## Highlights

Security Hack of F-35 Results in J-31. DOD says NO MORE in Cybersecurity Enforcement Push

3 North Korean Military Hackers Charged with Global Cyberattacks, Money Laundering, Extortion of $1.3B

Ransomware Attack on California's DMV

G2M Webinar Schedule

Over 900 people registered for our last webinar, with sponsors Weka, Kioxia, and NVIDIA. The advantage of registering, even if you cannot attend, is the webinar link and materials are emailed directly to registrants. We can appreciate that most people are too busy to attend webinars during the workday but still want look through the slide deck, particularly for webinars featuring major enterprise storage companies, startups, new product solutions, and providing meaningful approaches to data management and storage challenges.

If you are interested in sponsoring a webinar but don't see a topic that quite fits, we can modify topics or add topics to meet your objectives.

*Cheers! Mike Heumann*

## Security Hack of F-35 Results in J-31. DOD Says NO MORE in Cybersecurity Enforcement Push

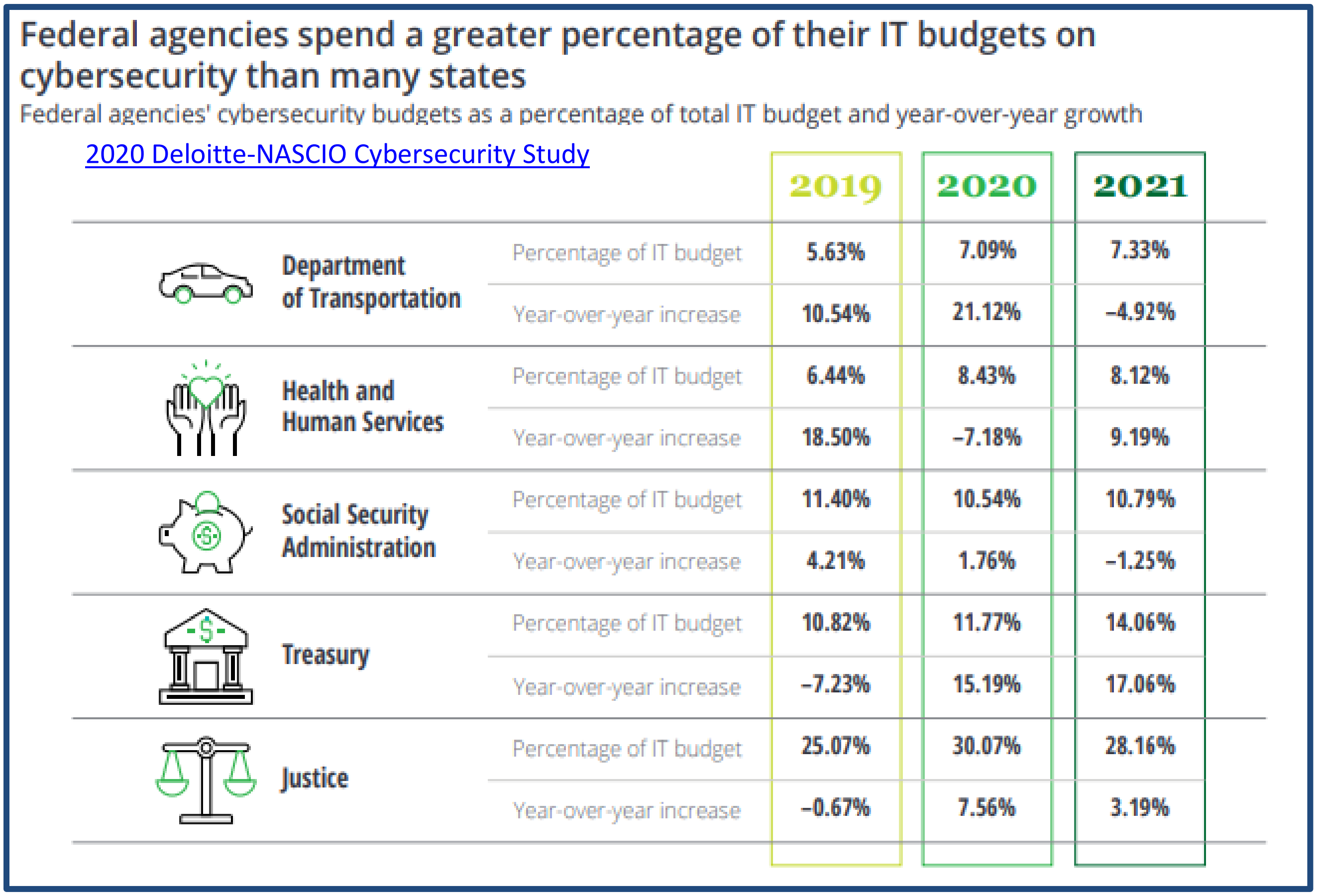
China's J-31's is "modeled after" the F-35. That is a nice way of referring to the Chinese hack of F-35 data in 2007 through contractor Lockheed Martin, to build their jet fighter, J-31. Contractors are required to meet standards regarding security protocols but those requirements have not been verified in the past. Stacy Bostjanick, Direct of Cybersecurity Maturity Model Certification (CMMC) says that contractors in the past did not take the protocols seriously and simply said they were complying in order to get business, resulting in the F-35 breach. Verification measures are needed because the voluntary compliance is resulting in too much mishandling of data.

"It's trust, but verify. This is the start of a new day in the Department of Defense where cybersecurity, as we've been saying for years is foundational for acquisitions, we're putting our money where our mouth is. We mean it," explains Katie Arrington, CISO for the undersecretary of Defense for acquisition and sustainment.

The Pentagon will need to certify at least 1500 contractors and subcontractors as part of fifteen contracts ranging in size and complications, as a light rollout of the program. The CMMC will allow only a level 1 result, nothing below standard. The goal is to level the playing field for contractors that actually are complying with security standards because the Pentagon will not be able to accept cheaper contract options that are not in compliance. Some contractors have left vulnerabilities in place for years, even when simply security fixes were available.

There has never been a comprehensive, objective assessment conducted of the security posture of the US Defense Industrial Base of over 300k companies.

“We have a great deal of standards for cybersecurity. What we are lacking is a unified standard. It is a major undertaking, but just like we got to ISO 9000, we need to get there with cybersecurity. If we were doing all the necessary security controls, we wouldn’t be getting exfiltrated to the level that we are. We need to level set because a good portion of our defense industrial base doesn’t have robust cyber hygiene. Only 1% of [Defense Industrial Base] companies have implemented all 110 controls from the National Institute of Standards and Technology. We need to get to scale where the vast majority of DIB partners can defend themselves from nation state attacks.” explains CISO, Katie Arrington.



Federal agencies spend a greater percentage of their IT budgets on cybersecurity than many states

Federal agencies' cybersecurity budgets as a percentage of total IT budget and year-over-year growth

2020 Deloitte-NASCIO Cybersecurity Study

| | | 2019 | 2020 | 2021 |
|---|---|---|---|---|
| Department of Transportation | Percentage of IT budget | 5.63% | 7.09% | 7.33% |
| | Year-over-year increase | 10.54% | 21.12% | –4.92% |
| Health and Human Services | Percentage of IT budget | 6.44% | 8.43% | 8.12% |
| | Year-over-year increase | 18.50% | –7.18% | 9.19% |
| Social Security Administration | Percentage of IT budget | 11.40% | 10.54% | 10.79% |
| | Year-over-year increase | 4.21% | 1.76% | –1.25% |
| Treasury | Percentage of IT budget | 10.82% | 11.77% | 14.06% |
| | Year-over-year increase | –7.23% | 15.19% | 17.06% |
| Justice | Percentage of IT budget | 25.07% | 30.07% | 28.16% |
| | Year-over-year increase | –0.67% | 7.56% | 3.19% |

# 3 North Korean Military Hackers Charged with Global Cyberattacks, Money Laundering, Extortion of $1.3B

Three North Korean computer programmers are charged with a global criminal conspiracy including cyberattacks, money laundering, and extortion of over $1.3B. The cybercrime charges include ransomware, phishing attacks, and digital bank heists.  The defendants are alleged to be members of the Reconnaissance General Bureau (RGB), a military intelligence agency of the Democratic People's Republic of Korea (DPRK), known as Lazarus Group and Advanced Persistent Threat 38 (APT38). According to the Department of Justice indictment, these defendants were stationed by the North Korean government in other countries, including China and Russia, and engaged in a single conspiracy to cause damage, steal data and money, and further the strategic and financial interests of the DPRK government.

Charges include 1) cyberattacks in 2014 on Sony Pictures Entertainment and AMC in retaliation for the movie, "The Interview," which depicted the assassination of DPRK's leader; 2) creation of WannaCry 2.0 ransomware, 3) phishing campaigns targeting employees of US defense contractors, energy companies, aerospace companies, technology companies, the US Department of State, and the US Department of Defense, among many, many other financial crimes.

"As laid out in today's indictment, North Korea's operatives, using keyboards rather than guns, stealing digital wallets of cryptocurrency instead of sacks of cash, are the world's leading bank robbers, said Assistant Attorney General John C. Demers of the Justice Department's National Security Division. "The Department with continue to confront malicious nation state cyber activity with our unique tools and work with our fellow agencies and the family of norms abiding nations to do the same."

A United Nations panel of experts say that North Korea is using cyberattacks to finance its nuclear weapons and ballistic missiles and that North Korea and Iran have resumed cooperation on long-range missile development projects.

# Ransomware Attack on California DMV

The California DMV uses Automatic Funds Transfer Services (AFTS) to verify changes of address with the national database. AFTS experienced a ransomware attack that may have compromised up to the last 20 months of California vehicle registration records, including names, addresses, license plate numbers, and VINs. Other municipalities may be affected as well. Ransomware expert and threat analyst at Emsisoft, Brett Callow, believes the Cuba Ransomware group is to blame.

The news comes on the heels of reports that the California DMV makes over $50M each year by selling drivers' personal information.

Hackers attack every 39 seconds.

17% of all sensitive files are accessible to every single employee in a company.

The percentage of insider incidents perpetrated by trusted business partners has typically ranged between 15%-25% across all insider incident types and industry sectors.

The underlying reasons for insider attacks are fraud, monetary gain, and IP theft.

### AI & Cybersecurity Events – All Virtual

| | |
|---|---|
| March 10 | Transform Your Operations with the Power of AI in 60 days |
| March 10-11 | Data Connectors Southern California Virtual Cybersecurity Summit |
| March 11-13 | Human Hacking Conference |
| March 12 | AI Day Conference 2021 |
| March 14-16 | 10th International Conference on Frontiers of Information Technology (ICFIT) |
| March 15-16 | 1st International Conference on Autonomous Intelligent Cyber-Defence Agents (AICA) 2021 |
| March 15-20 | SANS Cyber Security West |
| March 16 | CSO's Cybersecurity Summit 2021 |
| March 16-17 | ISMG Virtual Cybersecurity Summit: Healthcare |
| March 18 | FutureCon Western Conference |
| March 23-24 | Gartner Security & Risk Management Summit |
| March 23-25 | Priv8 |
| March 25 | Effective Training in Cybersecurity in the New Era of Staff Remotisation; Security Token Summit 2021 |
| March 25-26 | AI in Healthcare Summit 2021 |
| March 30-31 | ISMG Virtual Cybersecurity Summit: Connected Devices Security; World Data Compliance 2021 |
| March 31-April 1 | Infosecurity |

## G2M Research Multi-Vendor Webinar Series

Our February webinar was "Storage Architectures to Maximize the Performance of HPC Clusters" was sponsored by Kioxia (Matt Hallberg), NVIDIA (Reggie Reynolds), and Weka (Joel Kaufman). View the recording and/or download a PDF of the slides.

Our 2021 webinar schedule! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact **G2M** for a prospectus.

G2M
RESEARCH

| | |
|---|---|
| March 23: | One Year after COVID-19: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This? |
| April 20: | The Race to be Relevant in Autonomous Vehicle Data Storage (both On-Vehicle and Off-Vehicle) |
| May 18: | Responsive and Efficient Storage Architectures for Social Media |
| June 15: | It’s 2021 - Where Has NVMe-oF™ Progressed To? |
| July 13: | Computational Storage vs Virtualized Computation/Storage in the Datacenter: “And The Winner Is”? |
| Aug 17: | AI/ML Storage - Distributed vs Centralized Architectures |
| Sept 14: | Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence |
| Oct 12: | Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You? |
| Nov 9: | The Radiometry Data Explosion: Can Storage Keep Pace? |
| Dec 14: | 2021 Enterprise Storage Wrap-up Panel Discussion |

G2M
COMMUNICATIONS

Effective Marketing & Communications
with Quantifiable Results