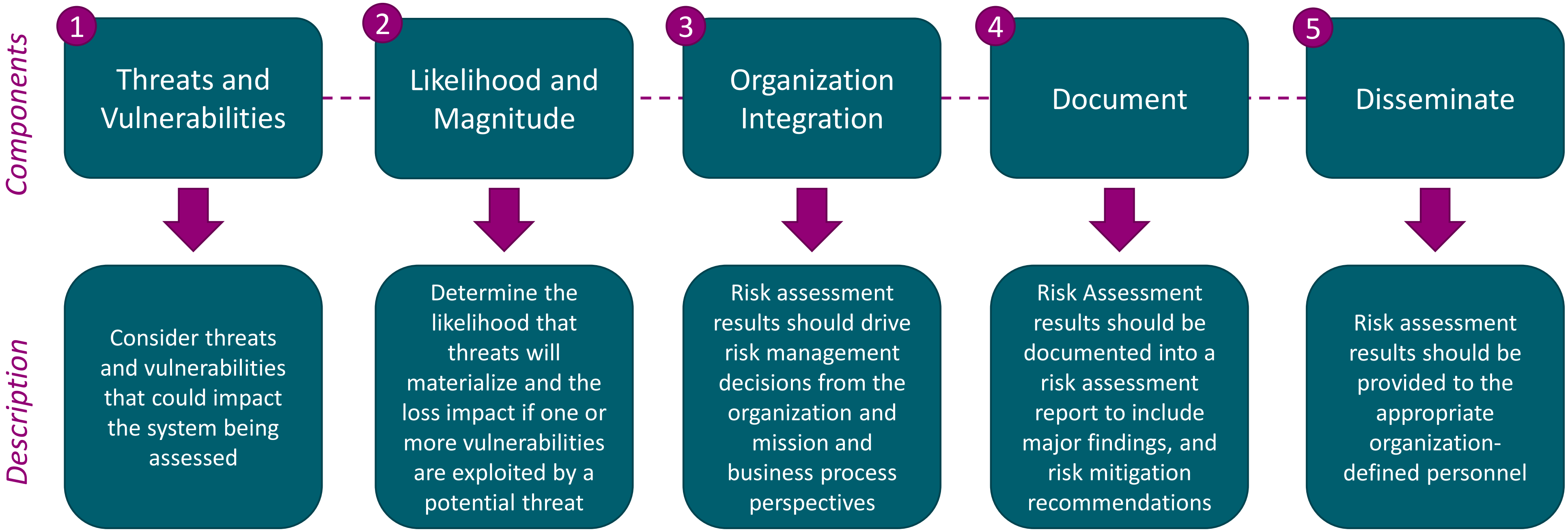
- A measure of the extent to which an entity is threatened by a potential circumstance or event.
- It is the combination of the likelihood of a threat occurring and the impact it would have if it did.

How to determine what risks should be considered?

- Organization level brainstorming and workshopping
- Review historical data and past incidents
- Scenario Analysis: What-ifs
- Enterprise-wide Risk Register

Organizations conduct risk assessments to determine risks that are common to the organization's core missions, business processes, infrastructure services, or information systems.

Requirements of a Risk Assessment



Components

1. Threats and Vulnerabilities
2. Likelihood and Magnitude
3. Organization Integration
4. Document
5. Disseminate

Description

1. Consider threats and vulnerabilities that could impact the system being assessed
2. Determine the likelihood that threats will materialize and the loss impact if one or more vulnerabilities are exploited by a potential threat
3. Risk assessment results should drive risk management decisions from the organization and mission and business process perspectives
4. Risk Assessment results should be documented into a risk assessment report to include major findings, and risk mitigation recommendations
5. Risk assessment results should be provided to the appropriate organization-defined personnel

RAs should be reviewed on an annual basis, and fully revised every three (3) years.

SEC530-01.0 , 6.1

Threats and Vulnerabilities

A threat is any potential danger or harm that could compromise the confidentiality, integrity, or availability of an organization’s information systems, data or networks

- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- PASTA (Process for Attack Simulation and Threat Analysis)
- MITRE ATT&CK
- DREAD

A vulnerability is a weakness or flaw in a system, application, or network that could be exploited by a malicious actor to gain unauthorized access, disrupt operations, or steal data

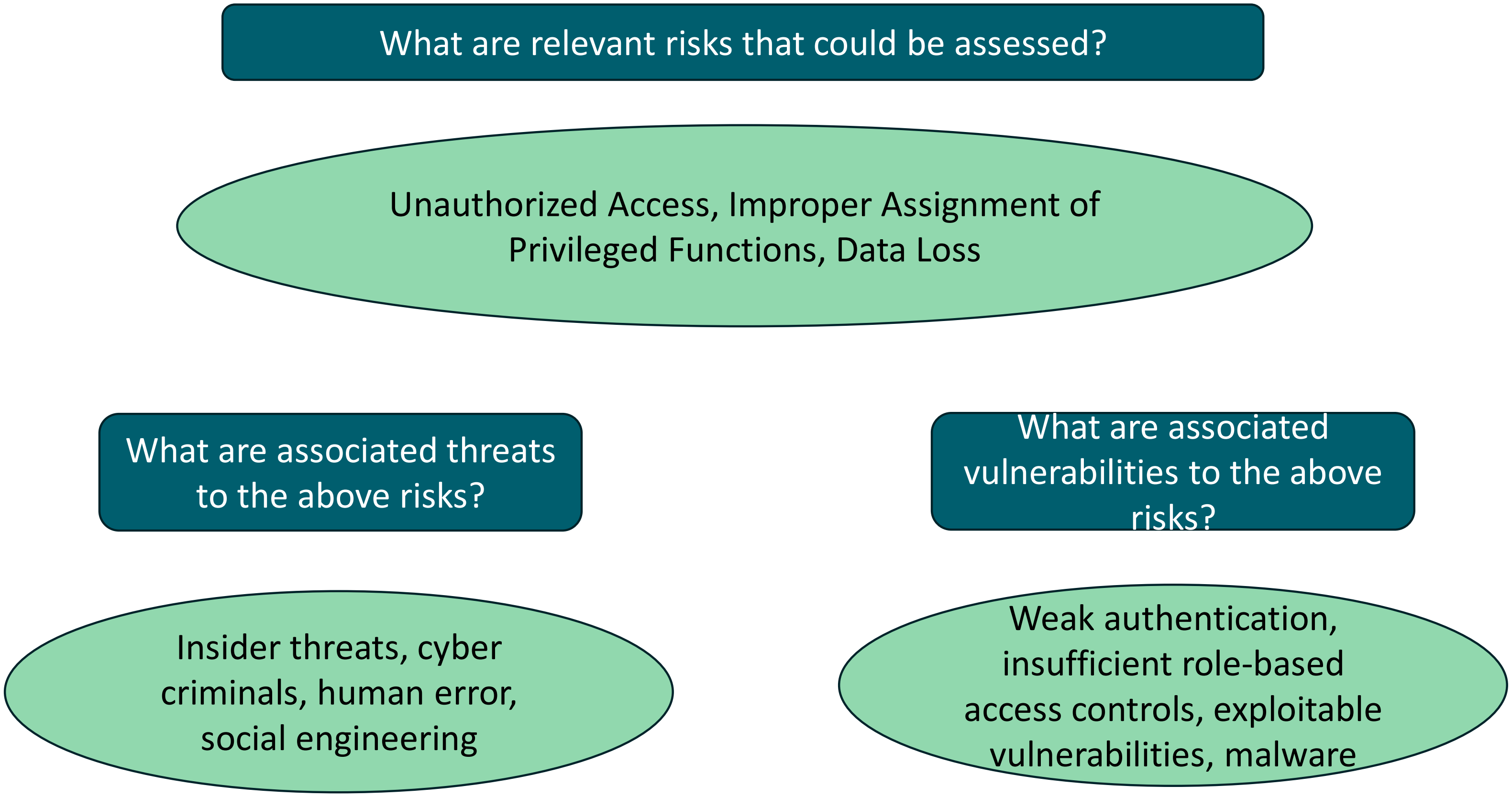
- OWASP Top Ten
- CIS Top Eighteen

Calculating Risk

Rating	Magnitude of Impact	Probability of Occurrence
Critical	Direct high impact such as mission essential functions unavailable and/or complete breach of sensitive information	There are no other controls in place that mitigate the risk and existing threats capable of exploiting the gap
High	Direct impact such as a temporary suspension of services or the loss of a subset of information	Few, if any, internal controls are in place to reduce the risk
Medium	Indirect impact	Internal controls reduce the threat; however, additional controls should be implemented to further mitigate the risk where feasible
Low	Indirect minimal impact	There are sufficient controls in place to substantially reduce the risk posed

Probability of Occurrence	Magnitude of Impact			
	Low	**Moderate**	**High**	**Critical**
Critical	High	High	Critical	Critical
High	Moderate	High	High	Critical
Moderate	Low	Moderate	High	High
Low	Low	Low	Moderate	High

Example: Information System Contains Confidential Information Such as Social Security Numbers



What are relevant risks that could be assessed?

Unauthorized Access, Improper Assignment of Privileged Functions, Data Loss

What are associated threats to the above risks?

Insider threats, cyber criminals, human error, social engineering

What are associated vulnerabilities to the above risks?

Weak authentication, insufficient role-based access controls, exploitable vulnerabilities, malware

Example: An Information System Contains Confidential Information Such as Social Security Numbers

Risks of unauthorized access, improper assignment of privileged functions, and data loss have been identified. Key components of the Risk Assessment include the following:

What is the magnitude of impact?

What is probability of occurrence?

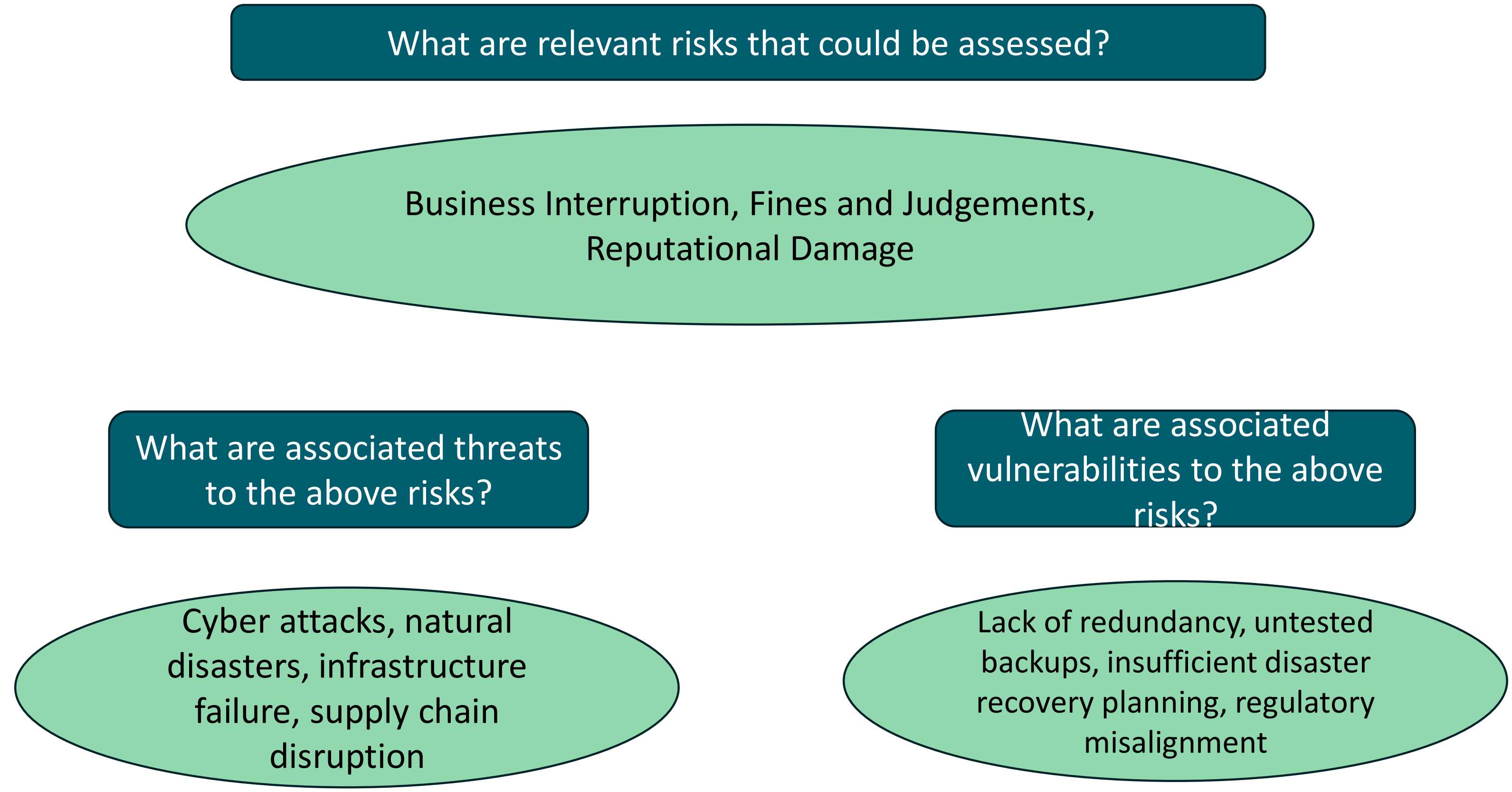
What is the total risk?

Risk	Factors to Consider	Magnitude	Probability	Total
Unauthorized access	Weak passwords	High	High	High

Risk	Factors to Consider	Magnitude	Probability	Total
Improper assignment of privileged functions	Strong Role Based Access	High	Low	Moderate

Risk	Factors to Consider	Magnitude	Probability	Total
Data Loss	Strong backups, Vulnerabilities present	High	Moderate	High

Example: Information System Supports an Agency Mission Essential Function



What are relevant risks that could be assessed?

Business Interruption, Fines and Judgements, Reputational Damage

What are associated threats to the above risks?

Cyber attacks, natural disasters, infrastructure failure, supply chain disruption

What are associated vulnerabilities to the above risks?

Lack of redundancy, untested backups, insufficient disaster recovery planning, regulatory misalignment

Example: An Information System Supports an Agency Mission Essential Function

Risks of business interruption, fines and judgements, and reputational damage have been identified. Key components of the Risk Assessment include the following:

What is the magnitude of impact?

What is probability of occurrence?

What is the total risk?

Risk	Factors to Consider	Magnitude	Probability	Total
Business Interruption	Robust Contingency Plan	High	Low	Moderate

Risk	Factors to Consider	Magnitude	Probability	Total
Fines and Judgements	Poor regulatory compliance	High	Critical	Critical

Risk	Factors to Consider	Magnitude	Probability	Total
Reputational Damage	Insufficient Disaster Recovery Plan	High	High	High

Example: An Information System Contains Accounting Information and is Third Party Hosted

What are relevant risks that could be assessed?

Loss of Data Integrity, Third Party Cyber Security Exposure, Reliance on Third Party

What are associated threats to the above risks?

Compromised Vendor, Malicious Threat Actors, Human Error

What are associated vulnerabilities to the above risks?

Poor data validation, misconfigurations, unpatched software, lack of visibility into vendor

Example: An Information System Contains Accounting Information and is Third Party Hosted

Risks of Loss of Data Integrity, Third-Party Cybersecurity Exposure, and Reliance on Third Party. Key components of the Risk Assessment include the following:

What is the magnitude of impact?

What is probability of occurrence?

What is the total risk?

Risk	Factors to Consider	Magnitude	Probability	Total
Loss of Data Integrity	Data Validation Controls	High	Low	Moderate

Risk	Factors to Consider	Magnitude	Probability	Total
Third Party Cyber Security Exposure	Lack of due diligence and continuous monitoring	High	Critical	Critical

Risk	Factors to Consider	Magnitude	Probability	Total
Reliance on Third Party	Diversification of vendors	High	Low	Moderate

Real World Examples: CrowdStrike 2025 Global Threat Report

eCrime Breakout Time

- Breakout time is the time it takes for an adversary to move laterally within the environment
- Average eCrime breakout time dropped to 48 minutes with the fastest breakout observed at just 51 seconds

Malware Detection

- Malware-free attacks use legitimate, built in tools and processes to carry out malicious actions
- 79% of detections in 2024 were malware free, up from 40% in 2019

Account Abuse

- Stolen credentials, misconfigured identity permissions, compromised service accounts, insider misuse
- Valid account abuse accounted for 35% of cloud incidents

Initial Access Vulnerability

- Over half of the vulnerabilities tracked by CrowdStrike were the kind that attackers could exploit to gain their first foothold into a system or network- before any malware deployment, lateral movement, or privilege escalation
- 52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access

CrowdStrike 2025 Global Threat Report

CrowdStrike 2025 Global Threat Report - Case Study

Curly Spider Introduction - Social Engineering Attack

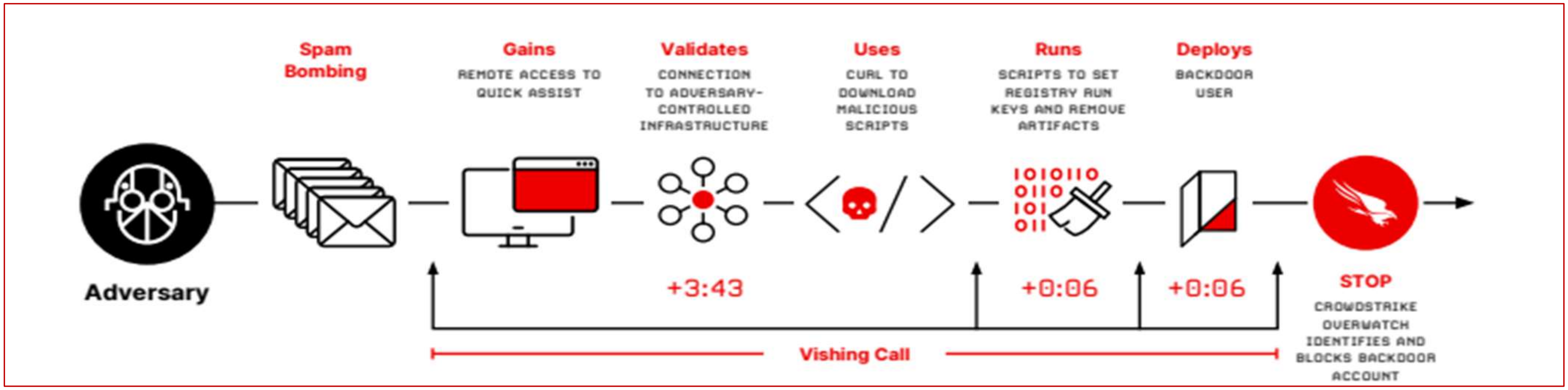
- Russian based cyber crime group that targets entities in North America and Western Europe- known for employing sharp social engineering techniques, notably through vishing campaigns.
- This case study highlights a social engineering attack to create a backdoor account in the environment

CrowdStrike 2025 Global Threat Report

CrowdStrike 2025 Global Threat Report- Case Study

Curly Spider Operation: How It Works

- A user will receive a large volume of spam emails impersonating charities, newsletters, or financial offers.
- Shortly after, a caller posing as help desk or IT support claims the spam is caused by malware or outdated spam filters.
- The user is instructed to join a remote session using an RMM tool, with the attacker guiding them through the installation and use of the tool.


Adversary
Spam Bombing
Gains
REMOTE ACCESS TO QUICK ASSIST
Validates
CONNECTION TO ADVERSARY-CONTROLLED INFRASTRUCTURE
Uses
CURL TO DOWNLOAD MALICIOUS SCRIPTS
Runs
SCRIPTS TO SET REGISTRY RUN KEYS AND REMOVE ARTIFACTS
Deploys
BACKDOOR USER
+3:43
+0:06
+0:06
STOP
CROWDSTRIKE OVERWATCH IDENTIFIES AND BLOCKS BACKDOOR ACCOUNT
Vishing Call

CrowdStrike 2025 Global Threat Report - Case Study

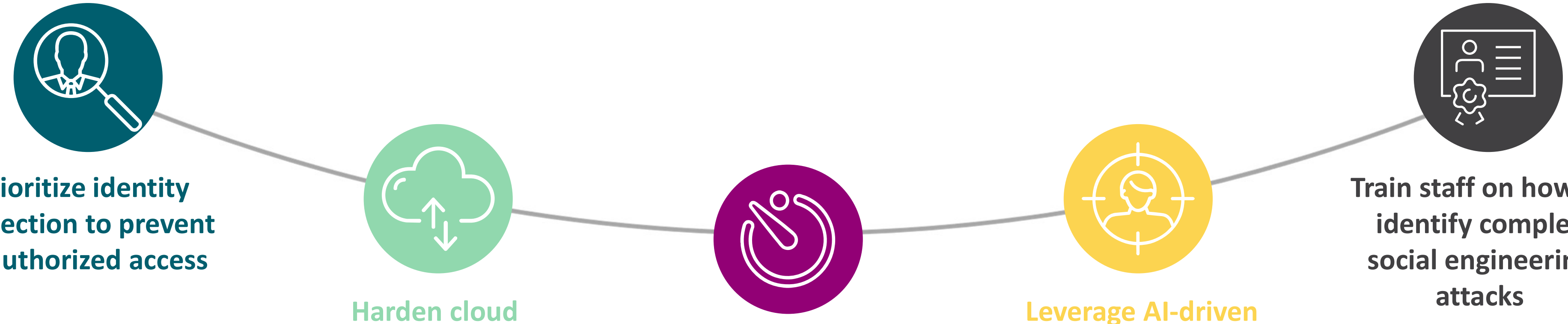
Curly Spider Impact

- After gaining remote access, the attacker changes system settings, creates a hidden user to run programs at startup, and deletes evidence to cover their tracks
- From there, the attacker sets up long-term access, creates a secret user account, and runs malicious software disguised as a normal program, helping them hide from detection
- These tactics often support ransomware operations.

CrowdStrike 2025 Global Threat Report

CrowdStrike 2025 Global Threat Report - Case Study

Curly Spider: How Could This Have Been Prevented?



Prioritize identity protection to prevent unauthorized access

Harden cloud environments against credential abuse and address misconfigurations

Accelerate response times to counter rapid breakout events

Leverage AI-driven threat hunting to detect stealthy adversary movements

Train staff on how to identify complex social engineering attacks

CrowdStrike 2025 Global Threat Report

Key Takeaways

- Organizations must prepare and mitigate against key risks, threats, and vulnerabilities
    - Relevant risks discussed today include unauthorized access, business interruption, and data loss
    - Threats include social engineering, cyber criminals, and human error
    - Vulnerabilities include lack of access controls, poor security awareness training, and insufficient backups.
- Risk management and risk assessments are a critical tool analyze threats and vulnerabilities, so that systems with the highest risk can be prioritized and appropriate actions taken to reduce risk.

Q&A

Contacting Us

- Matt Steinbach, CSRM Risk Management Manager- matthew.steinbach@vita.virginia.gov
- Risk Analysts by Secretariat
  - Andrew Wirz, Andrew.Wirz@vita.virginia.gov – Commerce and Trade, Finance, Independents, Security
  - Isaac Amoani, Isaac.Amoani@vita.virginia.gov – Agriculture & Forestry, Education, Labor, Natural Resources,
  - John Willinger, John.Willinger@vita.virginia.gov – Administration, Authority, Public Safety, Transportation
  - Marjean Adarkwa, Marjean.Adarkwa@vita.virginia.gov – Executive, Health and Human Resources

- VITA ISO Services- For agencies interested in support in conducting system level risk assessments
  - Michael Vannoy- Michael.Vannoy@vita.virginia.gov