EDUCAUSE Live! Participant Chat: Links and Abbreviated Transcript

CIO Insights on Cybersecurity

October 14, 2014: 1:00 p.m. ET (UTC-4; 12:00 p.m. CT, 11:00 a.m. MT, 10:00 a.m. PT)

Session Links:

- Passphrase Vaulting: https://protect.iu.edu/cybersecurity/safeonline/passphrases/vaults
- EDUCAUSE transmedia piece: http://www.educause.edu/visuals/shared/er/extras/2014/Good2bCIO/default.htm
- Toolkit for new CISOs: https://wiki.internet2.edu/confluence/display/2014infosecurityguide/Toolkit+for+New+CISOs
- Get involved in higher education cybersecurity efforts: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/community-engagement

Abbreviated Chat Transcript:

Keith: (13:04) I can't vote. I've heard of it but we aren't promoting it.


Hany Seyam: (13:06) what do you think to shift the e-mail to the cloud to avoid in house breach

Teresa Banks: (13:07) So glad to see so many participants from the University of Arizona!

Guest 5: (13:07) I have one of those on my phone.

Keith: (13:07) I'm surprised at the 53.4% ;-
Deyu: (13:08) how about cloud-based apps

Sue Traxler: (13:09) So where can we save our passwords since we have so many passwords nowadays? Are programs such as SplashID safe password storage programs?

Guest 5: (13:09) I use aWallet.

Lanita Collette, Northern Arizona University: (13:09) An enterprise-worthy password safe such as Thycotic's Secret Server is a recommended solution for managing passwords.

Deyu: (13:10) I use aWallet too, cloud-based. Is it safe?

Greg T - UTK: (13:11) @Deyu: According to Peter, no since the machine you run it on can potentially be compromised, but personally, I use LastPass and I think it is a reasonable compromise between convenience and security.

Alastair MacLeod: (13:12) We are on the cusp of going with Last Pass so I am also interested in the risks there

Tammy Clark, Univ of Tampa: (13:12) We use encrypted wireless (WPA2 with required authentication mechanisms). Michelle, are you saying your wireless implementation is wide open to the public or do you have encryption?

Kasia Taylor: (13:13) I wonder how many schools have Chief Information Security Officers?

Melissa Woo - University of Oregon: (13:13) Good question, @Kasia - personally I feel not enough campuses do.

Tammy Clark, Univ of Tampa: (13:14) I agree with you, Melissa:-)

Melissa Woo - University of Oregon: (13:14) Good to hear the feedback from all of you re: password saver apps. We have different approaches.

Melissa Woo - University of Oregon: (13:14) FWIW, I use a password saver app.

Frank@WCUPA.EDU: (13:14) I'm a Lastpass fan for a while now.

Melissa Woo - University of Oregon: (13:14) @Tammy :-)

Greg T - UTK: (13:14) @Melissa Thanks for that, I was hoping I wasn't crazy!

Evy L. - University of Arizona: (13:15) Tammy, we have a UA public Wi-Fi set up as well as a Private one set up. The public one is the one that she was talking about, but we do have another as well.

Ben Marsden, Smith College: (13:15) followup, is there a particular school size break for CISO (or equivalent) vs non-CISO?
Tammy Clark, Univ of Tampa: (13:15) Great, thanks Evy L.

Carlos S. Lobato: (13:15) Kasia, good questions and I would follow-up on how many schools have a formal written Comprehensive Risk-based Information Security Program in place.

Joanna LynGrama: (13:15) @Kaisa: Responses to the EDUCAUSE Core Data Service survey suggest that 32% of US institutions employ a person whose time is 100% devoted to information security. 1 in 4 of those people have the CISO title.

elizabeth_leake: (13:15) What percentage of accounts are compromised (poll, please).

Melissa Woo - University of Oregon: (13:15) Great question, @Ben. I believe EDUCAUSE/HEISC may have some anecdotal numbers about that. Worth more digging into.

Ron Loneker Jr - College of Saint Elizabeth: (13:16) Do any schools have policies requiring passcodes/passwords on personal devices?

Deyu: (13:16) @Greg T - UTK, thank you!

Valerie Vogel, EDUCAUSE: (13:17) IU has a nice page about Passphrase Vaulting: https://protect.iu.edu/cybersecurity/safeonline/passphrases/vaults

Tammy Clark, Univ of Tampa: (13:17) If you look at the breaches that affected Target, Home Depot and Kmart, all three were originally caused by spearphishing employees and third parties...security awareness is a big issue!

Greg T - UTK: (13:17) @Ron Loneker: UTK does if you want to connect the device to Exchange; it also enforces the remote wipe setting on the device.

Carlos S. Lobato: (13:17) I wonder how many schools have a formal Institutional IT Governance Program?

Karl Hassler 2: (13:17) I use human encryption clues for each site, stored in the cloud. Clues map to variables in the password construct, e.g., yellow spring wood kay pin shift

Ron Loneker Jr - College of Saint Elizabeth: (13:17) Thank you Greg

Kasia Taylor: (13:18) How do address the increasing need for remote access with the growth of online delivery

Frank@WCUPA.EDU: (13:18) I get a text every time my CC gets used.

Teresa Banks: (13:18) Ageed, Tammy Clark! We can have millions of dollars spent on tools, and one good spear phishing campaign can blow it all up. Security Awareness is critical!
Tim Tolson, UVa ISPRO: (13:18) An interesting related question is do you have your credit cards setup for immediate transaction notifications?

Joanna LynGrama: (13:19) @Carlos: 12% of institutions have formalized IT governance, risk, and compliance programs. If your institution is an ECAR subscriber you can view the report at: http://www.educause.edu/library/resources/it-governance-risk-and-compliance-higher-education

Evy L. - University of Arizona: (13:19) @Frank That's one of the reasons I love Google Wallet so much. I can add multiple cards to it, use it from my phone, get text messages every time it's used, etc.

Frank@WCUPA.EDU: (13:20) all our students and employees use 802.11x for wireless

Trish: (13:20) We have Guest wifi as well as Secure for employees/students. However, 70% of users still use Guest, they haven't taken the time to sign up/sign in for Secure.

Bart: (13:20) How do you balance funding campus wide security at a baseline versus funding high profile or critical research areas that require elevated security measures?

Melissa Woo - University of Oregon: (13:20) @Teresa and @Tammy - People are key!

Tim Tolson, UVa ISPRO: (13:20) For public wi-fi - how do you handle DMCA complaints and police requests for ID?

Deyu: (13:20) too many password to remember, any secure and easy ways to deal with that?

Patrick - University of the West Indies: (13:20) Information Security Concern: How to get staff, especially faculty and high level staff, to buy into the concept that Info. Security is everyone's responsibility


Ben Marsden, Smith College: (13:21) re: pwd managers, I clearly feel benefits outweigh the risks

Frank@WCUPA.EDU: (13:21) Key research for password vaults: who can open it if you forget your key?

Melissa Woo - University of Oregon: (13:21) @Pete Nerf? :-)

Kevin: (13:21) Andrew Carnegie said "Put all your eggs in one basket - then watch that basket!"

Teresa Banks-Univ of Arizona: (13:21) Thanks, Melissa! We have online training, but I will take any opportunity I can get to get one of our staff in front of an audience to really get that personal touch on awareness!

Melissa Woo - University of Oregon: (13:21) @Pete Seriously, that could backfire in terms of customer service, right?
Tim Tolson, UVa ISPRO: (13:22) I think using password manager is safer/better than repeating passwords, writing it down, and not changing ones. There are password managers that allow you to encrypt and store.


Teresa Banks-Univ of Arizona: (13:22) I agree that password managers can be great tools. Personally, I still don't save my most sensitive information in them (bank accounts, credit card accounts), but use them for less sensitive information.

Ricardo Carlos - Univ. of Arizona: (13:22) InfoSec concern: growing use of external apps (e.g. Dropbox) that IT depts. must account for in their incident response policies and procedures

Frank@WCUPA.EDU: (13:23) Yea. dropbox type apps are an issue for Discovery as well.

Tammy Clark, Univ of Tampa: (13:23) Patrick - University of the West Indies: to get people to buy in you have to work with campus departments and help them to understand their responsibilities. I've found that they will buy in if they clearly understand how to do so

Pete Hoffswell (Davenport U): (13:23) Slow public wifi can be managed with expectations set. "force" isn't the right word. Just make secure wifi more desireable.

Bo: (13:23) We have cyber insurance - not sure it is valued right yet. I struggle with it.

Carlos S. Lobato: (13:24) Question for CIOs, should the CISO report solely to them or should they have dual reporting to ensure unacceptable risks get reported to the decision makers???

CSU: (13:24) IS anyone using penetration testers or employing them?

David Saacke/W&L: (13:24) Dual

Frank@WCUPA.EDU: (13:24) I'm the CISO for our campus and report to one of the directors for net/servers.

Tammy Clark, Univ of Tampa: (13:24) Carlos, I think it's critical for CIO's and CISO's to establish a strong partnership. I report to the president of our university and I work closely with the CIO every day.

Deyu: (13:25) what is exactly a cyber insurance?

Melissa Woo - University of Oregon: (13:25) @Carlos I think that is environment/maturity dependent. In some cases, perhaps the CISO should report directly to the Pres (though that would be a very mature institution).

Frank@WCUPA.EDU: (13:25) though I do "nag" other departments within IT.
Cole Campise: (13:25) I am struggling with the idea of reporting line. At this time my CISO reports directly to me VPIT/CIO ... considering adding a dotted line

Bo: (13:25) I like to keep the CISO withing the CIO Office- seperate from the IT unit

Carlos S. Lobato: (13:25) Tammy, I recommend your reporting line

Melissa Woo - University of Oregon: (13:25) @Bo Good point. If Office of the CIO is at least somewhat independent of central IT, that might work well.

Tammy Clark, Univ of Tampa: (13:28) Deyu:Cyberinsurance is insurance in the event of a breach, but read the terms and conditions because they require policy holders to develop a strong and effective information security program and be able to demonstrate that, as well as encrypt data

Melissa Woo - University of Oregon: (13:28) @CSU - We do pen testing for PCI-DSS compliance.

Melissa Woo - University of Oregon: (13:30) @CSU - We'd consider pen testing for other reasons, going forward but would want to assess based on risk .

Valerie Vogel, EDUCAUSE: (13:30) Michele referenced the NIST Framework: http://www.nist.gov/cyberframework/

Deyu: (13:32) Tammy Clark, Univ of Tampa, thank you!

Andrew Mantuano - Bryn Mawr College: (13:32) Hi everyone -- I'd like to hear what you've been doing to address the training/awareness concern. Are you using third-party tools such as SANS Securing the Human or Wombat Security, in-house specialists, creating asynchronous materials (PowerPoints, other CBT), ect., and has it been effective?

Tammy Clark, Univ of Tampa: (13:32) Deyu:You're welcome! :-)

Teresa Banks-Univ of Arizona: (13:32) We have used customized online training for several years, but are switching to SANS Securing the Human this year.

Tammy Clark, Univ of Tampa: (13:33) Andrew, I use SANS Securing the Human and so far, 95% of staff, faculty and third parties at UT have taken this training (I assign between 4-8 modules at a time)

Carlos S. Lobato: (13:33) Andrew, we just created a Computer & Data Security training, which is going to be mandatory for all faculty & staff. We used PPT to develop, but it will be uploaded to our SABA training database.

Teresa Banks-Univ of Arizona: (13:33) Tammy, I'd love the opportunity to talk to you offline on your rollout of this and what modules you group together.
Deyu: (13:33) we have inhouse training for cybersecurity, it is bundled with each track and is a required course

Tammy Clark, Univ of Tampa: (13:34) Sure Teresa tclark@ut.edu

Teresa Banks-Univ of Arizona: (13:34) Thanks!


Alastair MacLeod: (13:34) We are doing a student curricular project where they are asked to design a security awareness campaign. We give cash prizes. We are an art and design school

Bo: (13:34) We are just rolling out a moodle course on Information Security Awareness - I can't rmeber from who, but we did a consortial purchase with other Universities here in Canada

Valerie Vogel, EDUCAUSE: (13:35) More about HEISC: www.educause.edu/security

Tammy Clark, Univ of Tampa: (13:35) Lots of great information security awareness resources in the Guide Joanna referenced:-)

Teresa Banks-Univ of Arizona: (13:35) That sounds very cool, Alastair! We have rolled out a new student awareness campaign that was designed by our student workers. They are certainly our largest audience, and the hardest one to reach.

Valerie Vogel, EDUCAUSE: (13:35) We're now accepting proposals for our conference! www.educause.edu/sec15

Bo: (13:35) That course was for all staff faculty and students - different courses

Tammy Clark, Univ of Tampa: (13:36) Teresa--I'm doing that also (having student workers design student-centric security awareness training)

Teresa Banks-Univ of Arizona: (13:36) I think having student involvement really helps us with our messaging, and obviously others have found that as well.

Frank@WCUPA.EDU: (13:37) The hard part is what "venue" to use to share information and conversations on a regular basis. Something easy for CISOs and CIOs to connect and interact.

Carlos S. Lobato: (13:38) I like these institutional considerations, I wonder how many schools have conducted a formal written Information Security Risk Assessment?

Andrew Mantuano - Bryn Mawr College: (13:38) Thanks for sharing, all!
Joanna LynGrama, EDUCAUSE: (13:39) @Carlos: We’ve got data on that in the Core Data Service.

Tammy Clark, Univ of Tampa: (13:39) Carlos--I have conducted a campus wide risk assessment when I arrived at UT in 2012 and I'm starting another one now--it’s vital as Peter said, to prioritize the issues.

Melissa Woo - University of Oregon: (13:39) @Frank - One of things we need to work on is effective communication between CISOs and CIOs.


Greg Smith, Missouri S&T: (13:41) We require completion of a set of SAN - Secure the Human modules. Deadline is end of the year and faculty have agreed that the penalty for not completing will be disabling their account.

Joanna LynGrama, EDUCAUSE: (13:41) @Carlos: In 2013, CDS responding institutions reported about 60% of institutions conducted an information security risk assessment on central IT systems and data.

Teresa Banks-Univ of Arizona: (13:41) I am really grateful for the chat feed. I have learned a TON from you all!

Tim Tolson, UVa ISPRO: (13:42) Carlos - UVa has written Risk Mgmt review - every 3 years has to be updated. Just finishing getting the reports in.

Trish: (13:42) Does anyone use SANS on a voluntary/opt-in basis?

Trish: (13:42) (sorry- I mean the SANS securing the human materials, if that wasn't clear)

Greg T - UTK: (13:43) @Trish UTK does for the moment; we ask faculty & staff to do the training but there's no stick for not doing it.

Tammy Clark, Univ of Tampa: (13:43) Greg Smith--that's awesome--getting faculty to participate is important also

Alastair MacLeod: (13:44) Teresa, were the student workers paid for their work on the campaign or was it a prize as a motivator?

Trish: (13:44) Greg - do you have any numbers on the participation rate?

Frank@WCUPA.EDU: (13:44) Dotted lines to the network/server groups would probably be good.

Greg T - UTK: (13:44) Trish- No; I'm at the department level and our CISO keeps pretty quiet.

Greg Smith, Missouri S&T: (13:44) 51% have completed the SANS training

Bo: (13:44) @trish we don't use SAN but use Bullseye - we are pitching it be mandatory - see how that goes next week :-)

Trish: (13:45) Greg T - Okay, thank you!

Trish: (13:45) Greg Smith - so even with mandatory training, only 51%?

Tammy Clark, Univ of Tampa: (13:46) It's important for the CISO to have the degree of autonomy needed to be successful

Tammy Clark, Univ of Tampa: (13:46) Whether situated within IT or outside

Teresa Banks-Univ of Arizona: (13:46) Tammy, I'm lucky enough to have had an artist working for me for the past few years, so she has been key in developing our materials. As well, the other student workers were also paid by our office. My plan going forward is to work with academic units (e.g., College of Fine Arts, Journalism department).

Greg Smith, Missouri S&T: (13:46) We are starting to get more aggressive in pushing for completion

Leland Lyerla: (13:47) Can you give advice for dealing with a "roll the dice" attitude from higher administration, particularly the CFO?

Melissa Woo - University of Oregon: (13:47) @Tammy Agreed re: autonomy regardless of reporting line

Tammy Clark, Univ of Tampa: (13:47) Teresa, that's great -- I hired marketing majors and I agree that is really helpful

Frank@WCUPA.EDU: (13:47) Incident response for IT could be modeled after FEMA Incident response for a common lanaguage. FEMA-IS-100 is a great free into course on it.

Teresa Banks-Univ of Arizona: (13:47) Great way to go, Tammy!

Trish: (13:47) Greg Smith - thank you! We have the SANS materials but haven't started our campaign yet. The decision to make it mandatory isn't on the table, but I'm trying to gauge what I should anticipate as far as voluntary completion goes

Teresa Banks-Univ of Arizona: (13:47) You're giving them real world experience. I have always said that we have to MARKET security -- get people to eat their vegetables and LIKE THEM!

Tammy Clark, Univ of Tampa: (13:48) Yes, that's right, Teresa! :-)

Melissa Woo - University of Oregon: (13:48) @Leland Could you please clarify "roll the dice"? Thanks.

Alastair MacLeod: (13:48) Thanks for sharing this stuff Teresa

Greg T - UTK: (13:48) Teresa- Wow, the materials on UA's infosec site are great. Just curious, how many staff are in your office?

Teresa Banks-Univ of Arizona: (13:48) Greg, we have 4 fulltime staff, and two student workers currently.
Pete Hoffswell (Davenport U): (13:49) "Push your luck", @leland? or "It won't happen to us.."

Greg Smith, Missouri S&T: (13:49) We were embarrassed by some phishing attacks that helped us to gain campus buying for the SANS Training. The training is actually pretty good.

Leland Lyerla: (13:49) Sorry, by that I mean a reactionary attitude that nothing has happened, so why worry?

Teresa Banks-Univ of Arizona: (13:49) Our website graphics were primarily designed by my student worker Rae Cooper and me.

Greg T - UTK: (13:49) Teresa- Thanks. They do good work!

Teresa Banks-Univ of Arizona: (13:49) Our student awareness page for our campaign is security.arizona.edu/think

Tammy Clark, Univ of Tampa: (13:49) Trish, whether you make the training mandatory or optional you will still need to campaign and actively seek buy in from your campus community or it may get ignored as everyone is busy and doing more with less

Leland Lyerla: (13:49) @pete- Exactly.

Melissa Woo - University of Oregon: (13:50) @Leland @Pete Our job is to communicate risk effectively so that the institution can make informed decisions re: infosec.

Teresa Banks-Univ of Arizona: (13:50) Thank you, Greg! I'm really proud of the work that Rae has done for us. She is graduating with a wonderful portfolio.

Pete Hoffswell (Davenport U): (13:51) I like the thought of "consider yourself already hacked". There are security holes, and there's a very good chance that they've been taken advantage of. That mindset may be a valuable platform for an infosec dialogue.

Tammy Clark, Univ of Tampa: (13:51) Pete, my addition to that thought is if you were hacked would you even know it

Leland Lyerla: (13:52) We are in the early stages of our program at a small private university. Gaining a foothold is proving to be a challenge.

Tammy Clark, Univ of Tampa: (13:52) that to me is a primary consideration as well

Melissa Woo - University of Oregon: (13:52) @Pete But of course - it's just a matter of when we discover the breach. :-(

Tammy Clark, Univ of Tampa: (13:52) Hang in there, Leland--the Guide has a CISO toolkit that I think you will find helpful as well as the topics and resources in the Guide
Valerie Vogel, EDUCAUSE: (13:53) Please watch for a special transmedia piece on CISOs in November! (See "Why CIO Is the Best Job on Campus" as a recent example of an EDUCAUSE transmedia piece: http://www.educause.edu/visuals/shared/erextras/2014/Good2bCIO/default.htm)


Leland Lyerla: (13:53) @Tammy - Thank you.

Carlos S. Lobato: (13:56) Good job at mentioning NIST requirements and how federal agencies now include a term as part of their grants & contracts. CISOs need to start learning more about FISMA requirements.

Tammy Clark, Univ of Tampa: (13:57) We use ISO 27001/2 and NIST and I agree with Peter about the commonalities between the two


Melissa Woo - University of Oregon: (13:58) Yes - please consider getting involved in HEISC!

Tammy Clark, Univ of Tampa: (13:58) Thanks to these CIO's for the great presentation

Melissa Woo - University of Oregon: (13:58) (Disclaimer: I'm co-chair of HEISC :-))

Melissa Woo - University of Oregon: (13:58) Thank you everyone for a lively conversation!