August 9, 2017

Hacking Healthcare
TLP White

Policy Analysis –

On Monday, The National Institute of Standards and Technology published a cybersecurity workforce framework (SP-800-181). The NICE framework (as we'll call it to differentiate from the NIST Cybersecurity Framework) is designed to enable a "common, consistent lexicon" for cybersecurity work within organizations and across sectors and the economy. The release of the NICE framework comes after nearly a decade of work by NICE - the National Initiative for Cybersecurity Education, a public-private program housed within NIST.

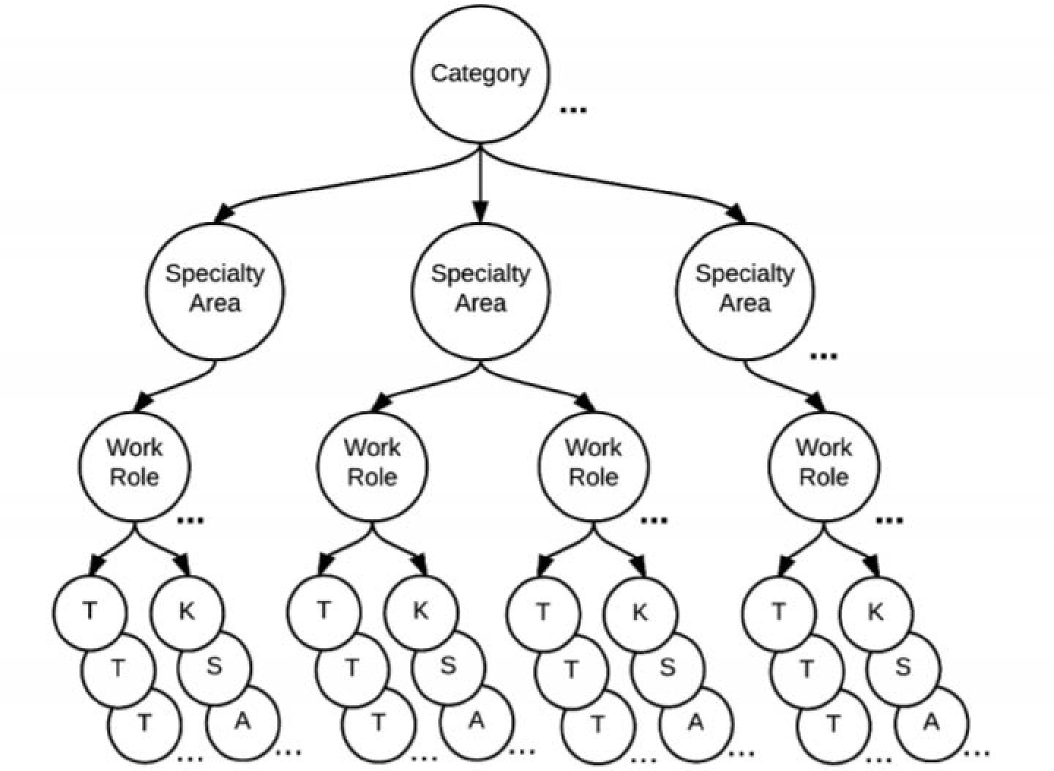


Figure 1 - Relationships among NICE Framework Components

August 9, 2017

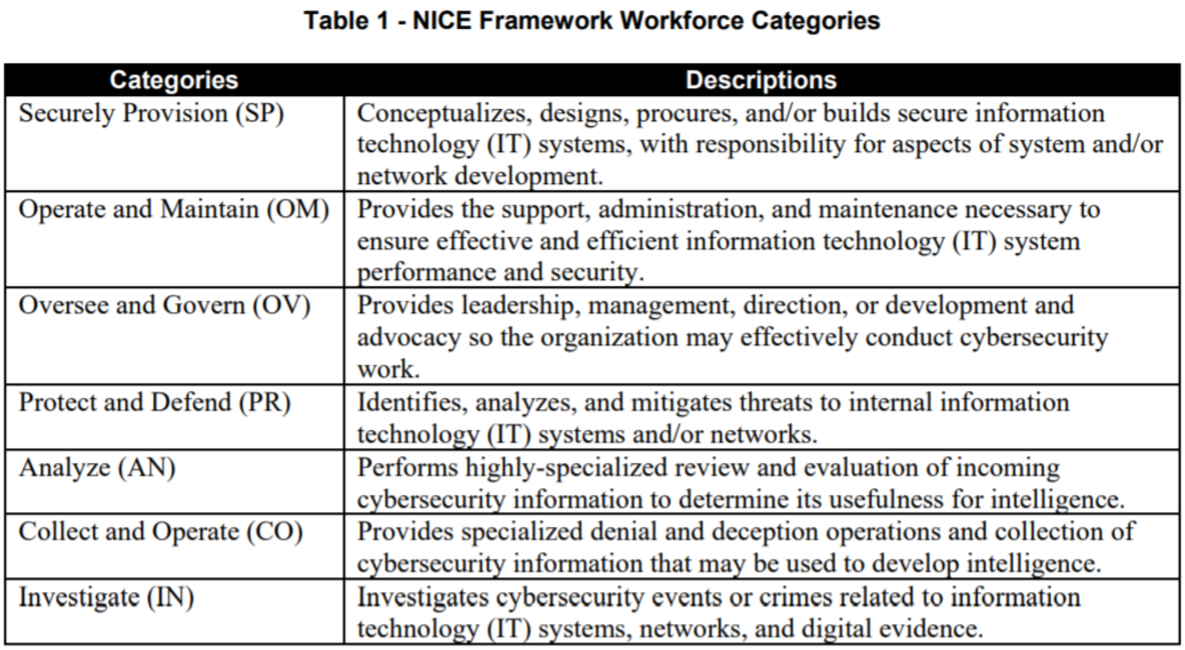


Table 1 - NICE Framework Workforce Categories

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Hot Links –

--On August 2, the President signed into law H.R. 3364 - Countering America's Adversaries Through Sanctions Act. The bill codified Obama Administration executive branch sanctions against Russia, including Russian cyber actors, meaning the Trump Administration must file a waiver with Congress if it is to rescind such sanctions. The bill also calls on the Administration to establish sanctions by October 1 against additional Russians deemed responsible for "significant activities undermining cybersecurity" – a qualifier left noticeably vague. Finally, the bill provides $250mm in funding over the next two years for the cyber-defenses of critical infrastructure and electoral processes within NATO and near-NATO allies.

--This week DHS announced that its CIO will resign. This follows other recent CIO departures including at Treasury. Some have speculated that this is part of an Administration-wide effort to shift the CIO position from a career post to one that is politically appointed. There are pros (e.g., influence with the Secretary and White House, ability to regularly infuse new ideas from leadership) and cons (e.g., lack of historical perspective, connection to career staff, federal IT skill set) to such an approach. We'll keep an eye out for additional announcements in this space.

--Marcus Hutchins (aka, MalwareTech), the researcher who found and activated the WannaCry 'Kill Switch,' was arrested as he left Defcon and indicted on criminal charges related to the creation and distribution of the Kronos banking trojan. He plead not guilty and was released on $30,000 bail. His next hearing is on Monday. Some within the security community have helped raise funds for his bail and legal defense. We'll be watching this case as it plays out, as well as any impact it has on the research community.

--The Department of Justice released a bug bounty guidance (cyber scoop)
--ICS-CERT alert issued for multiple Siemens medical vulnerabilities (SC)
--CareFirst customers granted right to sue over 2014 cyberattack (cyber scoop)

--Medical Device Cybersecurity Act Draws Industry Support (healthITsecurity)
--New Bill Seeks Basic IoT Security Standards (Krebs)
--Amazon Secret Healthcare IT Tech Team Focuses on EHRs, Alexa (healthITsecurity)

The Week Ahead –

Administration activity–
--Secretary Mattis to visit Seattle and Silicon Valley (8/10-11)
--Secretary Tillerson and Mattis to meet with Japanese Counterparts on cybersecurity (8/17)

Congressional Activity – The House and Senate are both in recess, though the Senate continues *pro forma* sessions, which means that recess appointments are unlikely. Both chambers are likely to return to business after Labor Day on September 5.

The Senate will be holding certain field hearings throughout the month:
--Field Hearing in Duluth, MN: Veteran Care in Rural Areas: Increasing Access through Choice and Capacity Improvement (8/10, 9:30 AM CDT – Senate Veteran Affairs)

Conferences and Webinars –
--HIPAA and the Compliance Officer (webinar) (8/9)
--Health IT Summit – Philadelphia (8/10)
--Basic Best Practices in Cybersecurity – Kentucky (NH-ISAC) (8/14)
--HIPAA Covered Entities: Managing the HIPAA Business Associate Process (webinar) (8/14)
--Free DMARC Webinar by Global Cyber Alliance: Brand Protection (8/15)
--HIPAA Hybrid Entities - What if Healthcare is only a part of what you do (webinar) (8/17)
--Basic Best Practices in Cybersecurity – Texas (NH-ISAC) (8/23)
--HIPAA Training for the Business Associate (webinar) (8/23)
--HIPAA and Personal Devices (webinar) (9/5)
--Basic Best Practices in Cybersecurity – Minnesota (NH-ISAC) (9/6)
--Medical Device Workshop at Medtronic – Mounds View, MN (NH-ISAC) (9/7)
--HIMSS Healthcare Security Forum (9/11-13)

Breaches –
--Australian Red Cross data breach caused by third-party error (SC)

Reports –
--Breach Barometer Mid-year Review (Protenus)
--Magic Quadrant for Web Application Firewalls (Gartner)
--GTIC 2017 Q2 Threat Intelligence Report (NTT Security)

Podcasts –
--Cyber Insurance: Overcoming Resistance (Healthcare Information Security Podcast)

August 9, 2017

Sundries –

August Vacation reading:

--Let your kids hack! (Reuters)

Policy and government cybersecurity:

--10 Members of Congress rake FCC over the coals in official net neutrality comment (techcrunch)
--One broadband choice still counts as "competition" after court decision (Ars)
--Senior US Official Claimed the FCC Got 'Hacked' After Security Professionals Found No Proof (gizmodo)
--U.S. government's cyber Scholarship-for-Service program would expand under Senate bill (cyber scoop)
--National Security Council cyber officials depart (politico)
--UK to strengthen data protection law (gov.uk)
--UK essential service operators with poor cyber security face massive fines (helpnet)
--Exclusive: FBI tracked 'fake news' believed to be from Russia on Election Day (CNN)
--De Blasio signs executive order to launch city 'cyber command' (NYPost)
--Suspected sextortionist hiding behind Tor is outed by booby-trapped video (Ars)
--Malware campaigns hit North Korea following nuclear ICBM tests (cyber scoop)

Op-eds:

--No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession (LawFare)
--You Can Thank Leakers for New Russia Sanctions (Bloomberg View)
--Theories of Harm in Data-Breach Litigation (LawFare)

Tech:

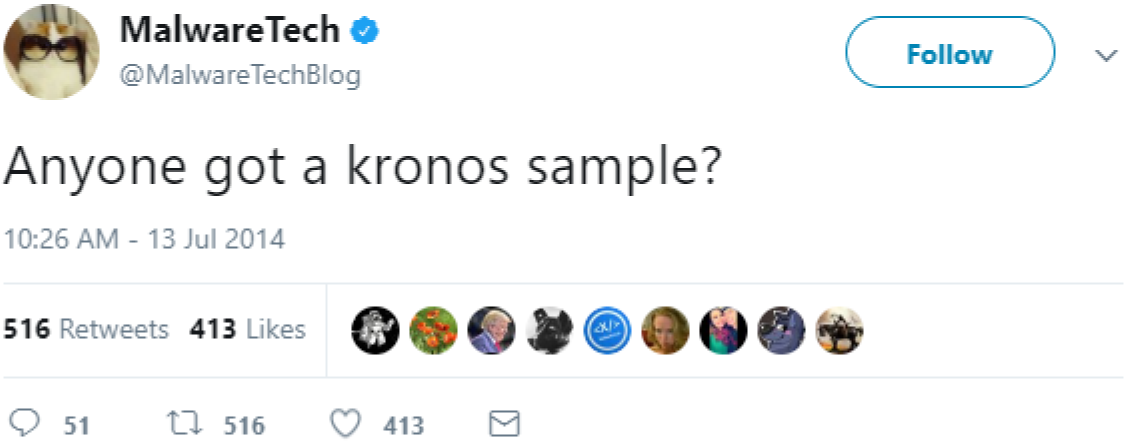
--Hotspot VPN accused of violating user privacy agreements (cnet)
--Mozilla's new file transfer service 'Send' (Ars)
--IBM Claims Big Breakthrough in Deep Learning (Fortune)
--Android 8.0's "streaming OS updates" will work even if your phone is full (Ars)

Network defense and threats:

--How to Choose the Right Data Protection Strategy (infosec island)
--Malicious content delivered over SSL/TLS has more than doubled in six months (helpnet)
--Automating Defenses Against Assembly-Line Attacks (Dark Reading)
--What leads women to cybersecurity, and what makes them stay? (helpnet)
--Cyber threats prompt return of radio for ship navigation Cyber threats prompt return of radio for ship navigation (Reuters)
--A Baccarat Binge Helped Launder the World's Biggest Cyberheist (Bloomberg)
--Game of Thrones hackers demand ransom (bbc)

August 9, 2017

(In)Secure Takes –



MalwareTech
@MalwareTechBlog

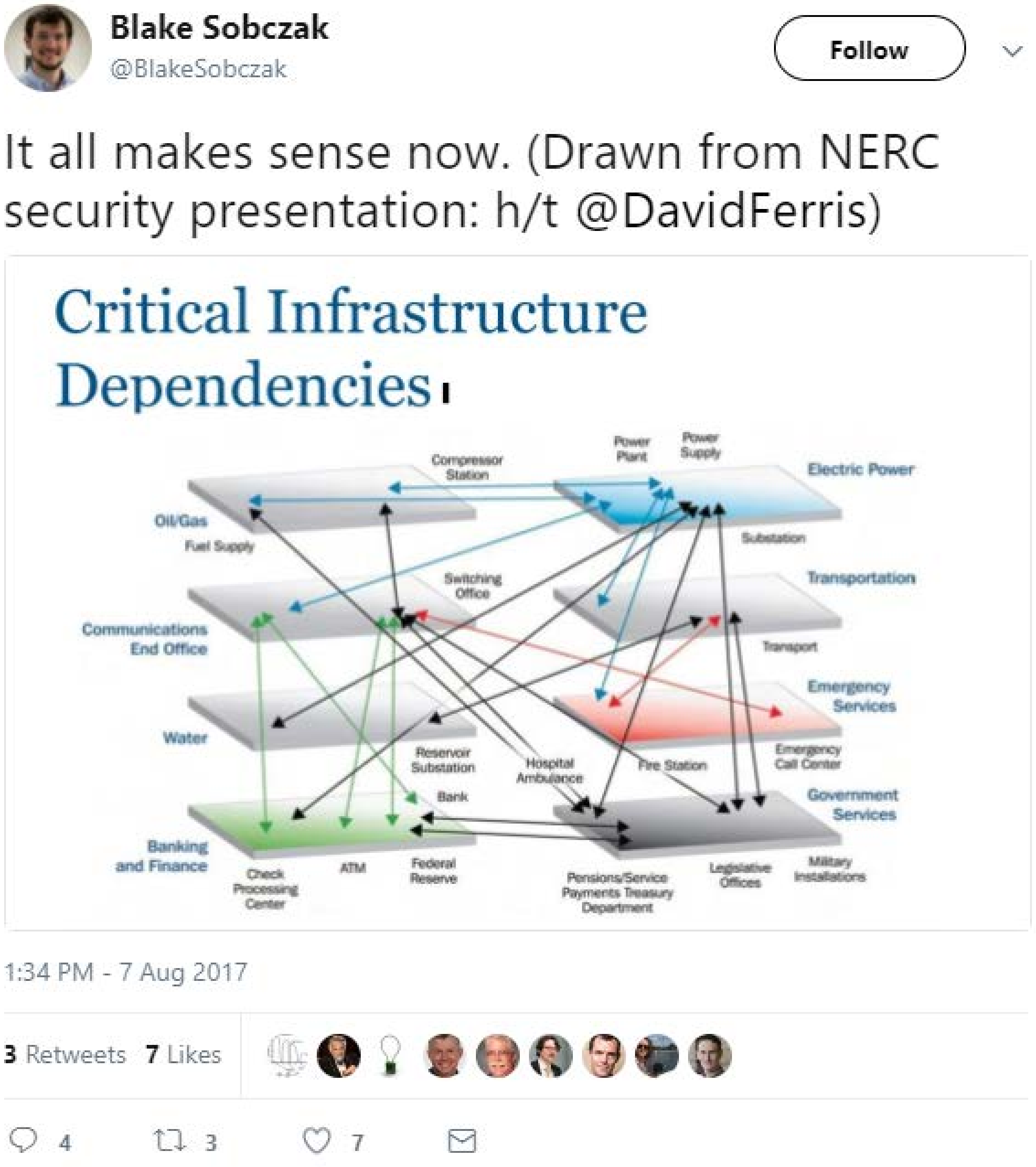
Anyone got a kronos sample?

10:26 AM - 13 Jul 2014

516 Retweets 413 Likes

51 516 413

August 9, 2017



Blake Sobczak
@BlakeSobczak

It all makes sense now. (Drawn from NERC security presentation: h/t @DavidFerris)

Critical Infrastructure Dependencies

1:34 PM - 7 Aug 2017

3 Retweets 7 Likes

Contact us: follow @NHISAC and email at bflatgard@nhisac.org