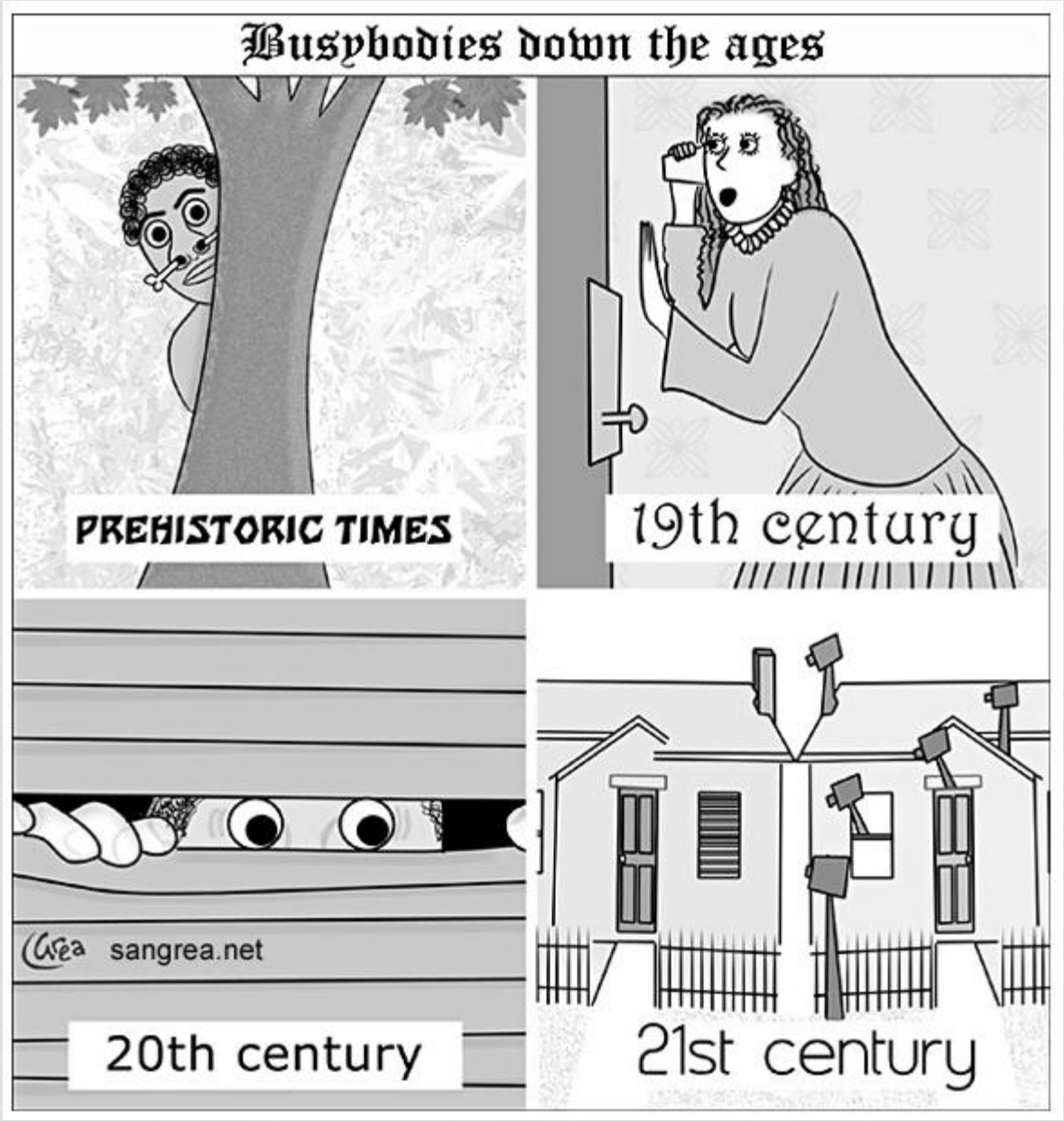
PRIVACY/SECURITY

JULY 7, 2016

ADDITIONS BY JACK KOLK, CISSP, CSSLP


Busybodies down the ages
PREHISTORIC TIMES
19th century
sangrea.net
20th century
21st century

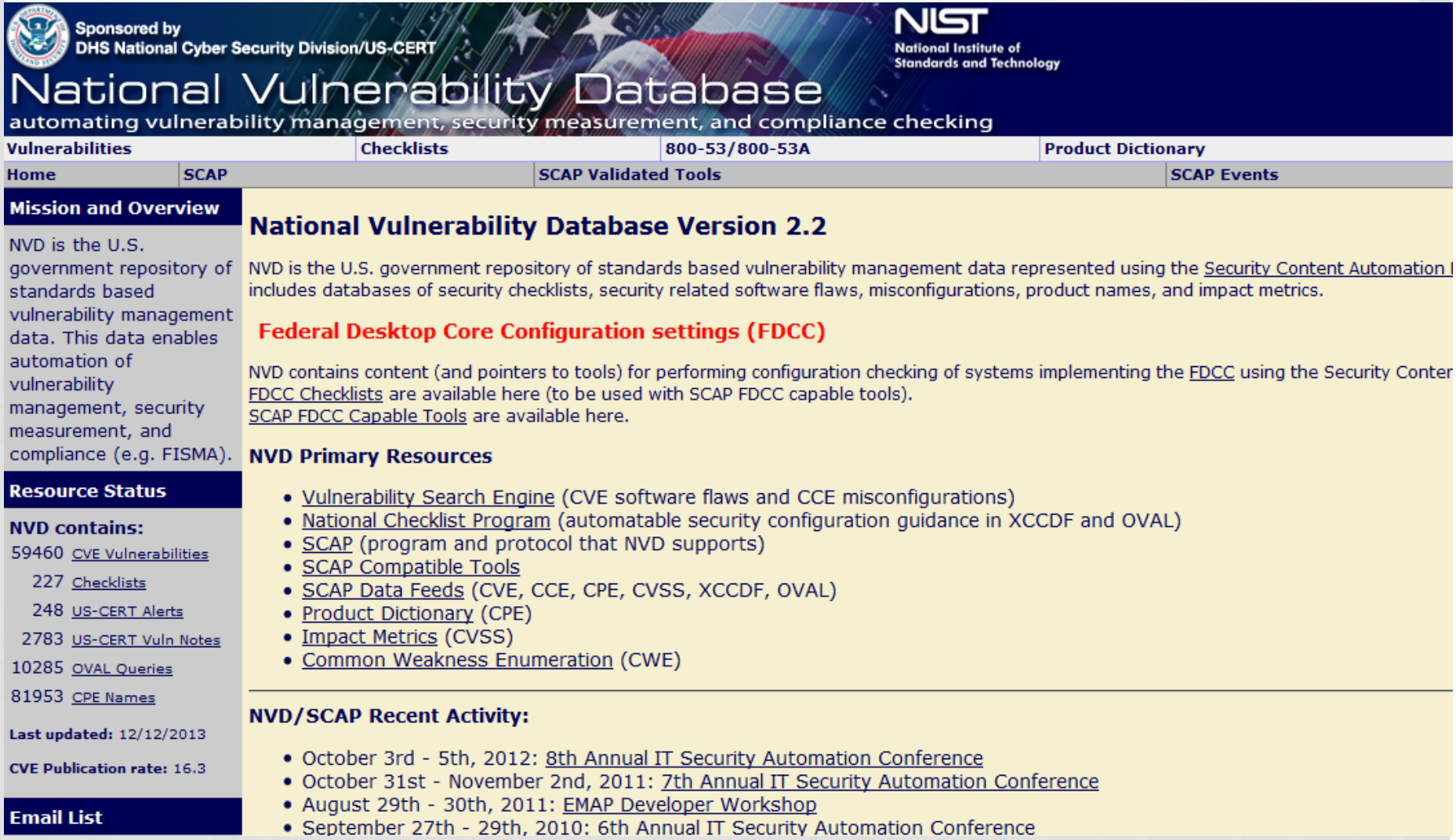
CONTENT

- General
  - Healthcare Environment (19)
  - Technology Environment (10)
- Systems
  - Analysis (14)
  - Design (5)
  - Selection, Implementation, Support, and Maintenance (8)
  - Testing and Evaluation (3)
  - Privacy and Security (6)
- Administration
  - Leadership (29)
  - Management (6)

PRIVACY & SECURITY OBJECTIVES

1. Participate in defining organizational privacy and security requirements, policies and procedures
2. Utilize procedures and tools to identify potential privacy and security breaches
3. Provide appropriate physical environment and safeguards to protect assets
4. Assess privacy and security risks
5. Implement processes to mitigate privacy and security vulnerabilities
6. Manager user access control according to established policies and procedures
7. Ensure confidentiality, integrity, and availability of data
8. Define organization roles (e.g., information security, physical security, compliance) responsible for managing vulnerabilities
9. Develop data management controls (e.g., data ownership, criticality, security levels, protection controls, retention and destruction requirements, access controls)
10. Maintain disaster recovery and business continuity plans
11. Perform privacy and security audits

VULNERABILITIES ARE MORE COMMON THAN YOU KNOW AND GROWING



VULNERABILITIES ARE MORE COMMON THAN YOU KNOW AND GROWING

Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics | FAQs

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments | Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

71073 CVE Vulnerabilities
298 Checklists
249 US-CERT Alerts
4369 US-CERT Vuln Notes
10286 OVAL Queries
104958 CPE Names

Last updated: 7/8/2015 2:57:45 PM

CVE Publication rate: 19.33

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

National Vulnerability Database

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Announcements

CVSS v3 Preview Information

CVE-ID Format Change Information

Federal Desktop Core Configuration settings (FDCC) / United States Government Configuration Baseline (USGCB)

NVD contains content (and pointers to scanning products) for performing configuration checking of systems implementing the FDCC/USGCB using the Security Content Automation Protocol (SCAP).
FDCC/USGCB Checklists are available here (to be used with SCAP 1.2 validated tools).
SCAP Validated Products are available here.

NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)

NVD/SCAP Recent Activity:

- September 9th - 11th, 2015: 2015 Cybersecurity Innovation Forum
- January 28th - 30th, 2014: 2014 Cybersecurity Innovation Forum
- October 3rd - 5th, 2012: 8th Annual IT Security Automation Conference

INTRODUCTIONS

- Multiple laws, regulations, standards for privacy and security
  - ISO
  - FISMA
  - HIPAA
  - Gramm-Leach-Bliley (GLB) 1999
  - PCI Processing Rules
  - UK Data Protection Act of 1998
  - European Data Protection Directive
- NIST is emerging as the de facto standard

PRIVACY VS SECURITY

- Privacy tends to define WHAT
  - Information/data is to be held confidential and is permitted to be disclosed to those with a need to know
- Security is the HOW
  - Set forth the technical, physical and procedural controls or limits

KROLL PREDICTS THAT THE NEW CYBERSECURITY ISSUES FOR 2014 WILL INCLUDE:

National Institute of Standards and Technology (NIST) and similar security frameworks will become the de facto standards of best practices for all companies: Cybersecurity strategies largely designed for companies that were part of the "critical infrastructure" will become more of an expectation for everyone, from conducting an effective risk assessment to implementing sound cybersecurity practices and platforms. Organizations that don't follow suit may find themselves subject to shareholder lawsuits, actions by regulators and other legal repercussions.

Alan Brill, senior managing director at Kroll, said this trend will move the United States in the direction of the EU, where there is a greater recognition of privacy as a right.

KEY COMPONENTS OF PRIVACY LAWS

- General rules of privacy
- Individual rights
- Privacy Administration requirements
- General Security

GENERAL RULES OF PRIVACY

- What data is to be protected
- How data is to be used, disclosed and safeguarded
- Which organizations are affected and covered by the rules

INDIVIDUAL RIGHTS

- Greater control of data by the individual
  - Right of access
  - Right to restrict access
  - Confidential communication channels
  - Accounting of disclosures
- Personal Representative
  - Gains access on behalf of the individual when that person is incapable of making decisions

PRIVACY ADMINISTRATIVE REQUIREMENTS

- Designation of privacy/security officer
  - Development of policies and procedures
  - Processing of complaints
  - Monitoring of ongoing compliance
  - Training program
  - Sanctions program

GENERAL SECURITY

- Controls of limitations on the data contained in systems
- Controls regarding the workforce members
- Controls regarding the physical environment where the data and people reside

COMPLIANCE PROCESS

- Awareness
- Assessment
- Remediation
- Maintenance

ASSESSMENT

- The process of identifying how an organization's current practices differ from international, federal and state laws, requirements and standards

DOCUMENT GATHERING

- General: Organizational charts, new employee training materials, results from the previous internal and external audits
- Workforce Information (Administrative): Employee handbook, Security and Privacy training materials, disclosure/sanctions policies, system use auditing and reporting
- Physical Safeguards: Related workforce clearance/access ability to physical structures, inventory of all software, portable devices, media, policies/procedures governing workstation security
- Technical Safeguards: Network diagrams, policies/procedures defining electronic access privileges, audit and integrity controls, authentication of person or entity, controls for transmission security

GAP ANALYSIS

- Compare regulatory requirement to organization's current baseline
- Determine the extent of the gaps
- Identify the steps necessary to achieve compliance

FACILITY WALKTHROUGH

- Goal is to identify areas which could result in unauthorized access to health information
  - Terminal Access
  - Facility Controls
  - Employee Interviews

TECHNICAL BASELINE

- Identify network infrastructure, network access points and network vulnerabilities from which to measure compliance gaps.
- Sample techniques may include:
  - Domain footprint
  - Vulnerability Scans
  - Ping Sweeps, Port Scans etc.
    - Port scans take ping sweeps to a different level. Port scans actually "look" at a machine that is alive and scan for an open port. Once the open port is found, it scans the port to find the service it is running. Once it finds the service the port is running, it gives the intruder power and knowledge about your system.
  - Password Evaluations
  - Network Port Scans

THREATS AND VULNERABILITIES

- Identification of threats
- Identification of Vulnerabilities
  - NIST ICAT vulnerability database:
    - http://icat.nist.gov
- Likelihood Determination
- Impact Analysis
- Risk Determination

THREATS AND VULNERABILITIES

- Threats are constantly evolving, you need to keep Up!

Hacker's Paradise – New Virus Transfers Stolen Data Using Inaudible Sounds

Posted by Sharon Solomon on Fri, December 6, 2013 @ 05:37 PM

4 Like | 0 Email | 1 Tweet | 1 +1 | 46 Share

Air-Gap Jumping Communication. Networkless hacking. Sci-fi movie themes are now turning into reality. German researchers Michael Hanspach and Michael Goetz have created what can potentially become the driving force behind the next-gen malware. Security experts be warned – offline computing is not going to be safe for long.

Inaudible sound signals can now carry stolen data, without requiring internet access. Any compromised laptop can be used as a communication hub that receives and transmits information. This is achieved by using the machine's audio hardware, even when the computer is offline.

Offline Computing Is Safe No More

Security researcher Dragos Ruiu claimed earlier this year that spyware dubbed badBIOS can link infected machines using sound wave signals alone. The IT community took this claim very sarcastically. But the latest German study has proved the doubters wrong and validated Ruiu's claims.

The findings at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) were quite conclusive. Two regular Lenovo business laptops were infected and used during the study. Signals in the low ultrasonic frequency range of around 20,000 Hz were conveyed to a distance of almost 20 meters at a rate of 20bps.

REMEDIATION

- The process of closing the gaps between current privacy and security practices and the requirements, laws, and standards

POLICIES AND PROCEDURES (P&P)

- Identify representative team to develop P&P
- Collect existing P&P that relate to privacy and security
- Identify business partners
- Interview supervisors and front line workers
- Contact trade associations, state bar, and other sources of information on relevant regulations, standards, and laws for your region
- Place draft P&P into customary "project plan" process

PHYSICAL ENVIRONMENT

- Cleaning Personnel
- Computer Screens
- Conversations
- Copying Health Information
- Desks/Countertops
- Disposal of Paper
- Home Office
- Information carried between buildings
- Key Policy
- PDAs
- Printers and Faxes
- Record Storage
- Workforce Vigilance
- Visitors

TECHNICAL ACCESS CONTROLS

- Minimum Necessary
- Principles for Access Profiles
  - Access to information must not be so restricted as to interfere with the quality and efficiency of healthcare
  - Access shall be sufficiently restricted to afford patients'/members' information as much privacy and security as possible
- Modification or Termination of Access

DATA MANAGEMENT CONTROLS

- Device and Media Controls
- Electronic Transmission of Health Information
- Integrity
- Data Authentication Controls
- Authentication of Person or Entity

MAINTENANCE

- The process of maintaining compliance – confirming that changes to policies and procedures have actually taken place and that staff has been trained to adhere to the new policy

TRAINING

- Methods of Training
  - Direct review of P&P
  - Powerpoint slides and lectures
  - Online/automated training
  - Use of examples/vignettes
  - Use of video
- Training Content
  - Awareness training
  - Workstation use
  - P & P
  - Sanctions/testing
- Training Delivery Controls

RISK MANAGEMENT

- Risk Assessment – The process to determine initial level of risk
- Risk Mitigation – The process to decrease the determined level of risk
- Evaluation and Assessment – The process to monitor and take action to maintain the decreased level of risk

AUDITING/MONITORING TOOLS

- Self Audit
  - Checklists
  - Facility walkthroughs
  - Interviews
- Report of Findings
  - Areas of Non-compliance
  - Corrective Action Plans

PRIVACY AND SECURITY INCIDENTS

- Implement Processes to:
  - Respond quickly to an alleged breach
  - Determine what occurred
  - Prevent recurrence of any violation or policy or law
  - Take steps to mitigate any harm
- Train All Workforce Members on Incident Reporting Processes (which needs to be in place!)

AUDIT TRAIL

- Provides a mechanism to monitor user activity (accountability by individual)
- Provides a mechanism to identify suspicious activity and/or breaches of information
- Provides necessary data for the organization to reconstruct any past events where integrity of data may be questions
- The act of monitoring functions as a deterrent to internal workforce members from seeking inappropriate access to health and other sensitive information

CONTINGENCY PLANNING

- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing and Revision
- Applications and Data Criticality Analysis

QUESTION 32

- Which of the following best describes the general concepts of privacy?
  - A. how data is to be protected, safeguarded, used, disclosed.
  - B. which organizations are covered by the rules.
  - C. which technology is to be used to safeguard data.
  - D. data integrity and availability.

ANSWER 32

- A. General privacy rules deal with an organization's ability to keep information protected, and to define to whom and when it is to be used or disclosed.

QUESTION 33

- The CIO of a health plan is gathering information related to the security posture of the organization in preparation for a security gap analysis. Which of the following is LEAST useful?
- A. network diagrams
- B. existing policies and procedures
- C. organizational charts
- D. credentialing data

ANSWER 33

- D. Credentialing information is not directly relevant to the security posture of the health plan.

QUESTION 34

- Which of the following best describes the general process of gap analysis for privacy and security compliance?
- A. identifying the gaps between legacy and target systems
- B. comparison of the regulatory requirements to the organization's current baseline
- C. comparison of different business functions within an organization
- D. analysis of industry best practices as compared with an organization's practices

ANSWER 34

- B. The general process of conducting a gap analysis includes comparing the requirements of the regulation (or law or other requirement) with the organization's current conduct specific to the requirement in question.

QUESTION 35

- The ability for an organization to ensure electronic health information in its possession is kept consistent with its source, protecting the data from improper alteration or destruction is defined as
- A. authentication
- B. integrity
- C. verification
- D. security

ANSWER 35

- B. Keeping data integrity means that the data is kept true to its source and that it is not inappropriately accessed, changed, altered, or destroyed.

QUESTION 36

- Which of the following would be the LEAST important consideration when implementing technical access controls?
- A. minimum necessary definitions
- B. principles for access profiles
- C. termination or modification of access
- D. general ledger data

ANSWER 36

- D. When implementing technical access controls, answers a, b, and c are all important considerations; answer d is not related.