PROJECT DESCRIPTION

DATA INTEGRITY

Recovering from a destructive malware attack

Donald Tobin
Michael J. Stone
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Anne Townsend
Harry Perper
Sarah Weeks
The MITRE Corporation

May 2016
di-nccoe@nist.gov

This revision incorporates comments from the public.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a community of interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

ABSTRACT

Threats of destructive malware, malicious insider activity, and even honest mistakes create the imperative for organizations to be able to quickly recover from an event that alters or destroys any form of data (database records, system files, configurations, user files, application code, etc.). Organizations must be confident that recovered data is accurate and safe. The NCCoE — in collaboration with members of the business community and vendors of cybersecurity solutions — will build an example solution to address these complex data integrity challenges.

Multiple systems need to work together to prevent, detect, notify, and recover when data integrity is jeopardized. This project explores methods to effectively monitor and detect data corruption in commodity components (server, operating system, applications, and software configurations) as well as custom applications and data. It also explores issues of auditing and reporting (user activity monitoring, file system monitoring, database monitoring, scanning backups/snapshots for malware and rapid recovery solutions) to support recovery and investigations. To address real-world business challenges around data integrity, the resulting example solution will be composed of open-source and commercially available components. Ultimately, this project will result in a publicly available NIST Cybersecurity Practice Guide—a description of the solution and practical steps needed to implement an example solution that addresses these existing challenges.

KEYWORDS

business continuity, malware, ransomware, integrity, attack vector, data recovery, malicious actor

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or

NCCoE, nor is it intended to imply that the entities, materials or equipment are necessarily the best available for the purpose.

CONTRIBUTORS

We gratefully acknowledge the contributions of: Ted Kolovos and Leslie Anderson

Table of Contents

1. Executive Summary

Purpose

In order to remain operational, organizations should be able to quickly recover from a data integrity attack and trust that the recovered data is accurate, complete, and free of malware. Widely reported data integrity attacks caused by unauthorized insertion, deletion, or modification have compromised corporate information including: emails, employee records, financial records, customer data. Some organizations have experienced systemic attacks that have caused them to temporarily cease operations. One variant of a data integrity attack, ransomware, encrypts data and holds them hostage while the attacker demands payment for the decryption keys.

The project described in this document could help organizations address the issue of detecting and recovering from a data integrity attack. NCCoE projects include an architectural description and a reference design – an example solution – that addresses a technical challenge. Reference designs integrate commercial and open source products to demonstrate an implementation of standards and best practices. These projects result in NIST cybersecurity practice guides, which provide detailed steps needed to implement the proposed architecture and to recreate the reference design. Once completed, organizations will be able to use the data integrity practice guide to implement some or all of the relevant security controls enhancing their ability to recover from data corruption attacks.

Scope

This project will answer specific questions pertaining to data integrity and recovery such as:

- What data was corrupted? When was it corrupted? How it was corrupted? Who corrupted it?
- Do any other events coincide with this corruption?
- What was the impact of the data corruption? (Systems affected, timelines, etc.)
- Which backup version should be used to recover data?

This project will address:

1) A file system integrity solution to allow recovery from trusted backups and snapshots.
2) A database integrity solution with transactions and versioning to allow for rollbacks to a known good state.
3) An overall automated system that incorporates the previous two areas and may include the following:

    a. Activity logging and monitoring.

b. Versioning and journaling file system.
c. Restoration of desktops, applications, and critical services quickly after cyber incidents.
d. Alert systems to notify administrators when baselines are changed on critical systems.

Assumptions/Challenges

Detecting Data Corruption in Back-ups

Data back-up software and systems focus on accurately restoring data as originally stored. This approach is effective for data that is known to be un-corrupted, although not necessarily vulnerability free. These systems generally do not provide a retroactive data testing scheme to test data for corruption by insiders or malicious applications while in storage.

Detecting malware in back-up data

Data back-up software and systems generally do not have manual or automated testing capabilities to identify and remediate malware in backed up data. Malware detection is typically done at runtime in operational systems by anti-virus/anti-malware software. In addition, the software is not designed to test data in non-real time. Malware that is designed to be dormant for periods of time may not be detectable until active with current anti-virus/anti-malware software. A time-shifting, self-contained testing environment that can emulate the passage of time may be able to detect time-sensitive or time-delayed malware activity in addition to malware with signatures for activity monitoring that was unknown at the time the backup was completed.

Automation of Backup Data Testing

Back-up data testing is typically used to verify that back-up data can be used to restore systems to operational readiness. Data back-up software and systems generally do not offer automated backup data integrity or malware testing capabilities.

Background

The NCCoE, working with the organizations across the set of critical infrastructure industries, including information sharing and analysis centers (ISACs), identified the need for a data integrity solution. The center held a workshop to identify key issues that affect consumer data protection, encapsulated in NISTIR 8050. This document identified data integrity (among other items) as a key cybersecurity issue that needs to be addressed. The need arises from the recognition that malicious actors are devising methods of corrupting data within organizations. The data corruption includes data modification as well as data destruction. In addition, the center met with representatives the financial sector ISAC (FS-ISAC) for guidance, and worked with the FS-ISAC Destructive Malware Data Integrity Task Force.

2. SCENARIOS

The example scenarios below illustrate some of the challenges that this project will address. The relevant functions and categories from the NIST Framework for Improving Critical Infrastructure Cybersecurity (referred to in short as the Cybersecurity Framework or CSF) that can be employed to mitigate the events throughout the attack are listed below. The specific NIST CSF subcategories are listed in parenthesis in each table.

Scenario 1 - Ransomware

For financial gain, an organized crime group has set up multiple seemingly legitimate domains that contain destructive malware to be automatically downloaded and discreetly/silently installed, without the user's knowledge, when a website on the domain is visited. Once the malware is installed it encrypts the organization's file system and requires a ransom payment in order to decrypt the files to be restored. Left unmitigated, the malware on one system is designed to move laterally within the network to other client and server systems within an organization's network, encrypting those systems and demanding ransom before access to those systems can be restored.

The project addresses Respond and Recover CSF categories

- Malware encrypts files and displays notice demanding payment for decryption
  - Respond/Recover:
    - notify security (DE.DP-4, RS.CO-2, DE.EA-5)
    - file integrity monitor (PR.DS-1, PR.DS-6, PR.PT-1)

The project does not address these Protect and Detect CSF categories

- User receives phishing email with executable attachment
  - Protect/Detect: email security and attachment scanning
- User runs the attachment containing malware which installs and infects the user's machine
  - Protect/Detect: Host-based Anti-malware, application whitelisting, EMET, sandboxing/virtualization
- Malware sets up command and control where it receives instructions and cryptographic keys
  - Protect/Detect: Host-based firewall/IDS, network-based firewall/IDS

Scenario 2 - Data destruction

An adversary wishing to impact the operations of a major lending or banking institution launches a spear-phishing campaign against individuals in the target corporation. Once any of the human targets clicks on a link or attachment, the malware downloads and

installs itself on that user's machine, and immediately starts looking to infect other systems across the enterprise. At a predetermined time, the malware starts encrypting all data on the infected machines. Then it writes over the original unencrypted content and deletes the encryption keys.

The project addresses Respond and Recover CSF categories

- Malware destroys data on user's machine
  - Respond/Recover:
    - back-ups (PR.DS-1, PR.IP-4)
    - file integrity monitor (PR.DS-1, PR.DS-6, PR.PT-1)

The project does not address these Protect and Detect CSF categories

- User receives phishing email with executable attachment
  - Protect/Detect: email security and attachment scanning
- User runs the attachment containing malware which installs and infects the user's machine
  - Protect/Detect: Host-based Anti-malware, application whitelisting, EMET, sandboxing/virtualization
- Malware performs reconnaissance and attempts to spread throughout the enterprise.
  - Protect/Detect: network-based firewall/IDS, use of P-VLANs

Scenario 3 - Data Manipulation (insider)

An employee incorrectly modifies company records either by accidental use or with ill intention to harm his employer by damaging its business operations, brand, or reputation. Using authorized credentials the employee already has or acquires, database entries are modified. Because the modifications the employee makes appear to be legitimate, a significant amount of time may elapse before the corruption is discovered.

The project address Respond and Recover CSF categories

- User modifies a configuration file in violation of established baselines
  - Protect/Detect:
    - **file integrity monitor** (PR.DS-1, PR.DS-6, PR.PT-1)
    - **user activity auditing** (DE.CM-3, PR.PT-1)
- Administrator modifies a user's file
  - Protect/Detect:
    - **file integrity monitor** (PR.DS-1, PR.DS-6, PR.PT-1)
    - **user activity auditing** (DE.CM-3, PR.PT-1, DE.AE-1)
- Administrator and/or script modifies data in a database
  - Protect/Detect:
    - **database transaction auditing** (PR.DS-1, PR.PT-1, DE.CM-1)

3. High-Level Architecture

The figure below depicts the proposed high-level environment and architecture to help ensure data integrity within the enterprise.

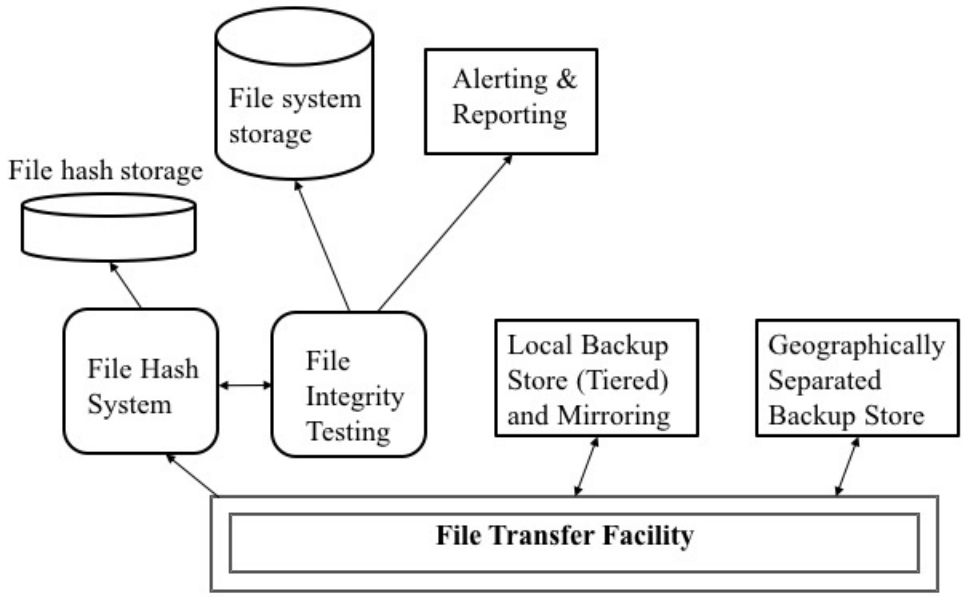

Figure 1. Data Integrity Building Block high-level architecture

Component List

Data integrity solutions include but are not limited to the following components:

- File integrity monitors
- File versioning systems
- File integrity testing capabilities
- User activity monitoring tools
- Configuration management systems
- Database rollback tools
- Virtual machine integrity/snapshots/versioning capabilities
- Versioning file systems
- Journaling file systems

Some of these are subcomponents of the components shown in the high-level architecture

Desired Requirements

To address the three scenarios, this project will use a collection of commercially available technologies to demonstrate security and functional characteristics of a data integrity solution. The data integrity solution shall include the automation of the following capabilities:

- data corruption testing
- data corruption detection
- data corruption event logging
- Secure data integrity monitoring and alerting information (checksums, off-site, hard-copy)
- detection and reporting of all file modifications / creations / deletions
- detection and reporting of all database modifications / creations / deletions
- correlation of file changes and users
- user activity recording
- anomalous user activity detection
- configuration management monitoring

4. Relevant Standards and Guidance

NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

NIST SP 800-27A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A

http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

NIST SP 800-33, Underlying Technical Models for Information Technology Security

http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

NIST SP 800-34, Contingency Planning Guide for Federal Information Systems

http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

NIST SP 800-160, Systems Security Engineering, An Integrated Approach to Building Trustworthy Resilient Systems

http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

ISO/IEC 27001, Information Technology – Security Techniques – Information Security Management Systems

http://www.iso.org/iso/home/search.htm?qt=27001&sort=rel&type=simple&published=on

ISO/IEC 15408-1, Information technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction

http://www.iso.org/iso/home/search.htm?qt=15408-1&sort=rel&type=simple&published=on

ISO/IEC 15408-2, Information technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414

ISO/IEC 15408-3, Information technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Components

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413

5. Security Control Map

Table 1 maps the characteristics of the applicable standards and best practices described in the CSF, and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that these characteristics will meet your industry's requirements.

Solution Characteristic	NIST CSF Category	Informative References
Automated data corruption testing	PR.DS-1 PR.DS-6	**NIST SP 800-53 Rev. 4** SC-28, SI-7 **ISO/IEC 27001:2013** A.8.2.3, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
Automated data corruption detection	PR.DS-1 DE.CM-1	**NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SC-28, SI-4 **ISO/IEC 27001:2013** A.8.2.3
Automated data corruption event logging	PR.DS-1 PR.PT-1	**NIST SP 800-53 Rev. 4** AU Family, SC-28 **ISO/IEC 27001:2013** A.8.2.3, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
Data integrity information must be secure	PR.DS-1 PR.DS-6	**NIST SP 800-53 Rev. 4** SC-28, SI-7 **ISO/IEC 27001:2013** A.8.2.3, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
Back-ups must be secure	PR.DS-1 PR.IP-4	**NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9, SC-28 **ISO/IEC 27001:2013** A.8.2.3, A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
Ability to detect and report on all file modifications/creations/deletions	PR.DS-1 PR.PT-1 DE.CM-1	**NIST SP 800-53 Rev. 4** AC-2, AU Family, CA-7, CM-3, SC-5, SC-7, SC-28, SI-4 **ISO/IEC 27001:2013** A.8.2.3, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1

Solution Characteristic	NIST CSF Category	Informative References
Ability to detect and report on all database modifications/creations/deletions	PR.DS-1 PR.PT-1 DE.CM-1	**NIST SP 800-53 Rev. 4** AC-2, AU Family, CA-7, CM-3, SC-5, SC-7, SC-28, SI-4 **ISO/IEC 27001:2013** A.8.2.3, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
Ability to correlate file change with user	PR.PT-1 DE.CM-1 DE.CM-3	**NIST SP 800-53 Rev. 4** AC-2, AU Family, CA-7, CM-3, CM-10, CM-11, SC-5, SC-7, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
User activity recording	PR.PT-1 DE.CM-3	**NIST SP 800-53 Rev. 4** AC-2, AU Family, CA-7, CM-10, CM-11 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
User activity anomaly detection	PR.PT-1 DE.CM-1 DE.CM-3	**NIST SP 800-53 Rev. 4** AC-2, AU Family, CA-7, CM-3, CM-10, CM-11, SC-5, SC-7, SI-4 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
Configuration management (install, monitor, recover)	PR.DS-1 PR.IP-3 PR.IP-9 PR.PT-1 DE.AE-4	**NIST SP 800-53 Rev. 4** AU Family, CA-7, CM-3, CM-4, CP-2, IR-4, IR-5, IR-8, SA-10, SC-28, SI-4 **ISO/IEC 27001:2013** A.8.2.3, A.12.1.2, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.5.1, A.12.6.2, A.12.7.1, A.14.2.2, A.14.2.3, A.14.2.4, A.16.1.1, A.17.1.1, A.17.1.2

Table 1: Solution to security category map

The list of characteristics and corresponding capabilities is not exhaustive. Furthermore, capabilities are listed to provide context for the characteristics and are not meant to be prescriptive.

APPENDIX A – REFERENCES

[1] NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1, February 12, 2014 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[2] "Joint Statement: Destructive Malware." Ffiec.gov. March 30, 2015. Accessed July 10, 2015. https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC Malware.pdf.

[3] Karen Scarfone, Murugiah Souppaya, Paul Hoffman. "NIST Special Publication 800-125 Guide to Security for Full Virtualization Technologies" NIST.gov January 2011 http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

[4] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[5] Financial Sector Information Sharing and Analysis Center Best Practices for U.S. Financial Institutions, Reducing Risks Associated with Destructive Malware, November 2, 2015

[6] Souppaya, Murugiah, and Karen Scarfone. "NIST Special Publication 800-83 Rev 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops." NIST.gov. July 1, 2013. Accessed August 29, 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

[7] "Spotting the Adversary with Event Log Monitoring". NSA.gov. December 16, 2013. Accessed August 17,2015. https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf

[8] "Eight Best Practices for Disaster Recovery." CIO.com. November 18, 2004. Accessed August 29, 2015. http://www.computerworld.com/article/2568383/disaster-recovery/eight-best-practices-for-disaster-recovery.html

[9] Ron Ross, Janet Carrier Oren, Michael McEvilley "NIST Special Publication 800-160 draft Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems" NIST.gov May 2014 http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

[10] Arnold Johnson, Kelley Dempsey, Ron Ross, Sarbari Gupta, Dennis Bailey "NIST Special Publication 800-128 Guide for Security-Focused Configuration Management of Information Systems" NIST.gov August 2011 http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf

[11] The CIS Critical Security Controls for Effective Cyber Defense, version 6. Center for Internet Security. October 15, 2015

[12] Federal Enterprise Architecture Framework, version 2. January 29, 2013 https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

[13] Richard Kissel, "NISTIR 7298, Glossary of Key Information Security Terms, revision 2" May 2013 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

APPENDIX B - ACRONYMS AND ABBREVIATIONS

CSF	Framework for Improving Critical Infrastructure Cybersecurity
FS-ISAC	Financial Sector ISAC
ISACs	Information Sharing and Analysis Centers
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology

APPENDIX C – GLOSSARY

Active attack: An attack that alters a system or data SOURCE: CNSSI-4009

Adversary: Individual, group, organization or government that conducts or has the intent to conduct detrimental activities. SOURCE: SP 800-30

Agent: A program acting on behalf of a person or organization

Alert: Notification that a specific attack has been directed at an organization's information systems. SOURCE: CNSSI-4009

Analysis: The examination of acquired data for its significance and probative value to the case

Antivirus software: a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. SOURCE: SP 800-83

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. SOURCE: SP 800-32

> Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. SOURCE: CNSSI-4009

Configuration control: process of controlling modification to hardware, firmware, software, and documentation to protect the information system against improper medication prior to, during, and after system implementation

Continuous monitoring: maintaining ongoing awareness to support organizational risk decisions

Cyber attack: an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disruption, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks. SOURCE: CNSSI-4009

Data: A subset of information in an electronic format that allows it to be retrieved or transmitted SOURCE: CNSSI-4009

Data Integrity: The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. SOURCE: SP 800-27

The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. SOURCE: CNSSI-4009

Data Loss: The exposure of proprietary, sensitive, or classified information through either data theft or data leakage SOURCE: SP 800-137

Data Security: Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure SOURCE: CNSSI-4009

Decrypt: Generic term encompassing decode and decipher SOURCE: CNSSI-4009

Encrypt: Generic term encompassing encipher and encode. SOURCE: CNSSI-4009

Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g. budgets), human resources, security, and information systems, information and mission management. SOURCE: CNSSI-4009

Incident: A violation of imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. SOURCE: SP 800-61

Last known good configuration: a MS Windows startup option that uses the most recent system settings that worked correctly. SOURCE: http://windows.microsoft.com/en-us/windows/using-last-known-good-configuration#1TC=windows-7

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. SOURCE SP 800-83

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to performs its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. SOURCE: CNSSI-4009

Threat: Any circumstance or event with the potential to adversely impact organization operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. SOURCE: CNSSI-4009

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200