From Art to Science: How Risk Can Transform Your Information Security Program

HEISC Webinar
May 30, 2017

Chat Transcript


_EDUCAUSE Help - Karen Wetzel: Chat with attendees using this chat area or tweet using this hashtag: #HEISC

_EDUCAUSE Help - Karen Wetzel: As we wait for today's session to begin, feel free to introduce yourself in the chat.

Jamie D: Jamie Daniel from the University of Puget Sound - looking forward to formalizing our risk assessment process with our Information Security Manager. Enjoying a cool & slightly wet day in the beautiful Pacific NW.

Valerie Vogel, EDUCAUSE: Welcome Jamie! We're glad you could join us today!

cyber blake: Isn't Risk a board game?

Jamie D: It is indeed, a good one!

Karen A. Wetzel: Again, welcome to today's event! We'll be starting in just a couple minutes.

Matthew Dalton: Glad you could join us, Jamie!

Karen A. Wetzel: Thank you for participating in today's HEISC webinar "From Art to Science: How Risk Can Transform Your Information Security Program". If you have any technical difficulties, please post a note in the chat area.

Karen A. Wetzel: The audio recording, slides, and transcript will be available after today's event from the EDUCAUSE cybersecurity website: www.educause.edu/security

_EDUCAUSE Help – Karen Wetzel: If you experience any audio issues, please click on the Audio Issues Link in the lower right hand corner. This page will open in your browser, within a new tab or window.

Silvio Balzano-Fordham: Those that have informal assessments...how do you go about doing that? I would like to hear more...
David Escalante, BC: Darts, Silvio, darts... :-)

Silvio Balzano-Fordham: I use a Ouija board myself...

cyber blake: Magic 8 ball

David Escalante, BC: The advantage of darts is that you can pop peoples' bubbles during the process! :-)

Matthew Dalton: Hopefully not lawn darts, David.

Sue McGlashan: Yes

Valerie Vogel, EDUCAUSE: Binary Risk Assessment: http://binary.protect.io/

Valerie Vogel, EDUCAUSE: For this 3rd poll, you can type in a short answer.

Nick Lewis - Internet2: For managing risk, it's also managing the costs associated and effective security spending.

Silvio Balzano-Fordham: Agreed.

Silvio Balzano-Fordham: It's a balancing act.

Matthew Dalton: True, Nick. It's always a balance between the risk appetite and the cost of mitigation.

Joanna Lyn Grama: How do you handle business units choosing to accept a risk that the security department things must be mitigated or addressed somehow? (i.e.,

Joanna Lyn Grama: I mean, what is the documentation process?

_EDUCAUSE Help – Karen Wetzel: See the IT Risk Register from EDUCAUSE Governance, Risk, and Compliance program: https://library.educause.edu/resources/2015/10/it-risk-register

Mandy Winegarden: Documentation wise - Our risk acceptance/treatments are in a final document that's signed by both CISO and a Dean/VP to acknowledge.

Matthew Dalton: Joanna - That's a great question, and ties into my first caveat of Risk only being good for the "known". Often departments/units will accept risk without you even knowing about it.

Sue McGlashan: I find this risk register very high level - not that helpful in trying to help people improve at the level of applications that access sensitive data.

Matthew Dalton: It's important to include all parties to help attempt to reduce that risk.
Silvio Balzano-Fordham: But you also don't want the opposite to occur, which sometimes does...IT accepting risk instead of the departments/units

Jenny P. (Longwood): @Silvio: #truth

Sue McGlashan: And agree with Silvio - one of the questions we get is "so, can we use this application?" rather than - "ok, we accept the risk"

Matthew Dalton: Silvio - Agreed

Mandy Winegarden: Sue, we get that question a lot too. The more we use standardized templates that feel like real deliverables in our language around risk, the less we are getting that kind of inquiry for "approval"

Silvio Balzano-Fordham: @Sue: I share my risk register with a risk committee and talk them through it.

Mandy Winegarden: We do a lot of meetings to walk people through the concepts and results as well

Amy Tunison: Mandy, are you willing to share your templates?

Joanna Lyn Grama: @Sue: Yes, the IT GRC risk register was meant to be very high level for strategic IT risks. Definitely need something more granular for an infosec risk management program

_EDUCAUSE Help – Karen Wetzel: Chat with attendees or ask the speaker a question using this chat area or tweet using the hashtag: #HEISC

Mandy Winegarden: I can check with my team! I know we've gotten inspiration from others so that shouldn't be a problem!

Silvio Balzano-Fordham: We all get inspiration from others...

Joanna Lyn Grama: If an institution has never done a risk assessment before, any advice on which departments/areas to target for a first risk assessment?

Mandy Winegarden: @Silvio so true. Thank goodness for it!

Shanna Erdman: Mandy, I would be interested in looking at these templates too

Shanna Erdman: If you were willing to share

Sue McGlashan: Matthew - how do we measure "reputation"?
Mandy Winegarden: @Shanna and @Amy. I copied down your names and I will double check with my team and follow up with you

Sue McGlashan: Please add me, Mandy

Mandy Winegarden: You bet!

Cari: Hi Mandy, I would be interested as well! cfriesen@socc.edu

Shanna Erdman: Thank you!! I hope we can help each other

Matthew Dalton: Sue - that can vary from institution to institution. It largely is articulated by your executives, and your University Relations, marketing, etc.

Nick Lewis - Internet2: Then, develop the institutional processes around the risk register. Register is great, but need the process and buy-in!

Valerie Vogel, EDUCAUSE: @Mandy – If you could also share the template with me, our HEISC GRC working group members would also be interested in seeing it. (vvogel@educause.edu)

Sue McGlashan: Agree about education!

Mandy Winegarden: @Valerie and @Cari – Of course. I added you both to my list for follow-up

Valerie Vogel, EDUCAUSE: hanks so much, Mandy!

Joel Garmon -- WFU: If it is a university-wide risk, then an individual department cannot accept the risk, must be at a higher level or the risk committee

José A. Domínguez (UO): @Mandy, could you please add jad@uoregon.edu too ... Thx

Jess: Risk is only discussed in IT. How can executive management be made aware of the risk conversation?

Joel Garmon -- WFU: We also focused risk assessments on departments that handle PII

_EDUCAUSE Help – Karen Wetzel: Please continue to send your questions or comments to the chat area and we'll get to them as soon as we can.

Mandy Winegarden: How does your risk program integrate with policy/governance?

Silvio Balzano-Fordham: @Joel, agreed. If not at departmental level, it has to go up...

Barney: Is the conversation about risk the same when talking to IT as when talking to executive leadership? What are the significant differences?
Sue McGlashan: Language and metrics, I think

Valerie Vogel, EDUCAUSE: Here is a blog about speaking with the board about infosec (somewhat related to @Barney's question): [http://er.educause.edu/articles/2016/1/leading-an-effective-briefing-with-board-executives-about-information-security](http://er.educause.edu/articles/2016/1/leading-an-effective-briefing-with-board-executives-about-information-security)

_EDUCAUSE Help – Karen Wetzel: Before signing off, please share your feedback on this event at: [https://goo.gl/forms/vi7MEPittlx5IdSx2](https://goo.gl/forms/vi7MEPittlx5IdSx2)

Barney: I see it the other way around - executive define risk, IT deal with the threats and vulnerabilities.

Silvio Balzano-Fordham: That goes to what I said...the conversation with the execs is informative (both ways) where IT is directive (you need to address this)

Sue McGlashan: IT needs ownership in making sure that they do not introduce insecure practices that increase likelihood of "something" happening

Silvio Balzano-Fordham: Yes.

Silvio Balzano-Fordham: But deadlines get in the way sometimes...

_EDUCAUSE Help – Karen Wetzel: A recording of this webinar will be made available after today’s event at www.educause.edu/security

_EDUCAUSE Help – Karen Wetzel: If you have questions about future events or suggestions for new topics, e-mail us at security-council@educause.edu

_EDUCAUSE Help – Karen Wetzel: Thank you so much for joining today's event!

Silvio Balzano-Fordham: Thank you all!

Antonio Crespo (Barnard College): Thanks everyone!

Jamie D: Thank you!

Joanna Lyn Grama: Thank you to the speakers---great info!

cyber blake: Thanks everyone.

Keir Novik (SFU): Thank you, excellent webinar!

randy: Thanks

Sue McGlashan: Thanks
Barney: Thank you.

José A. Domínguez (UO): Thank you for the webinar. It was very useful.

Mandy Winegarden: Thanks all!

_EDUCAUSE Help – Karen Wetzel: EDUCAUSE Cybersecurity
Website: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative