USA & WORLD

- US system for **death investigations** is a detriment to public health.
- Eye-scanning **Cryptocurrency** launches with $1 Billion valuation.
- NY district attorney’s “**No Fly List**,” a secret roster of LE officers.
- **House** passes **bills** on both supply chain, telecom security.
- 36 years of **weather data** assesses US solar and wind power needs.
- FTC **study** shows how ISP’s fail to protect sensitive information.
- Utah protesters claim hospitals are **killing** people who have COVID.
- **Coding bootcamps** as an alternative to college.
- How school systems are/aren’t **adapting to COVID**.
- **Study**: evidence for inheritance of trained immunity in mammals.
- Why are U.K. Covid cases **so high** compared to the rest of Europe?
- Why weren’t COVID boosters **tweaked** to better match variants?
- States with colder weather **see an increase** in Covid cases.
- China **denies** testing nuclear-capable hypersonic missile.
- U.S. policy needs to **adjust** to deal with assertive China over Taiwan.
- Digital **spies** with a nexus to Chinese interests have successfully compromised parts of the global telecommunications network.
- Facebook plans to hire 10,000 in Europe to build ‘**metaverse**‘.
- Reporter **exposes flaws** on state website that made teachers PII "vulnerable to public exposure“ - Gov. vows to **prosecute** newspaper.

Student **survey**: Depression, stress and anxiety leading barriers to learning as access to trusted adults drops.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Findings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FINDING ONE</strong></td>
<td>page 5</td>
</tr>
<tr>
<td>Sixty-one percent of students said they learn a lot every day — up from 39 percent in the spring and on par with pre-pandemic levels — but experiences differ across student groups.</td>
<td></td>
</tr>
<tr>
<td><strong>FINDING TWO</strong></td>
<td>page 9</td>
</tr>
<tr>
<td>Feeling depressed, stressed, or anxious has risen to the number one obstacle to learning. Hispanic or Latine, multiracial, and Black or African American students faced more obstacles on average than did white or Asian students.</td>
<td></td>
</tr>
<tr>
<td><strong>FINDING THREE</strong></td>
<td>page 13</td>
</tr>
<tr>
<td>Sense of belonging recovered from spring 2020, and students experienced increased academic support from their teachers.</td>
<td></td>
</tr>
<tr>
<td><strong>FINDING FOUR</strong></td>
<td>page 16</td>
</tr>
<tr>
<td>Males continued to rate their health and well-being more positively than did females and students who identify in another way. Overall, students reported less availability from adults in school to support their mental and emotional health, but more programs and services.</td>
<td></td>
</tr>
<tr>
<td><strong>FINDING FIVE</strong></td>
<td>page 19</td>
</tr>
<tr>
<td>One in four high school seniors’ postsecondary plans have changed since the start of the pandemic.</td>
<td></td>
</tr>
</tbody>
</table>

![Graph](https://www.youthtruth.org/assets/1697/1697.png)

**DEPRESSION, STRESS, AND ANXIETY HAS INCREASED AS AVAILABILITY OF ADULTS TO TALK TO WHEN FEELING STRESSED HAS DECREASED**

- Feeling depressed, stressed, or anxious as obstacle to learning
- Availability of an adult from school to talk to when feeling stressed or having problems
- Pre-COVID: 39% Spring 2020: 46% Fall 2020: 46% Spring 2021: 49%
CALIFORNIA

- What to expect as “bomb cyclone” continues through California.
- Cal-Secure: A look at the states’ new cybersecurity roadmap.
- Proposed public health protections governing oil and gas drilling.
- USGS report: how a major earthquake could disrupt services.
- PG&E’s controversial wildfire mitigation plan.
- How a 1963 Supreme Court case can be used in police reform.
- UC creates recommendations for responsible use of AI.
- Atmospheric river storms, the largest in 9 months, soak NorCal.
- Newsom signs Executive Order to tackle supply chain issues.
- President of San Jose State resigns in fallout over sexual abuse.
- School outbreaks atypical – why the vaccination requirements?
- Searchable database of the highest paid CA employees.
- 13 new California laws that could change your life.
- Legislature repeals non-disclosures clauses.
- State leaders increase support for dual enrollment.
- CDC: CA only state to improve level of COVID transmission.
- Contrasting economic policy in California and Texas.
- Institutions should address affordable housing needs.
- Post-pandemic California: Comeback or decline?
- Housing supply levels off as market heads into off season.
• West Coast storm hits SoCal. Here's when to expect rain.
• State declares drought emergency for SoCal.
• California Air Resources Board (CARB) opens HQ near UCR.
• Riverside Unified teacher placed on leave for 'offensive' lesson.
• COVID cases among students, faculty force closure of LA school.
• Employee COVID-19 testing center opens on campus.
• VP of Sustainability pushes UC to provide resources for Latinos.
• UCR part of $12M grant for atmospheric measurement network.
• Training: Introduction to ArcGIS Online (9 November from 2–3 PM).
• UCSB Cyber Security Awareness Month: Social Engineering.
• UCR Center for Invasive Species Research spotlights 'stink bugs.'
• Lawsuit alleges abuse by UCSD coach led to student's suicide.
• UCSD’s COVID-19 Protocols: Thorough planning, poor execution.
• Protest against COVID vaccine mandate led in IE.
• San Diego area students skip school to protest vaccine mandate.
• Vaccine alters SoCal’s Covid path: rural areas suffer.
• 2028 Olympics: Los Angeles cleared for major airport expansion.

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

- 25 October:
  - Provost's Office Hours - Fall Series
- 22 October:
  - Passing of Robert Anderson
- 21 October:
  - UCOP COVID-19 Digest
- 20 October:
  - Update on Winter quarter instruction at UCR
- 19 October:
  - REMINDER: 5th Year Senior Leadership Review for Vice Chancellor and Dean Deborah Deas
- 18 October:
  - UCR 2021-2022 Winter Holiday Closure

Please Reference Notes Section For More Information
NOTABLE

• CISA, FBI, and NSA Release BlackMatter Ransomware Advisory to Help Reduce Risk of Attack
• The new math of cybersecurity value
• Twitter Suspends Accounts Used to Snare Security Researchers
• Cyber Criminals Using Spoofed Unemployment Benefit Websites to Defraud US Public
• 'A lot' of firms are developing offensive cyber techniques, hoping for investment
• A History of the Data-Tracked User
• Is Cybersecurity Insurance Out of Reach for Government?
• Netherlands can use intelligence or armed forces to respond to ransomware attacks
• Enterprise cybersecurity: Aligning third parties and supply chains
• Cyber resilience: Protecting America’s digital infrastructure
• Ransomware attacks against hospitals are having some very grim consequences
• Ransomware is leading hospital boards to pour more money into cybersecurity
• The Downside to State and Local Privacy Regulations
• Privacy Tips for Your Syllabus
• California Hospital Sued Over Data Breach
Risk-based cybersecurity

• Companies are moving to a risk-based cybersecurity stance.
• The approach recognizes that not all assets are created equal, nor can they be equally protected in today’s all-encompassing digital environment.
• Some assets are extraordinary—of critical importance to a company and its business.
• If a company’s customer interface is not secure, the risk can become existential.
• Safeguarding such assets is the heart of an effective strategy to protect against cyberthreats.
Risk-based cybersecurity

- Companies can only move to this advanced position if they already have in place the underlying capabilities needed to ensure digital stability and customer trust.
- Furthermore, as they develop and improve these capabilities, their guiding objective becomes the demonstrable and quantifiable reduction of enterprise risk.
- These capabilities can be grouped into seven action areas.
- The UC IS-12: IT Recovery policy identifies risks and resources that should be recovered in the event of an unavoidable or unforeseen disaster, whether natural or human-made.
Most companies have yet to reach the advanced levels of cybersecurity management demanded by today’s business environment.

**Cybersecurity maturity level survey**, score (0 = low, 4 = high) (n = 114)

- **Level 0**: Zero capabilities
- **Level 1**: Ad hoc management
- **Level 2**: Mature foundations
- **Level 3**: Advanced functions
- **Level 4**: Proactive approach

![Bar chart showing the distribution of cybersecurity maturity levels among a sample of 114 companies. The chart indicates that the majority of companies are at Level 0 or Level 1, with a smaller portion at Level 2 and a few at Level 3 and Level 4.](chartوها)
Cybersecurity maturity varies within sectors more than it varies from sector to sector.

Cybersecurity maturity level, industry sector breakdown, score (0 = low, 4 = high) (n = 114)

- Level 4: Proactive approach
- Level 3: Advanced functions
- Level 2: Mature foundations
- Level 1: Ad hoc management
- Level 0: Zero capabilities

More mature

Less mature

Healthcare  Banking  Industrial  Insurance  Consumer  Other  TMT

Max  75th percentile  Average  25th percentile
More profitable companies build stronger cybersecurity capabilities.

**Level of cybersecurity maturity, (0 = low, 4 = high) (n = 114)**

- **Leading organizations**
- **Aspiring leaders**
- **Remaining organizations**

**Profitability in last fiscal year, % average net margin**

- **Leading organizations**
- **Aspiring leaders**
- **Remaining organizations**

Source: S&P Capital IQ; McKinsey Cybersecurity Maturity Survey 2021
Leading organizations—those with the highest average level of cybersecurity maturity—are mostly larger companies.

Ownership structure among surveyed organizations, by cybersecurity groupings, %

- **Leading organizations**:
  - Share with revenue above $5 billion: 75%
  - Other: 25%

- **Aspiring leaders**:
  - Share with revenue above $5 billion: 57%
  - Other: 43%

- **Remaining organizations**:
  - Share with revenue above $5 billion: 28%
  - Other: 72%

Source: S&P Capital IQ; McKinsey Cybersecurity Maturity Survey 2021
The Treasury Department’s Financial Crimes Enforcement Network (FinCEN) has published the ‘Financial Trend Analysis’ in response to the increase in number and severity of ransomware attacks against U.S. critical infrastructure since late 2020.

In May 2021, hackers used a ransomware attack to extort a multi-million dollar ransom, which also disrupted the Colonial Pipeline and caused gasoline shortages.

Other recent attacks have targeted various sectors, including manufacturing, legal, insurance, health care, energy, education, and the food supply chain in the United States and across the globe.

“Ransomware and cyber-attacks are victimizing businesses large and small across America and are a direct threat to our economy.” Treasury Secretary Janet L. Yellen
Treasury Department Report

- Total Suspicious Amount from Ransomware-Related Suspicious Activity Reports (SARs) and Transactions, 2011 to June 2021
The median average payment amount for ransomware-related transactions was $102,273.