Five questions for Dan Jones[1]

As the University of Colorado's Chief Information Security Officer (CISO), Dan Jones leads and coordinates the systemwide information security program in partnership with the campuses and system administration. The Office of Information Security[2] works with the campuses to provide services and expertise to support confidentiality, integrity and availability for data across the university.

A conversation with Jones about information security often hits upon a key word: complexity. And that's without referencing the CU Boulder alumnus' own complex dual role at CU, which also has him serving as the Associate Vice Chancellor for Integrity, Safety and Compliance at CU Boulder. In that post, he oversees public safety, flight operations, compliance coordination, accessible technology and, yes, information security.

Last year's onset of the pandemic only added to the complexity of cybersecurity across CU.

"We talk about the 'attack surface' – from the perspective of an attacker, that's where can they target you," Jones said. "When you have more systems at employee homes, it spreads that attack surface that much larger, which makes it harder to manage the environment for Information Technology. We have more devices being used, and more people using personal devices at home. So it increases the complexity of security."

In his free time, Jones likes to keep things simple: reading, cooking, getting outdoors.

"I'm hoping I'll be able to get out the paddleboard soon," Jones said. "Hiking or getting out on the water are how my wife and I spend time. That was one of the advantages of the pandemic, was getting to see my wife more often."

1. What special circumstances do CU and other institutions of higher education face when cultivating a culture of positive information security?

When I talk to my colleagues in the private sector about higher education, I use the analogy, from Frances Draper (a wonderful colleague who recently passed away), of a research university being like a small city with a lot of high-tech industries. It's like you have city government, a medical clinic, city services, businesses and maybe even some residential, when you consider student housing.

We're really one of the most highly regulated sectors. We have student data and FERPA (Family Educational Rights and Privacy Act) requirements, there's health insurance and HIPAA (Health Insurance Portability and Accountability Act), there's Department of Energy requirements, requirements for grants and contracts. So that makes it more difficult: How do you think about security without having to think about 20 different sets of regulations? A typical IT person or faculty member, they're not going to be able to keep track of all those regulations. So how do we present a set of expectations that maps to all those different requirements?

Because we don't have a top-down corporate infrastructure, a large part of what we have to rely on is training and awareness to make sure everyone understands their security requirements.

2. How does the Office of Information Security approach the management of sensitive data?

I'll start with top-down: So as CISO, my role is thinking strategically in terms of what is the university to do to protect our IT resources, to protect the information of our students and employees and alumni. So it's thinking strategically about that, and understanding that keeping the university secure isn't something that only the Office of Information Security achieves. It takes everyone.

The office also oversees security operations for CU Boulder and system administration. So if there's a security incident, we're managing that, doing monitoring, looking at logs and comparing that with intelligence we get from partners – "Oh, we've been told about this potential bad thing. Do you see that somewhere on your network?"

Where most employees see us, hopefully, is in the training-and-awareness realm. We want to make sure people have

the information they need, understand what they need to do and how to play their part in protecting the university.

3. The Accellion cyberattack[3] earlier this year brought information security to top of mind for the CU community. What's the latest on CU's response, and what security challenges loom on the horizon?

In June, Ukraine and U.S. authorities did make arrests of the gang[4] that was involved with the Accellion breach. So it's good to see that the federal government was able to make progress and see some justice there.

The attackers published stolen data on the dark web. CU got a copy of that to validate what was published relative to the notifications we sent out. We then wanted to do our due diligence and make sure nothing was missed. We determined roughly 1,200 files were deleted, so we sent out notices at the end of June to the individuals who were part of that last batch.

We're going to do an exercise to make sure the university learns from this. One of the lessons from Accellion is, we have to do more to build better data services so people don't have to download spreadsheets and send them around in email. That will be a focus going forward.

In addition to other core security improvements, we're partnering with IT to make sure we continue, as attacks get more sophisticated, to have better technical protections around email. Multifactor authentication is a priority for the university.

4. How has the field of IT and cybersecurity evolved since you began your career?

It's the level of complexity. We have known for a long time there are things you need to do, like make sure you have good passwords. And two-factor authentication isn't necessarily new, but it's the level of complexity – the number of different applications, the increased reliance on data – that has changed.

There are more people who need to use data and do analysis as part of their day-to-day job. And the data is so interwoven: It's not just that I'm an employee with data that I created and am keeping track of, or I'm a faculty member tracking grades – and that's it. Somebody else needs that grade information, has to correlate that information with other grades, has to correlate that information with student success.

Another part of the change is how quickly the rate and speed of malicious attacks has increased. We used to do an annual experiment where we would set up a new system on the internet, sometimes called a honeypot, and you'd wait and see how long it took for someone to try to attack it. We don't do this anymore, because it went from us waiting months to only waiting minutes, just because of the speed of the systems that attackers have. You can't set up a new system without it being discovered and people trying to take advantage of it within literally minutes.

You also see that in terms of people sending phishing emails: They may not know whether an account actually exists, but they're making a bet that dan.jones exists, and they'll try permutations on that with common names.

5. What responsibility does each faculty and staff member have in supporting information security and in maintaining the confidentiality and integrity of information?

The first thing people need to do is be aware of the sensitivity of the data they have. Ask yourself, if this were my information, how would I want someone else to protect it? If I have a spreadsheet with student IDs and names and grades, I can't just email that out broadly or make it available to anyone with a Google account. I have to protect sensitive information that's in my hands.

Also, ask yourself, do I need this data? We don't need data lying around. If you don't need it on your desktop or laptop because the university has another copy of it, get rid of it.

Likewise, just like people need to be aware of their own safety at home – you want to lock the door – they need to be aware that people are going to try to take advantage of them. There are malicious individuals who really are trying to trick you. That could be by sending fraudulent or phishing emails, which try to trick people into divulging information or

getting them to go to a malicious website. Always be conscious about clicking links on an email. Be skeptical. It's the old adage, if it looks too good to be true, it probably is.

Increasingly, people need to be aware of, when they're using their personal device – their home computer or their phone – that they're responsible for security on that. So don't put sensitive data on your personal device. If you're reading email on your phone, make sure you have a PIN and basic security in your device.

The most important thing people can remember is to ask: If you have a question, check with your desktop support person or security team. If you get a weird email, stop, pick up the phone and ask about it.

Another good resource is our website: https://www.cu.edu/security[2].

System policy updates: Equal pay, sexual misconduct[5]
[6]

CU's Office of Policy and Efficiency has announced changes to several Administrative Policy Statements (APSs) related to the Colorado Equal Pay Act and to APS 5014, pertaining to sexual misconduct.

Equal pay

The updated APSs related to equal pay are:
5002 - Faculty Appointment Process 5009 - Performance Ratings for University Staff 5013 - Acting and Interim Appointments for University Staff Positions 5016 - Faculty Retirement Agreements 5023 - Letters of Offer for University Staff 5024 - Tuition Assistance Benefit 5053 - Multi-Year Contracts for Instructional, Research and Clinical Faculty with Teaching Responsibilities or Librarian Appointments 5060 - Faculty Appointments
These changes were reviewed by the campus chancellors and approved by President Todd Saliman to be effective retroactively to Jan. 1, 2021.

Sexual misconduct

The changes to APS 5014-Sexual Misconduct, Intimate Partner Abuse and Stalking [7]were made in response to recent federal court decisions and Department of Education guidance.

The changes were reviewed by the campus chancellors and approved by President Todd Saliman to be effective on Sept. 2, 2021.

For more detailed information, go to https://www.cu.edu/ope/aps/latest-changes[8].

For additional information on systemwide APSs, go to http://www.cu.edu/ope[9].

Overall CU retirement plans fees lowered by almost 50%[10]

A new recordkeeping and administrative fee structure for the University of Colorado 401(a) Mandatory Retirement Plan, CU 403(b) Voluntary Retirement Plan and Student Employee Retirement Plan (SERP) will debut Oct. 1.

The change reduces overall fees paid by CU faculty and staff by nearly 50%. The fixed-dollar, per-participant fee structure ensures each plan participant pays a fair, reasonable cost for the plan services provided.

Each participant will pay a single flat fee, based on their total account balance in all their CU retirement plan accounts. Fees will range from $0 to $186 annually.

The new, tiered fee structure:

Plan account balances as of the last day of the previous quarter

Quarterly fee

Annual fee

$0 to $5,000

$0

$0

$5,000.01 to $20,000

$7.75

$31

$20,000.01 to $50,000

$15.50

$62

$50,000.01 to $200,000

$23.25

$93

$200,000.01 to $500,000

$31.00

$124

$500,000.01 to $1,000,000

$38.75

$155

Greater than $1,000,000

$46.50

$186

Previously, each participant paid a percentage their total balance.

Under the new agreement, the average investment, recordkeeping and administrative fees for CU 401(a) plan participants are estimated to be 0.21%. A benchmark comparison can be made to other similarly sized plans, whose overall fees average 0.58%. CU 403(b) plan participants' average fees are estimated to be 0.25%, with a benchmark comparison of 0.79% for other similarly sized plans.

"This new fee structure is designed to encourage our employees to save money and grow these accounts," said Michelle Martinez, director of strategic benefits initiatives, CU Employee Services. "We don't want their savings eaten up by fees, but rather we want to encourage them to build their savings and be prepared for retirement, whenever that may be."

CU routinely reviews its retirement program to ensure it provides competitive retirement benefits. Employee Services developed a request for information (RFI) to review retirement plan vendors, in partnership with Innovest consultants, and sent it to multiple vendors, including TIAA.

Over the past few years, CU and TIAA streamlined the CU plans, contacted hundreds of former student employees to cash out or rollover small SERP account balances, and simplified the SERP fund line up. This freed time for TIAA consultants to focus on more CU active employee accounts. This also contributed to the lower administrative fees.

The plan servicing fee covers additional services such as recordkeeping, legal, accounting, investment advisory, and other plan and participant services. To learn more about what makes up CU's retirement plan fees, watch this short video[11].

The annual plan servicing fee will be assessed quarterly. The first fee will be applied on the fourth quarterly statement of the year (Dec. 31, 2021). Employee Services recommends employees review their quarterly statement and notify the department of any discrepancies.

Register for TIAA webinar

TIAA will host a webinar, noon-1 p.m. Sept. 23, for plan participants to learn more about these changes. To register, go to TIAA.org/cu/webinars[12].

Call for nominations: 2021 UCSC Staff Excellence Awards [13]

Amid wildfires and a pandemic, here's how to keep your indoor air clean [14]

Register now for ALTEC language classes, beginning Monday[15]

A self-learning algorithm may help predict how genetic disease occurs[16]

Researchers abuzz about bee health[17]

Mass memorials: A place to grieve, heal, remember [18]

Morris, Palmer joining CU Denver's Office for Diversity, Equity, and Inclusion [19]

Thompson to retire, continue teaching after leading multiple expansions as Continuing Ed dean[20]

Rinaldo named director of Center for Asian Studies [21]

Links
[1] https://connections.cu.edu/spotlights/five-questions-dan-jones[2] https://www.cu.edu/security[3] https://www.cu.edu/accellion-cyberattack[4] https://denver.cbslocal.com/2021/06/16/university-colorado-cyber-attack-ukraine-clop-ransomeware/[5] https://connections.cu.edu/stories/system-policy-updates-equal-pay-sexual-misconduct [6] https://connections.cu.edu/sites/default/files/policy_top.jpg[7] https://www.cu.edu/ope/aps/5014[8] https://www.cu.edu/ope/aps/latest-changes[9] http://www.cu.edu/ope[10] https://connections.cu.edu/stories/overall-cu-retirement-plans-fees-lowered-almost-50[11] https://player.vimeo.com/video/266515171?portrait=0[12] http://www.tiaa.org/cu/webinars[13] https://connections.cu.edu/stories/call-nominations-2021-ucsc-staff-excellence-awards[14] https://connections.cu.edu/stories/amid-wildfires-and-pandemic-here-s-how-keep-your-indoor-air-clean[15] https://connections.cu.edu/stories/register-now-altec-language-classes-beginning-monday[16] https://connections.cu.edu/stories/self-learning-algorithm-may-help-predict-how-genetic-disease-occurs[17] https://connections.cu.edu/stories/researchers-abuzz-about-bee-health-0[18] https://connections.cu.edu/stories/mass-memorials-place-grieve-heal-remember[19] https://connections.cu.edu/people/morris-palmer-joining-cu-denver-s-office-diversity-equity-and-inclusion[20] https://connections.cu.edu/people/thompson-retire-continue-teaching-after-leading-multiple-expansions-continuing-ed-dean[21] https://connections.cu.edu/people/rinaldo-named-director-center-asian-studies