VA and Other Federal Agencies Need to Address Significant Challenges

GAO Update to:

The Information Security and Privacy Advisory Board

December 4, 2019

About the Report: GAO-20-256T

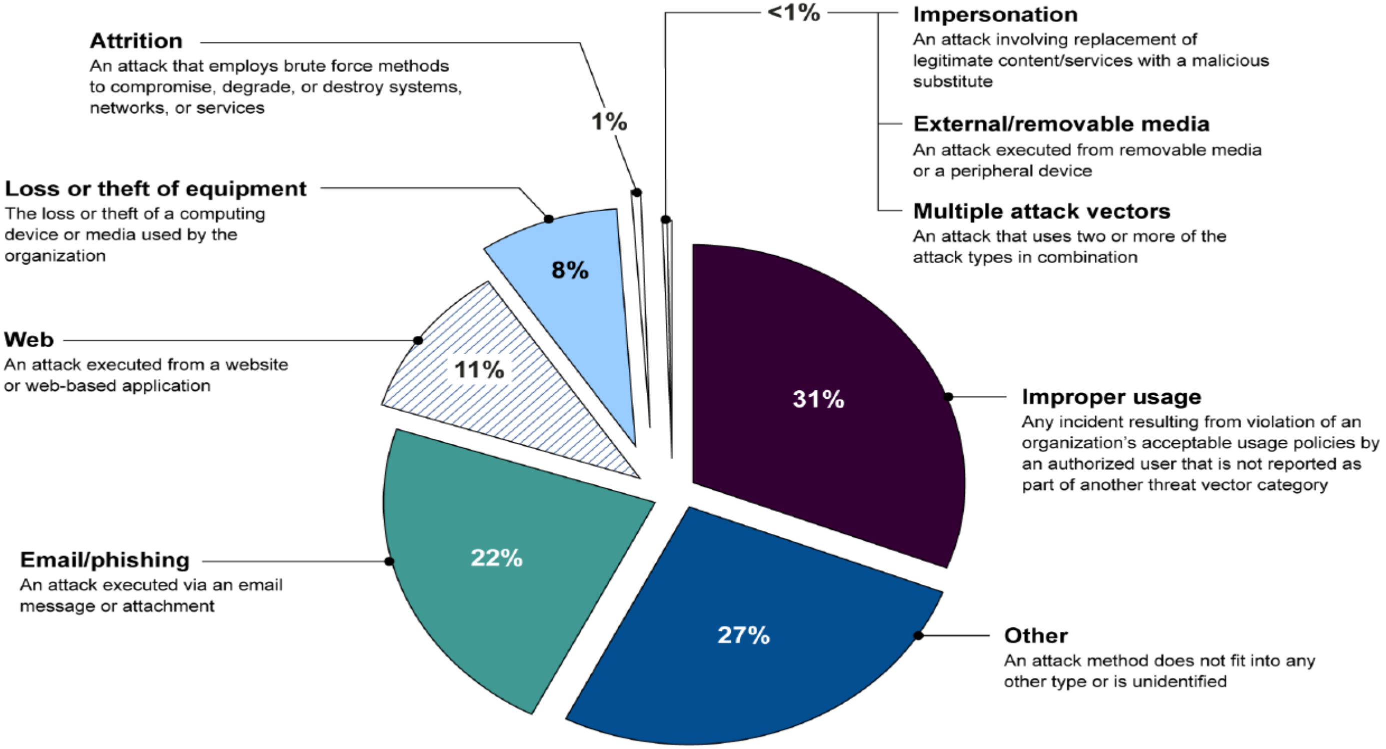
- *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges* (Nov. 2019)
- Presented as testimony before HVAC Subcommittee on Technology Modernization
- Summarized status of information security across CFO Act agencies and at VA
- Based largely on prior GAO work
- Reviewed relevant OMB, IG, and agency reports

Background

- Federal law and policy set requirements for securing federal systems and information:
  - FISMA
  - E.O. 13800
  - NIST Cybersecurity Framework
- Civilian CFO Act agencies have spent billions on IT security related activities in FY 2018
- Federal agencies continue to report large numbers of security incidents, although VA has reported fewer incidents in recent years

Background – Federal information security incidents by threat vector, FY 2018

31,107 total information security incidents



Attrition
An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

Loss or theft of equipment
The loss or theft of a computing device or media used by the organization

Web
An attack executed from a website or web-based application

Email/phishing
An attack executed via an email message or attachment

Impersonation
An attack involving replacement of legitimate content/services with a malicious substitute

External/removable media
An attack executed from removable media or a peripheral device

Multiple attack vectors
An attack that uses two or more of the attack types in combination

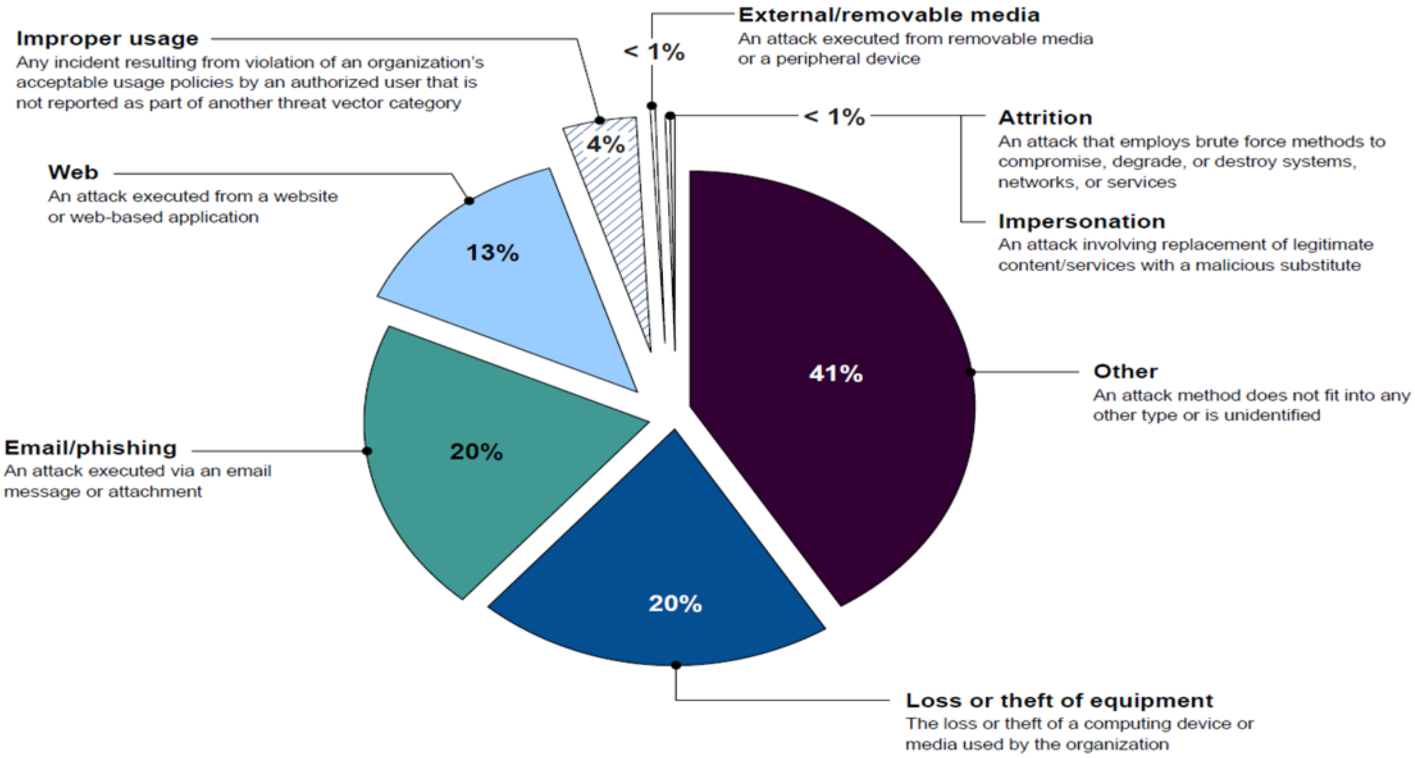
Improper usage
Any incident resulting from violation of an organization's acceptable usage policies by an authorized user that is not reported as part of another threat vector category

Other
An attack method does not fit into any other type or is unidentified

Source: United States Computer Emergency Readiness Team incident report data for fiscal year 2018. | GAO-19-545

Background – VA information security incidents by threat vector, FY 2018

1,776 total information security incidents



Improper usage
Any incident resulting from violation of an organization's acceptable usage policies by an authorized user that is not reported as part of another threat vector category

External/removable media
An attack executed from removable media or a peripheral device

Attrition
An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

Impersonation
An attack involving replacement of legitimate content/services with a malicious substitute

Web
An attack executed from a website or web-based application

Other
An attack method does not fit into any other type or is unidentified

Email/phishing
An attack executed via an email message or attachment

Loss or theft of equipment
The loss or theft of a computing device or media used by the organization

ource: GAO analysis of Office of Management and Budget data for fiscal year 2018. | GAO-20-256T

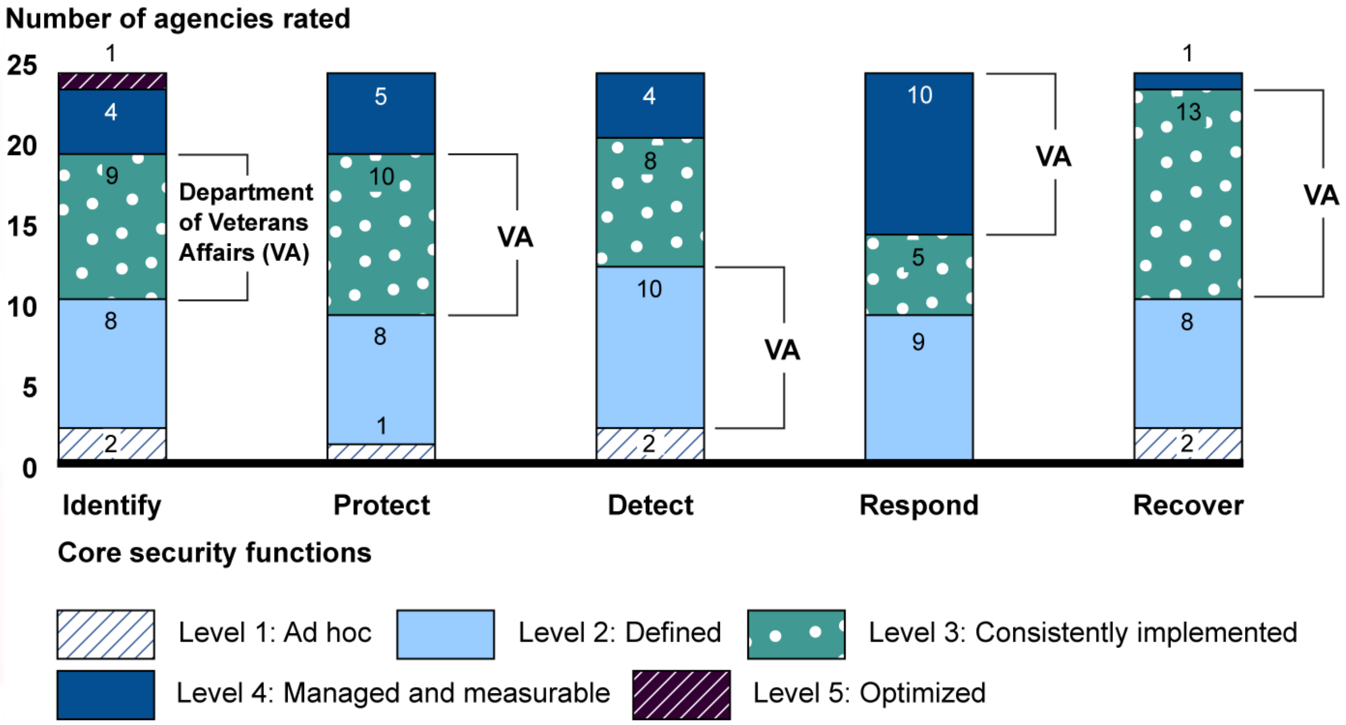
Federal agencies, including VA, continue to have deficient information security programs

- IGs for 18 of 24 CFO Act agencies determined that their agency's IS program was not effectively implemented during FY 2018

- IGs used a five-level maturity model to rate their agency's IS policies, procedures, and practices related to the five core security functions – *identify, protect, detect, respond, and recover* – defined in NIST's cybersecurity framework

- Level 4 (managed and measurable) and Level 5 (optimized) represent effective levels of security

IG ratings for five core security functions of 24 CFO Act agencies for FY 2018



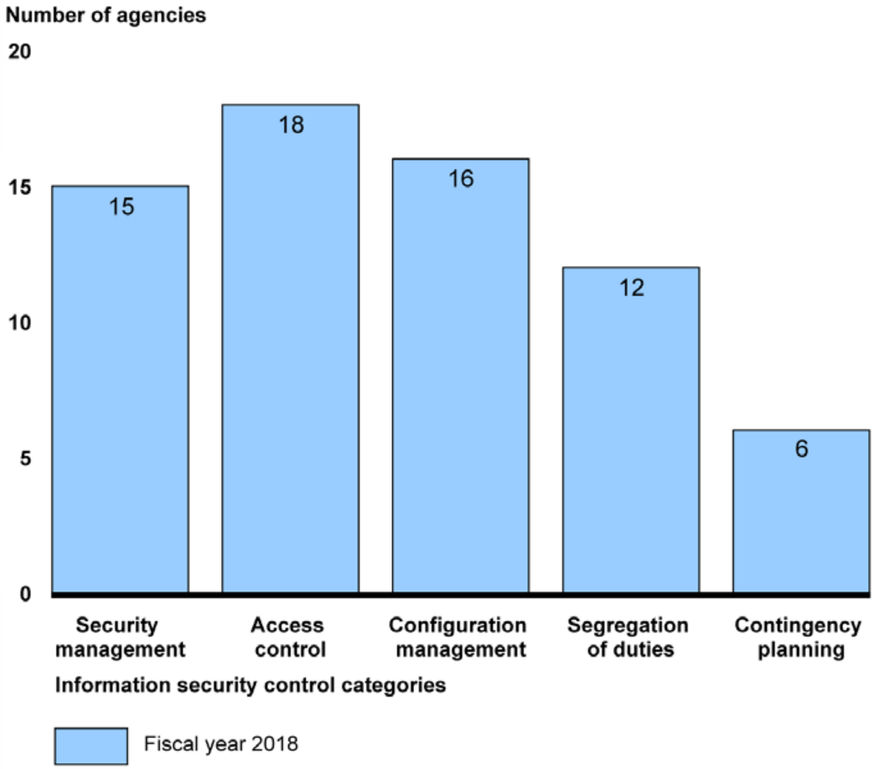
Source: GAO analysis of agency fiscal year 2018 *Federal Information Security Modernization Act of 2014* (FISMA) reports and the Office of Management and Budget's *Fiscal Year 2018 Annual FISMA Report to Congress.* | GAO-20-256T

Most CFO Act agencies had significant IS control deficiencies over financial reporting

- Agency IGs or IPAs reported for FY 2018:
  - 6 agencies w/ material weaknesses in IS controls
    - DOD, DHS, HUD, OPM, USDA, VA
  - 12 agencies w/ significant deficiencies
  - 6 agencies w/out significant deficiencies
    - DOE, DOI, DOJ, NRC, NSF, USAID

  - IS was a major management challenge for 21 of 24 agencies
    - Not reported as a MMC for ED, NRC, NSF

Most CFO Act agencies had deficiencies in most IS control categories for their financial systems



Source: GAO analysis of agency financial reports for fiscal year 2018. | GAO-20-256T

Most civilian CFO Act agencies, including VA, have reported meeting many cyber targets

Key milestone	Performance Metric & Target	Number of agencies reported meeting targets	VA status
Software asset management	95% of software assets are covered by a whitelisting capability.	10	Not met
Hardware asset management	95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.	16	Not met
Authorization management	100% of high and moderate impact systems are covered by a valid security authorization to operate.	14	Not met
Mobile device management	95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	19	Met
Privileged network access management	100% of privileged users are required to use a Personal Identity Verification (PIV) card or Authenticator Assurance level 3 (AAL3) multifactor authentication method to access the agency's network.	18	Met
High-value asset access management	90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	14	Met
Automated access management	95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	15	Not met
Intrusion detection and prevention	At least 4 of 6 intrusion prevention metrics have met an implementation target of at least 90% and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source.	8	Met
Exfiltration and enhanced defenses	At least 3 of 4 exfiltration and enhanced defenses metrics have met an implementation target of at least 90%.	23	Met
Data protection	At least 4 of 6 data protection metrics have met an implementation target of at least 90%.	16	Met

VA faces key security challenges as it modernizes and secures its IT systems

1. Effectively implementing information security controls

2. Adequately mitigating known security deficiencies

3. Fully establishing elements of a cybersecurity risk management program

4. Identifying critical cybersecurity staffing needs

5. Managing IT supply chain risks as part of IT modernization programs

Related GAO Reports

- GAO-19-545, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices* (July 2019)
- GAO-19-384, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges* (July 2019)
- GAO-19-144, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs* (March 2019)
- GAO-18-667T, *Information Security: Supply Chain Risks Affecting Federal Agencies* (July 2018)
- GAO-16-501, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems* (Sept. 2016)

GAO contact information

- Di’Mond Spencer, Analyst-in-charge, SpencerD@gao.gov, 202-512-6684

- Greg Wilshusen, Director, WilshusenG@gao.gov, 202-512-6244

Questions