



P&RCIO NEWSLETTER

SERVING THE P&R COMMUNITY
VOLUME 3, ISSUE 3



SPRING 2011

Personnel and Readiness (P&R) Hosts an Information Technology (IT) Summit

POINTS OF INTEREST:

- Personnel and Readiness Hosts IT Summit
- Emerging Threats to Cyber Security
- Information Assurance Symposium

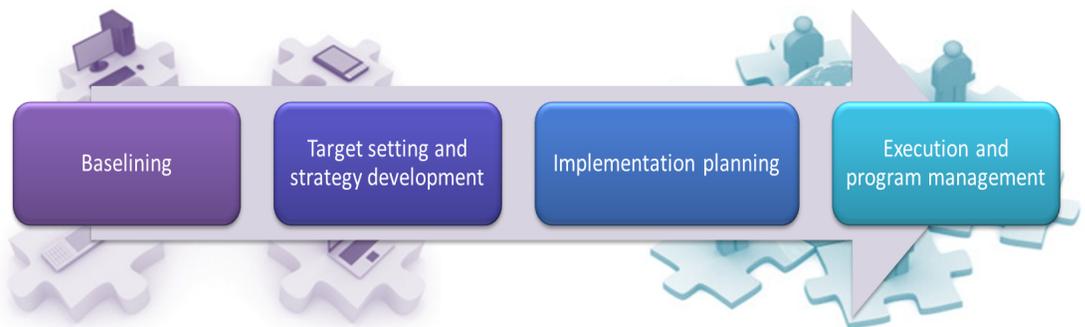
In August 2010, the Secretary of Defense issued a memorandum directing a Department of Defense (DoD)-wide effort to consolidate information technology (IT) assets. On December 6, 2010, Dr. Clifford Stanley issued a memorandum requesting support for an Office of the Under Secretary of Defense (OUSD) Personnel and Readiness (P&R) IT Summit. The purpose of this event was to bring senior leaders together to focus on streamlining IT functions across the P&R enterprise and generate savings for the Department. Attendees included IT leadership from Civilian Personnel Management Service (CPMS), Defense Commissary Agency (DeCA), Defense Manpower Data Center (DMDC), Defense Personnel Security Research Center (PERSEREC), Defense Travel Management Office (DTMO), Department of Defense Education Activity (DoDEA), Federal Voting Assistance Program (FVAP), P&R, P&R Information Management (IM), Requirements and Strategic Integration

(RSI), Reserve Affairs (RA), TRICARE Management Activity (TMA), and Wounded Warrior Care and Transition Policy (WWCTP).

RSI and P&R IM hosted a Summit Kick-off on Tuesday, February 1, 2011. Mr. Jim Neighbors, Principal Deputy of RSI, communicated the goal of the effort, which was to find ways to improve processes and performance without causing harm to the mission. P&R reviewed the four-step approach to this effort: baselining, target setting and strategy development, implementation planning, and execution and program management. Following the Summit Kick-off, P&R collected information and conducted interviews with its organizations. P&R analyzed the data collected with the goal of identifying priority opportunity areas. The end result of this work was a baseline analysis of existing assets, performance, and health of the various P&R organizations. The findings from this baseline analysis were used as a starting point for discussion at the P&R IT Summit

held on Wednesday, March 16, 2011. These findings focused on four areas: infrastructure, application development and maintenance, overhead and support, and end users.

Summit discussion resulted in recommendations to implement enterprise-wide software licensing across P&R, leverage enterprise-wide hardware purchasing, consolidate data centers and reduce their overall footprint, implement virtualization, improve call center and help desk efficiency, and address IT governance across P&R. At the Summit, P&R provided an individual analysis to each organization; attendees will review these analyses and determine their best ideas for future savings. Organizations will lead working groups based on their specific thoughts, and some will pilot their cost-saving ideas. Moving forward, P&R will gather additional information from each organization for future analysis to be presented at a follow-up Summit in the May 2011 timeframe.



A New Decade, A New Threat: Emerging Trends in Cyber Threats

In a recent analysis, security firm Kaspersky Lab created a cyber threat forecast for 2011-2020 based on major issues and developments that have come to exemplify the last decade of technology. The study identified several key trends that have affected the way we do business as well as conduct our personal lives.

These key trends included:

- Mobility allowing Internet access from virtually anywhere
- Exponential growth and competition in mobile platforms
- Viruses and malware transforming from nuisance to cyber threat
- Waning dominance of Microsoft Windows™ in the personal computer (PC) market
- Social networking and search engines driving Internet usage to new heights
- E-commerce transforming into a legitimate and viable alternative to the traditional bricks-and-mortar shopping experience



Kaspersky forecasted that the most defining change for the next decade will be the continued migration from Windows as the goliath in the PC market to the growing number of non-Windows based alternatives, both in the mobile and non-mobile arenas. While exploiting vulnerabilities in Windows machines will continue to play a major role in cyber threats due to the sheer number of machines running the operating system (OS) globally, it could be very lucrative for would-be attackers to target these newer platforms where the old adage

‘security through obscurity’ has run rampant, including those developed by the rising star of the last decade: Apple.

Users continue to utilize mobile platforms for communication, e-commerce, news, and entertainment at an exponential rate as being constantly connected is increasingly being seen as a necessity to many users. Unfortunately, many mobile platforms currently provide little in the way of OS and application security via traditional methods used on our personal and business machines, including anti-virus and anti-malware programs. This lack of security, combined with the remarkable computing power of mobile devices that now allows users to perform many of the same functions they would on PCs, provides attackers with new avenues to unleash cyber threats such as mobile botnets, spam, and phishing attacks.

Source: www.securelist.com/en/analysis/204792165/Cybercrime_Outlook_2020_From_Kaspersky_Lab

2011 Information Assurance Symposium in Nashville

For many years, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and the United States Cyber Command has conducted an annual Information Assurance (IA) Symposium. This year’s event was organized into five themes focusing on partnering, sharing, preventing and detecting attacks, cyber readiness, and contingency environments. It was an excellent opportunity to learn more about how IA is vital to the mission, protection of vital assets, equipment, facilities, and - most importantly - the lives of citizens and warfighters.

Some of the topics of interest at the

symposium were “Open Source Threats,” “The Courts and Cyberspace,” “Roadblocks to IA Certification and Accreditation Reciprocity and How to Break Through the Barriers,” “Operations Security and Social Networking,” and “Information and Mission Centric Security Strategy.” These and many other tracks highlighted lessons learned from key events, opportunities, or initiatives of interest to the IA community and provided an opportunity to emphasize the need for proactive collaboration among cyber professionals in government, industry, and academia.

For more information on the IA Sym-

posium, please visit www.nsa.gov/ia/events/index.shtml or the Symposium Expo page at www.informationassuranceexpo.com.

