OEM: Weekly SITREP

October 12, 2021
USA & WORLD

- US schools gave kids laptops - then they spied on them.
- WHO calls for climate action to assure sustained recovery.
- Texas school shooting leaves four injured.
- Justice Department: Threats against School Officials.
- World experiencing a cybercrime pandemic.
- Studies (1, 2) warn US could see 'twindemic.'
- 4 key points from Facebook whistleblower's testimony.
- FDA authorizes ACON Laboratories Flowflex home test.
- US deaths from virus in 2021 surpass 2020 total.
- J&J seeks FDA clearance for booster shots.
- Burnout isn't just fatigue. It's far more insidious.
- China purchased PCR tests months before first reported case of COVID - findings challenge beginning of pandemic.
- Study: Trends in anxiety & depression severity during pandemic.
- NIH Director to step down by the end of year.
- AstraZeneca asks FDA for emergency authorization for AZD7442 antibody treatment to prevent COVID.
- How being unvaccinated can impact your wallet.

Figure 1. Monthly Outlays Fiscal Years 2019, 2020, 2021
Billions of Dollars

- Outlays for unemployment compensation were $80 billion (or 17 percent) lower in 2021 than in 2020.
- In both 2020 and 2021, spending on unemployment compensation was significantly higher than in 2019 because of enhanced benefits authorized by the CARES Act that were extended by the CAA and ARPA.
- Spending on those benefits reached its peak in the summer of 2020.
- Outlays for unemployment compensation declined in 2021.
• 770 new laws coming to California.
• UCB prof awarded Nobel prize for research on minimum wage.
• San Jose apologizes to Chinese immigrants & their descendants.
• Emergency response team helps schools navigate wildfires.
• UCD & UCSF study: no significant difference in Delta viral positivity load between vaccinated and unvaccinated – the vaccinated can still infect others.
• Kaiser suspends thousands of employees who shunned vaccine.
• UC Regents approve a controversial housing project at the site of Berkeley’s historic People’s Park - litigation expected.
• Homes that survived the 2018 Camp Fire illustrate preventive measures that likely helped houses resist wildfire.
• Commitment to safety leading state out of the pandemic.
• Newsom proclaims State of Emergency in response to oil spill.
• HB oil spill draws opposition to offshore oil production - Supply chain may have been a factor in disaster.
• Newsom vetoes bill that would have required law enforcement officers to undergo regular training.
• SpecOps soldiers evade ninja attack at California airport.

About a quarter or more of lecturers don't return to their jobs each year

Source: CalMatters analysis of UC personnel data obtained through a public records request – "Juris Roser Files" for UC lecturers

The findings, together with union data that shows lecturers on average work for two years at the UC, suggest that the university system relies on inexpensive labor to educate its 285,000 students. But while about 1,400 lecturers don’t return annually, their overall ranks keep growing at the UC.
Southern California Kaiser employees vote to authorize strike.
UC President recognizes KUCR's 55 years of service.
UCR granted $5 million for stem cell research training.
“Breaking the promise of opportunity”: UCR brags about narrowing achievement gaps, but rejects 1/3rd of its applicants. “Turning down a lot of people can cover up a lot of problems.”
SoCal Edison: Possible Public Safety Power Shutoffs.
UCLA anesthesiologist escorted out of workplace.
UCSD DIY’ers build homemade air purifiers for campus, claim filters catch 90% of Covid virus particles.
4,000 lightning strikes recorded during SoCal storm.
Case Breakers believe Gary Francis Poste a.k.a. the Zodiac Killer, is responsible for a 1966 murder in Riverside.
Riverside approves plan for more than 20k new homes by 2029.
Companies will pay nearly $78 million to clean up contaminated groundwater at two toxic waste sites.
Riverside County Sheriff Chad Bianco linked to Oath Keepers.

RivCo EOC is currently activated to Level 3 (virtual) in support of the ongoing COVID-19 response.
COMMUNICATIONS

- 11 October:
  - Provost's Office Hours - Fall Series
- 08 October:
  - Research Student Participation - A Mind-Body Strategy for Physical and Mental Well-Being
- 07 October:
  - UCOP COVID-19 Digest
- 06 October:
  - myStrength App Provides Personalized Emotional Support to Help On-Site Work Anxiety
- 05 October:
  - UCR ITS Security Alert - UC community PII may have been used in attempts to open unauthorized bank accounts at financial institutions such as Chime and Go2Bank
  - 5th Year Senior Leadership Review for Vice Chancellor and Dean Deborah Deas

Please Reference Notes Section For More Information
NOTABLE

- Fire Prevention 2021 Campaign “Learn the Sounds of Fire Safety!”
- October marks Cybersecurity Awareness Month
- CalOES: Cyber Security Awareness Month
- Stanford School of Medicine Symposium Series: Effects & Lessons of the Pandemic
- John Hopkins Podcast: Where Are We in the COVID-19 Pandemic?
- ‘Risk Appetite: The facts, the myths, and the links with culture, maturity and sustainability’
- The business continuity plan of the future
- CISA releases new tool to help organizations guard against Insider Threats
- Burn-out an "occupational phenomenon": International Classification of Diseases
- How to Build an Incident-Response Plan, Before Security Disaster Strikes
- Understanding How Facebook Disappeared from the Internet
- The Data Equity Framework is a systematic way of looking at data projects
- Lightning could spark more California fires as world warms
- Coalition for Epidemic Preparedness Innovations: Accelerating pandemic response efforts
- Inside the CIA’s secret Kabul base
2021 Cybersecurity Awareness Month

- October is Cybersecurity Awareness Month!

- “Do Your Part. #BeCyberSmart.”

- Use the hashtag #BeCyberSmart before and during October to promote your involvement in raising cybersecurity awareness.

2021 focus and outreach:
- October 4 (Week 1): Be Cyber Smart.
- October 11 (Week 2): Phight the Phish!
- October 18 (Week 3): Explore. Experience. Share. – Cybersecurity Career Awareness Week
- October 25 (Week 4): Cybersecurity First


- The challenges faced by the cybersecurity community today are hitting mainstream headlines. However, new approaches to information sharing, securing technologies, and human-centric cyber training can empower organizations and professionals to enable a safer, more secure world.
Cybersecurity Career Awareness Week
October 18 - 23, 2021

Do Your Part.
#BeCyberSmart

Cybersecurity starts with YOU and is everyone's responsibility.

About the Campaign
Learn more about Cybersecurity Awareness Week

Discovering Cybersecurity Careers
Examine resources about cybersecurity careers

Cybersecurity in Your Community
Explore cybersecurity in your neighborhood
2021 Cybersecurity Awareness Month

**CYBERCRIME**

**What is it?**
Cybercrime is any crime which is committed electronically.

This can include...
- Theft
- Fraud
- Sometimes even murder

**Why should you care?**
- Crime is a danger offline and on!
- Cyber self-defense basics can go a long way to keeping you and your data out of the hands of bad actors.

**Examples**
- Identity theft
- Child sexual abuse materials
- Financial theft
- Intellectual property violations
- Malware
- Malicious social engineering
2021 Cybersecurity Awareness Month

MALWARE

What Is It?
Any software intended to...
- Damage
- Disable
- Or give someone unauthorized access to your computer or other internet-connected device

Why should you care?
- Most cybercrime begins with some sort of malware. You, your family, and your personal information is almost certainly at risk if malware finds its way onto your computer or devices.

Examples
- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Viruses
- Worms
2021 Cybersecurity Awareness Month

RANSOMWARE

What Is It?
Malware designed to make data or hardware inaccessible to the victim until a ransom is paid.

Examples
- Cryptolocker
- Winlock
- Cryptowall
- Reveton
- Bad rabbit
- Crysis
- Wannacry

Why should you care?
- Often downloaded as malicious email links
- Damage to both financial stability and reputation
- No guarantee that you will get your data back, even if you pay
- Often used as a decoy for other malicious activity
Keeping Safe on Social Media

• Social media sites and apps are great ways to connect and share information.

• User profiles, timelines, social media status, friend lists, and message services grant your contacts insights into your day-to-day activities.

• However, these sites can also provide adversaries with the critical information they need to disrupt your life and harm or harass you, your co-workers, or even your family members.

• The following guidance can better prepare you to protect against online threats.

Identify Critical Information
Critical information is any information considered sensitive or that could do harm if compromised. Here are some examples:

- Names, photos, and relationships
- Usernames, passwords, computer and networking information
- Operational, security, and logistical data
- Mission capabilities or limitations
- Job title, location, salary, grade, and clearance
- Schedules, travel itineraries, and locations
- Social Security numbers, credit cards, and banking information
- Work or personal addresses and phone numbers
- Interests, hobbies, likes, and dislikes
Cyber Threat’s to Emergency Services

- Cyber Espionage
  - Limited, geopolitically-driven
- Cyber Crime
  - Somewhat frequent, ranging severity
- Influence Operations (IO)/Disinformation
  - Observed IO narratives aimed at widening existing wedges in society
- Hacktivism
  - Common during times of ideological conflict

“Emergency operations communications, database management, biometric activities, telecommunications, and electronic security systems are conducted virtually and are vulnerable to cyber disruptions”

~ DHS 2015 Emergency Services Sector-Specific Plan
Cyber Threat Impact to Emergencies

**Human**
- More than 2,500,000 career and volunteer ESS personnel in five disciplines
- Law Enforcement
- Emergency Management
- Fire and Rescue Services
- Emergency Medical Services
- Public Works

**Physical**
- **Facilities**
  - for daily operations, support, training, or storage
- **Equipment**
  - specialized for discipline and capability (e.g., personal protective, communications, surveillance)
- **Vehicles**
  - specialized for discipline and capability (e.g., ambulances, HazMat, aircraft, and watercraft)

**Cyber**
- **Virtual Operations**
  - Emergency operations communications, database management, biometric activities, and security systems are frequently operated in cyberspace.
- **Internet**
  - The Internet is widely used by the sector to provide information and distribute alerts, warnings, and threats relevant to the sector.
- **Information Networks**
  - Computer-aided dispatch and watch and warning systems, information-sharing portals, and social networking are leveraged to keep the ESS informed and connected.
Resources

Cybersecurity Guidance from nsa.gov

• Mobile Device Best Practices
• Telework Best Practices
• Identity Theft Threat and Mitigations
• Limiting Location Data Exposure
• Compromised Personal Network Indicators and Mitigations
• Best Practices for Keeping Your Home Network Secure
• NSA's Top Ten Cybersecurity Mitigation Strategies

Threats to mobile devices are more prevalent and increasing in scope and complexity. Users of mobile devices desire to take full advantage of the features available on those devices, but many of the features provide convenience and capability but sacrifice security. This best practices guide outlines steps the users can take to better protect personal devices and information.