Homeland
Security

Better Reporting Guidelines for Better Data

Christopher Washington, US-CERT
Brian Allen, US-CERT

Disclaimer

This presentation is intended for informational and discussion purposes only.

The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the DHS official seal or other DHS visual identities, including the US-CERT or ICS-CERT name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security, including US-CERT and ICS-CERT. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS, US-CERT, ICS-CERT or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

This presentation is Traffic Light Protocol (TLP): WHITE. Recipients may share TLP: WHITE information without restriction, subject to copyright controls. For more information on the TLP, see http://www.us-cert.gov/tlp.

DHS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

Who Is US-CERT?

US-CERT Mission:

- To provide a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world

Operations:

- 24 x 7 Operations Center
- Provides technical assistance to information system operators
- Disseminates actionable information regarding cyber-threats and vulnerabilities

Incident Reporting:

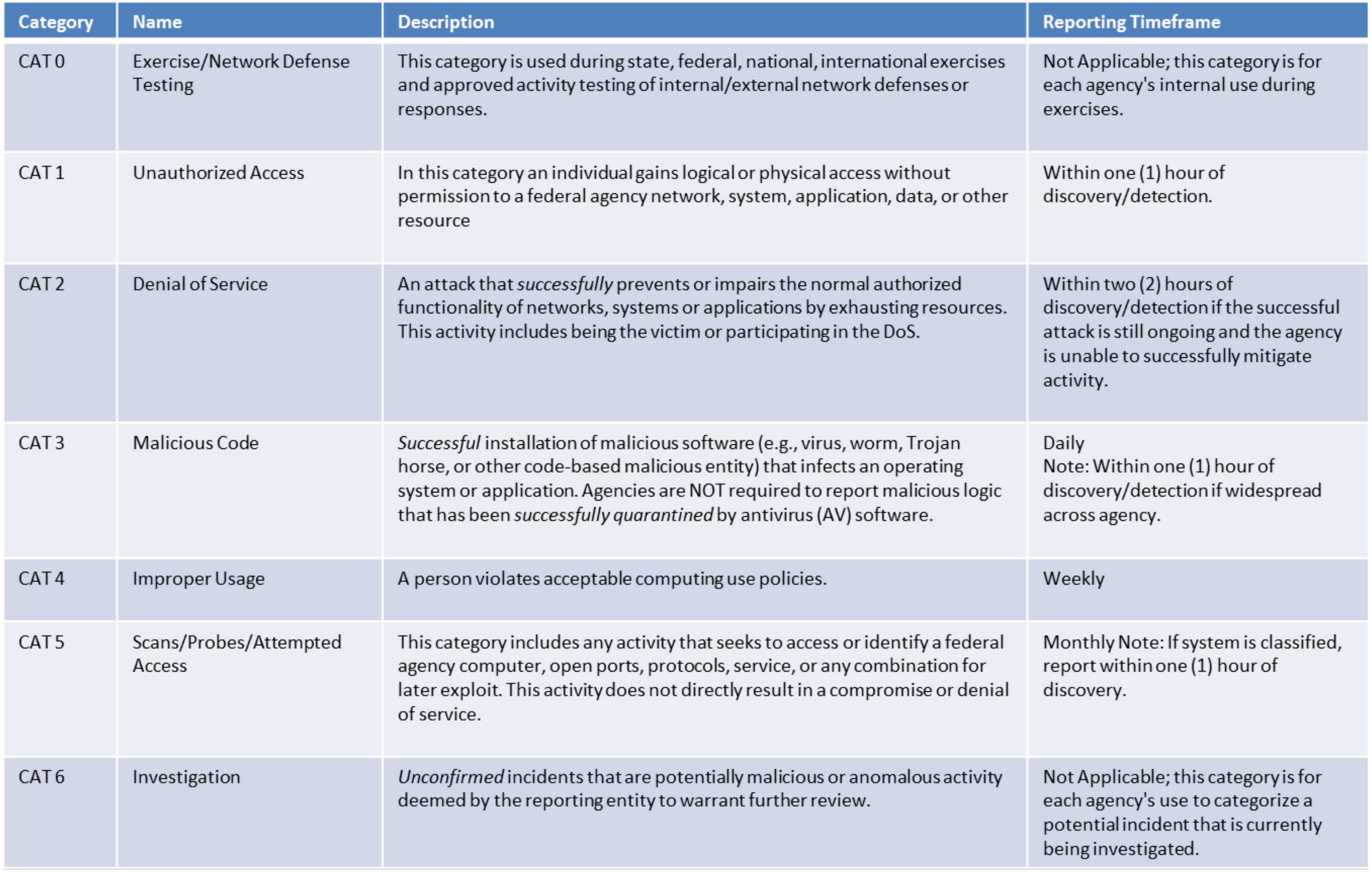
- Per FISMA, Federal agencies are required to report all incidents to US-CERT

Federal Incident Reporting

Cyber Incident reporting before October 1, 2014:

- Based on NIST 800-61 Revision 1
- System of 6 categories
- OMB M-07-16 – All Personally Identifiable Information (PII) incidents (including paper) must be reported within 1 hour

Pre-Oct 2014 Reporting Taxonomy



Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	Denial of Service	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	Improper Usage	A person violates acceptable computing use policies.	Weekly
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Identified Issues

Difficult to assess impact and prioritize incidents

Does not separate incidents (impactful) from events (non-impactful)

Incidents can apply to multiple categories (Ex: Malware used to gain unauthorized access to system)

Categories fuse **causes** (malware, inappropriate usage) with **effects** (Unauthorized Access, Denial of Service)

- Cause = Method (or Attack Vector)
- Effect = Impact

Updating the Guidelines

US-CERT aligned with NIST 800-61 Rev 2

Separate Cause and Effect

- Cause – Attack vector data
- Effect – Functional impact data
- Effect – Information impact data
- Effect – Recoverability data

New incident reporting guidelines:

- Separate incidents (confirmed loss of CIA) from (events) reporting requirements
- Establish a 1 hour timeframe for mandatory reports
- Eliminate requirement to identify cause upon submitting initial report
- Non-cyber incidents no longer required

Incident Prioritization and Impact Analysis

Multidimensional Approach to Prioritizing Incidents:

Functional impact

- Impact to service availability / business functionality

Information impact

- Confidentiality comprised or data destruction / information exfiltration

Recoverability

- Time and resources to recover from incident

Functional Impact Matrix

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Information Impact Matrix

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Recoverability Impact Matrix

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Attack Vectors

External/Removable Media: An attack executed from removable media or a peripheral device—e.g., malicious code spreading onto a system from an infected USB flash drive.

Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., DDoS intended to deny access to a service; brute force attack against an authentication mechanism).

Web: An attack executed from a website or web-based application—e.g., a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.

Email: An attack executed via an email message or attachment—e.g., exploit code hidden in attachment or malicious URL within the body of an email.

Attack Vectors (cont’d)

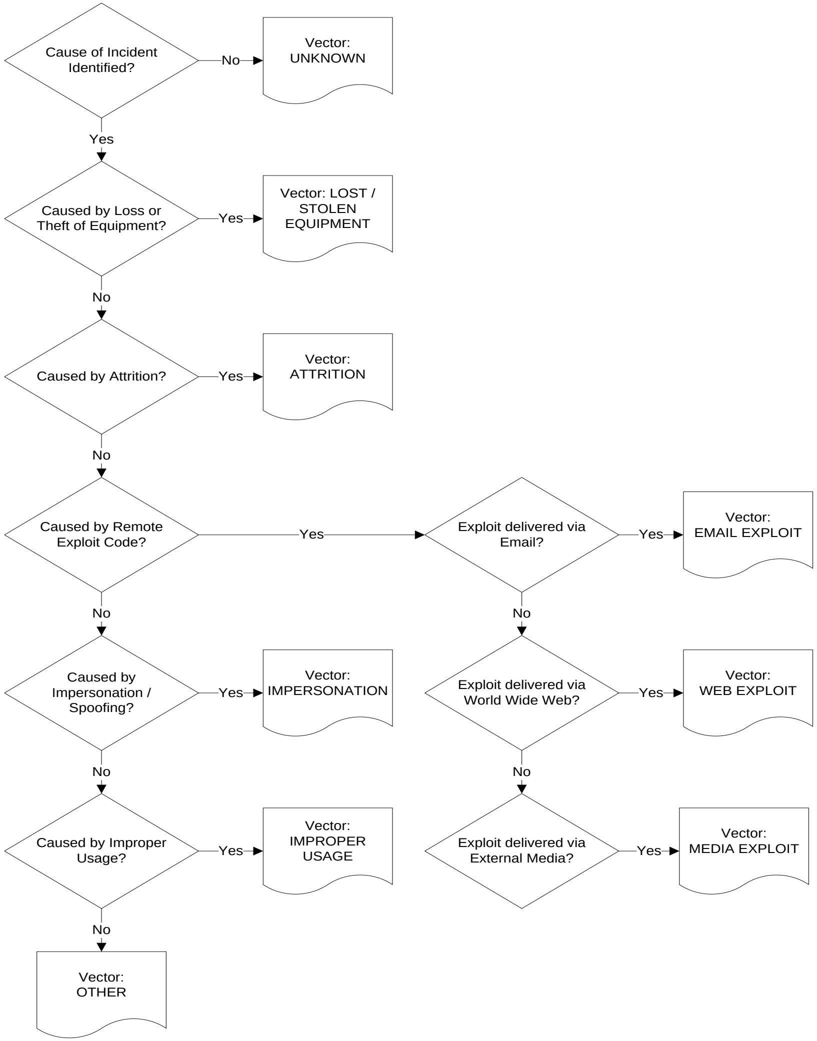
Impersonation: An attack involving replacement of something benign with something malicious—e.g., spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.

Improper Usage: Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories—e.g., a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.

Loss or Theft of Equipment: The loss or theft of a computing device or media used by the organization—e.g., laptop, smartphone, or authentication token.

Other: An attack that does not fit into any of the other categories.

Cause Analysis Workflow


Cause of Incident Identified?
No
Vector: UNKNOWN
Yes
Caused by Loss or Theft of Equipment?
Yes
Vector: LOST / STOLEN EQUIPMENT
No
Caused by Attrition?
Yes
Vector: ATTRITION
No
Caused by Remote Exploit Code?
Yes
Exploit delivered via Email?
Yes
Vector: EMAIL EXPLOIT
No
No
Caused by Impersonation / Spoofing?
Yes
Vector: IMPERSONATION
Exploit delivered via World Wide Web?
Yes
Vector: WEB EXPLOIT
No
No
Caused by Improper Usage?
Yes
Vector: IMPROPER USAGE
Exploit delivered via External Media?
Yes
Vector: MEDIA EXPLOIT
No
Vector: OTHER

Three Pronged Approach

Process Preparation:

- Rewrote Incident Reporting Guidance
- Released to community for feedback and feasibility check
- Coordinated with OMB to update M-series Memo
- Published and socialized government-wide

Technology Preparation:

- Updated incident management system
- New data fields
- Updated incident reporting web form
- Updated incident reporting schema and STIX mapping
- End-to-end testing

People Preparation:

- Revamp incident handling procedures
- Train Staff

Strategic Benefits

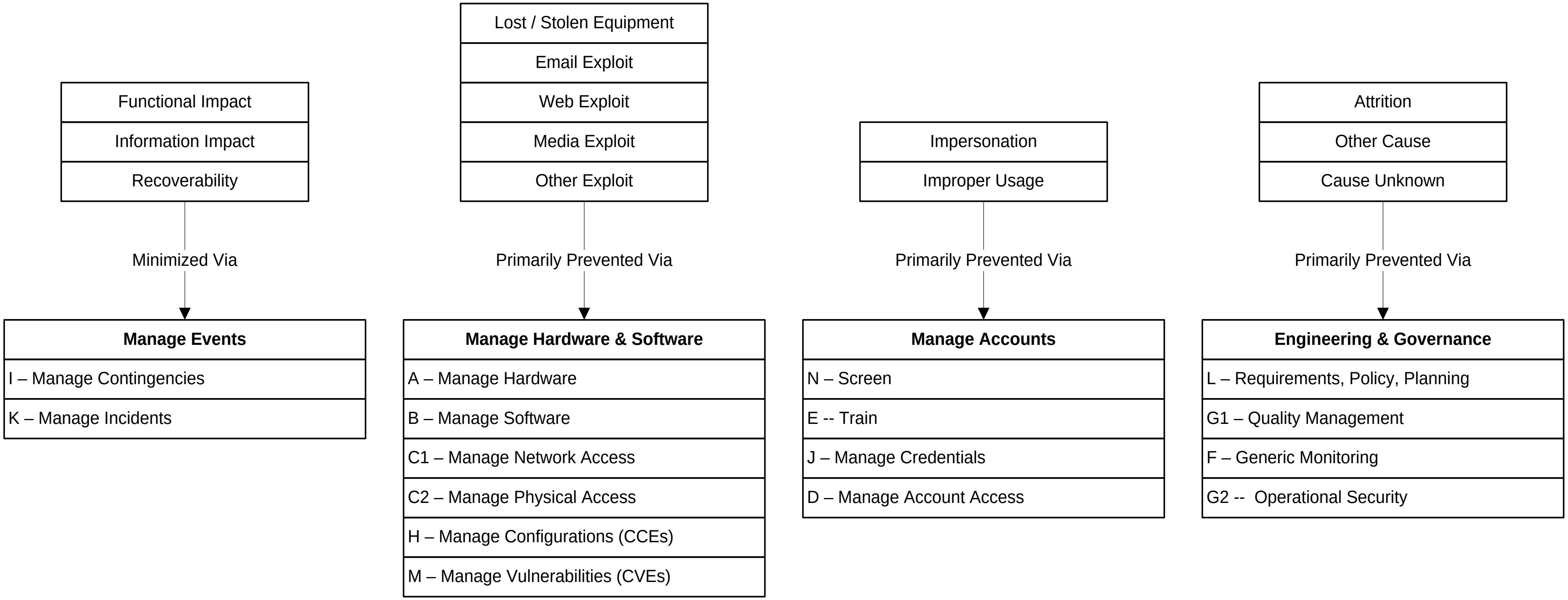
Improvement in understanding the risks facing the federal government

Improved the timeliness of actionable reporting

Improved usefulness of data entry resources

Rich, consistent data to support both tactical and strategic decisions

Incident Reporting Categories & Security Controls Relationships



Functional Impact
Information Impact
Recoverability

Minimized Via

Manage Events
I – Manage Contingencies
K – Manage Incidents

Lost / Stolen Equipment
Email Exploit
Web Exploit
Media Exploit
Other Exploit

Primarily Prevented Via

Manage Hardware & Software
A – Manage Hardware
B – Manage Software
C1 – Manage Network Access
C2 – Manage Physical Access
H – Manage Configurations (CCEs)
M – Manage Vulnerabilities (CVEs)

Impersonation
Improper Usage

Primarily Prevented Via

Manage Accounts
N – Screen
E -- Train
J – Manage Credentials
D – Manage Account Access

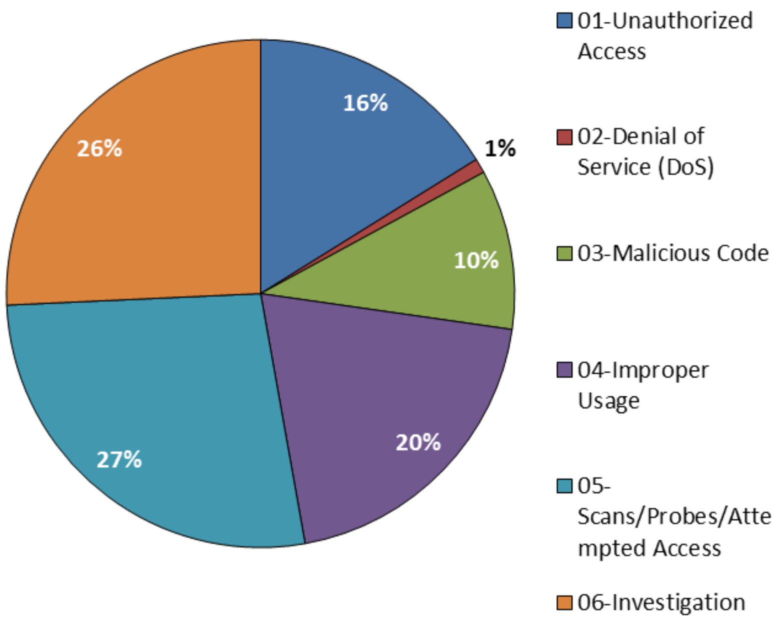
Attrition
Other Cause
Cause Unknown

Primarily Prevented Via

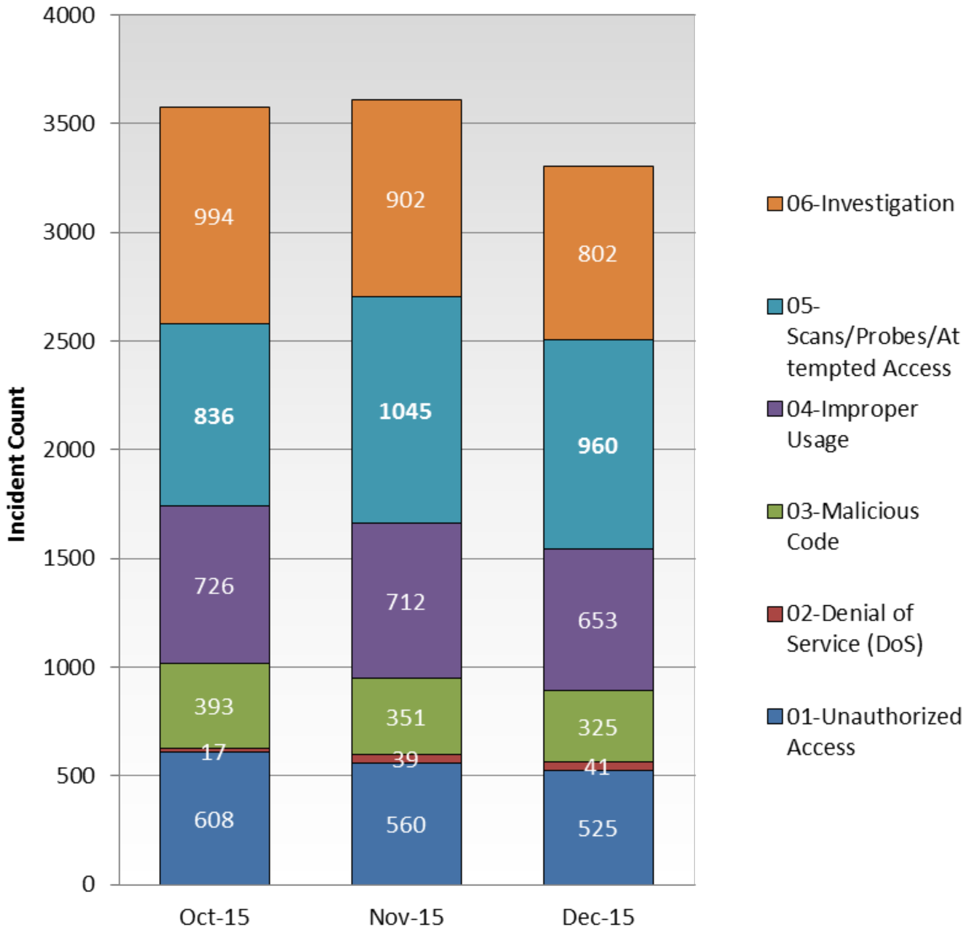
Engineering & Governance
L – Requirements, Policy, Planning
G1 – Quality Management
F – Generic Monitoring
G2 -- Operational Security

Data Example: Category System

Incidents by Category

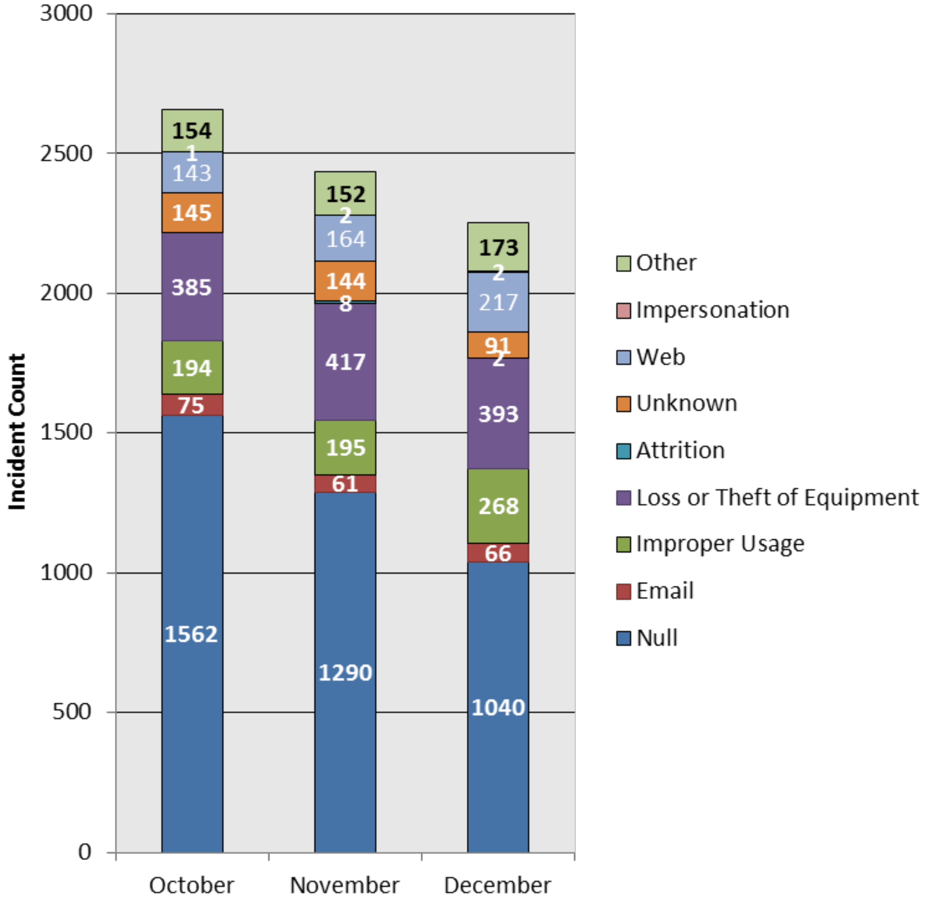


Incidents by Month and Category

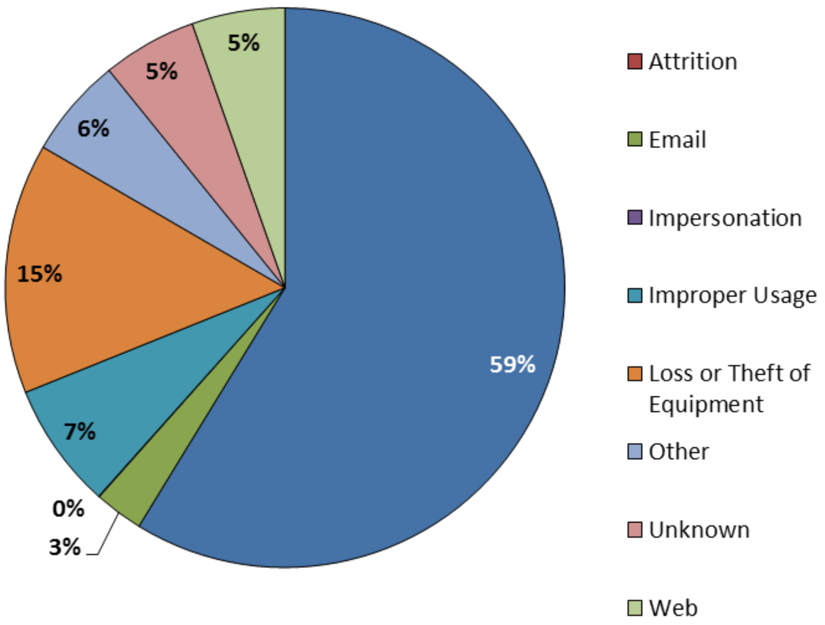


Data Examples: Incidents by Vector

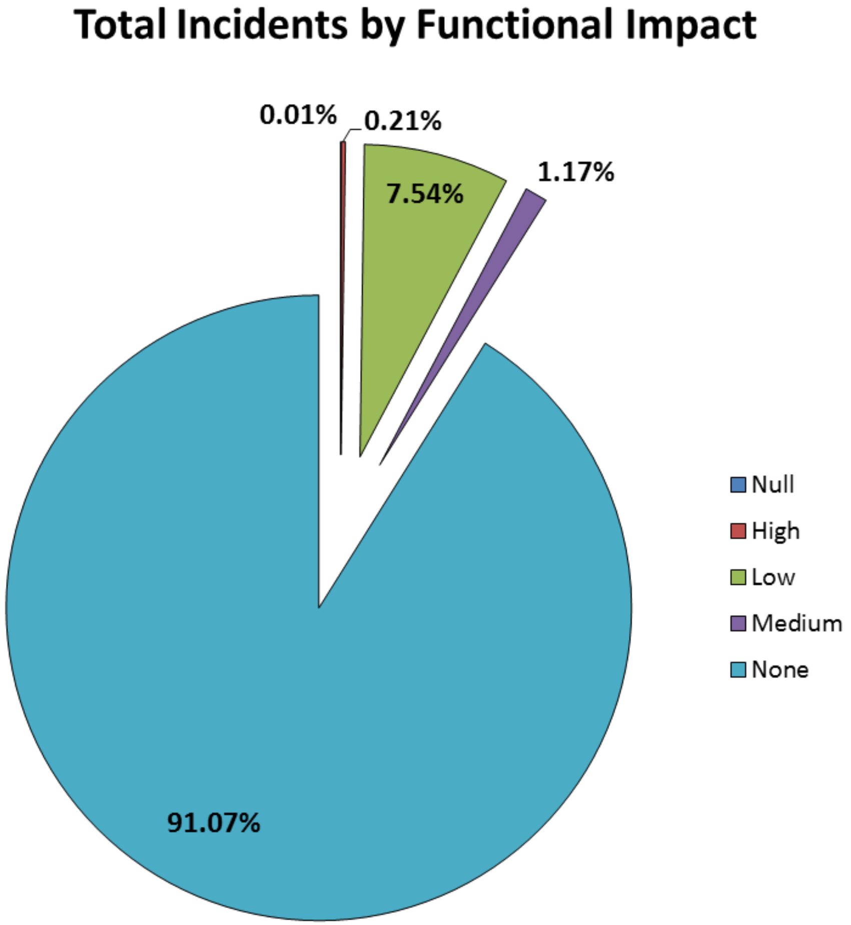
Incidents by Vector and Month (Oct–Dec 2015)



Incidents by Vector (Oct–Dec 2015)



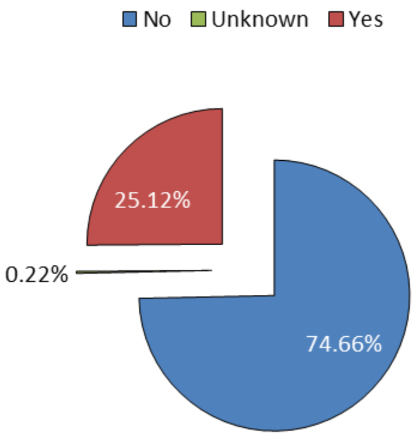
Data Examples: Functional Impact



Functional Impact	Incident Total	% of Total
Null	1	0.01%
High	23	0.21%
Medium	125	1.17%
Low	807	7.54%
None	9753	91.07%

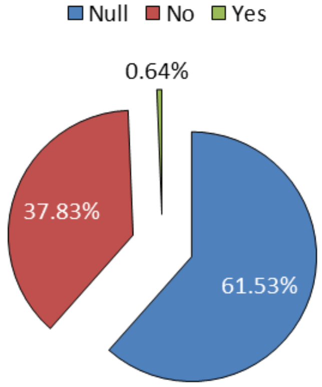
Data Examples: Information Impact

Incidents with Privacy Data Affected



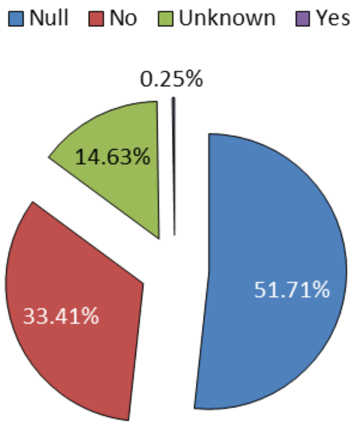
Privacy	Incidents
No	5710
Unknown	17
Yes	1921
Total	**7648**

% of Incidents with Proprietary Data Impacted



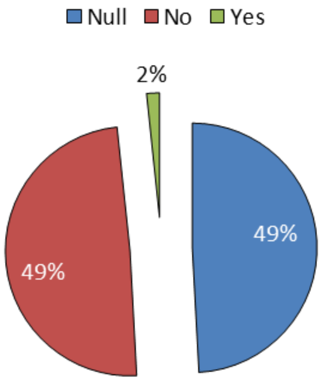
Proprietary	Incidents
Null	4706
No	2893
Yes	49
Total	**7648**

% of Incidents with Data Integrity Impacted



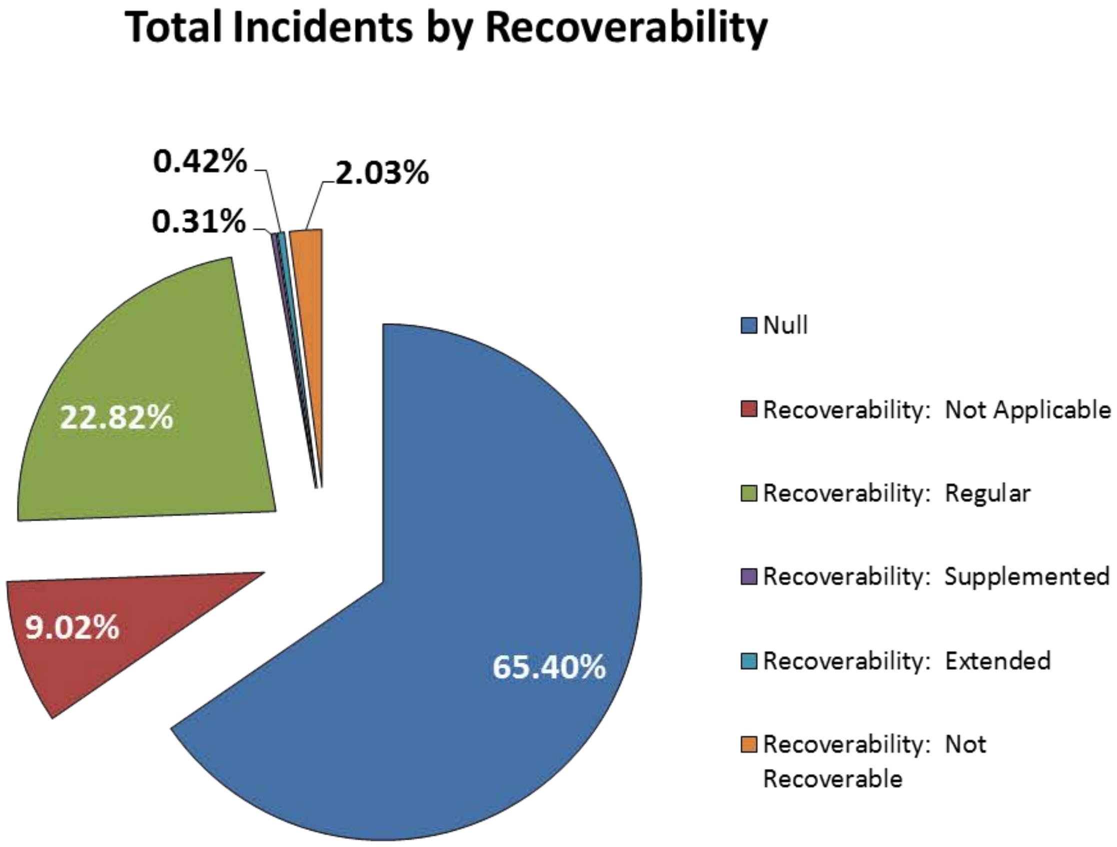
Integrity	Incidents
Null	3955
No	2555
Unknown	1119
Yes	19
Total	**7648**

% of Incidents with Classified Data Impacted



Classified	Incidents
Null	3759
No	3762
Yes	127
Total	**7648**

Data Examples: Recoverability


Total Incidents by Recoverability

Recoverability	Incident Total	% of Total
Null	5002	65.40%
Not Applicable	690	9.02%
Regular	1745	22.82%
Supplemented	24	0.31%
Extended	32	0.42%
Not Recoverable	155	2.03%
Total	**7648**	**100.00%**

Looking Forward

Running incidents through alternative models

- Microsoft Broad Street
- Kill chain
- Severity Scoring System
- Research and Development

Governance model for updating the guidelines

- Periodical review with Federal CIO Council
- Changes made in coordination with OMB and NIST

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security