Captured Chat from the April 7th, 2021 Security Summit

8:17:00 am - You:
Slides and many other resources are available at summit.ecmecc.org

8:20:17 am - Nicole Pruden:
Slides and many other resources are available at summit.ecmecc.org

8:35:40 am - Nicole Pruden:
Slides and many other resources are available at summit.ecmecc.org

8:42:38 am - Kimberly Briske:
We have looked at risk assessments, but haven't completed one. Not sure if there is a poll on this coming up, but I'd love to learn more from the group about how many have completed assessments and what has changed as a result of them.

8:56:30 am - Chris Lee:
Are you still doing Risk Assessment Workshop?https://docs.google.com/forms/d/e/1FAIpQLScsmAC_YkdgdSZUWOzgRmymSWZQLwqs8xex04grG495UDMwHQ/viewform

9:00:45 am - Nicole Pruden:
Hey Chris, we haven't held any recently but that is something we're certainly interested in exploring!

9:02:45 am - Justin LeClair:
I think her microphone is having connection issues

9:02:57 am - William Groskreutz:
I agree Justin

9:04:07 am - Mary Mehsikomer:
Yes

9:05:08 am - Nicole Pruden:
Feel free to use the Q&A or Chat for Questions!

9:06:53 am - Mike Dronen:
@Dan, do you see insurers changing their policies/premiums for schools specific to whether or not a school district uses multi-factor authentication (MFA)?

9:10:08 am - Amy Diedrich:
Great question Mike, we will be addressing that a bit later in the presentation. The short answer is they may not issue a policy without MFA

9:11:14 am - Mary Mehsikomer:
Wow. I have been wondering about the ransom question.

9:11:52 am - Mike Dronen:

Thanks Amy

9:12:32 am - Eric Simmons:
From Marc's question earlier: MN Technology Leaders are meeting tomorrow, April 8 @ 9:30 AM https://meet.google.com/may-opnk-ihp : IT Board Policy, Student and Staff Privacy policies, and Student Data Privacy Agreements (524 and beyond). We intend to put together policy review and revision work sessions. Mntechleaders.org . Email me with any follow up! esimmons@isd2144.org

9:13:09 am - Mary Mehsikomer:
If you are not on the mailing list for MN Technology Leaders and would like to be, email Eric or me at mary.mehsikomer@sourcewelltech.org

9:13:37 am - Pete Royer:
Biggest question, do you lower the rates the more a school district has Security policies and procedures in place?

9:15:43 am - Mary Mehsikomer:
Marc Johnson is always sending spam. He's terrible. (just kidding)

9:15:59 am - Amy Diedrich:
Pete we are currently using that as a way to lessen the increase that all schools will see this year. We will talk more about this years renewal later in the presentation that is where we will spend most of the time

9:30:42 am - Eric Simmons:
And that's all email, correct? Even if we use web-based email like Gmail?

9:31:01 am - Chris Lee:
how much resistance from staff using personal devices for MFA?

9:31:04 am - Ryan Cloutier:
MFA is now a minimum reasonable security control. lack of MFA may not be defensible as being non negligent anywhere you can implement MFA do so all apps and systems.

9:31:52 am - Mike Klun:
Is this for all systems? Are you asking for MFA for financial system? We use SMART and would have to contact them for MFA.

9:32:29 am - Ryan Cloutier:
Yes all systems including 3rd party's you can use something like Duo to help with managing multiple MFA systems in a single pane of glass

9:32:50 am - Amy Diedrich:
Understanding what controls are in place with your third party vendors is critical. It is still considered district data

9:33:31 am - Nicole Pruden:
@mike I believe smart has MFA abilities. It might even be required by them already

9:34:21 am - Kimberly Briske:

Smart has security questions, I believe, but not a MFA to another device/account.

9:34:49 am - Nicole Pruden:
@Chris I've heard of some resistance to using personal devices for MFA, but there are physical tokens that can also be used.

9:35:07 am - You:
You are doing fine, Dan on pace! Great information!

9:38:14 am - Ryan Cloutier:
Paper is still the best method for plans

9:39:01 am - Nicole Pruden:
@Kimberly - you are correct default is just security questions.

9:41:16 am - Ryan Cloutier:
Poor configurations was what caused Solarwinds, those customers who had it configured correctly were unaffected. (take away know your configurations and restrict internet access when not 100% needed)

9:43:13 am - Mike Dronen:
The The K-12 Cybersecurity Resource Center report states, that up to 75% of school breaches fault the vendor as the root cause! Page 14 of this report:
https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf

9:51:59 am - Eric Simmons:
For our collaboration as schools later: MFA Implementation ideas for all staff Google accounts. Not something we do now beyond admin roles and don't think we are alone..!

9:53:15 am - Nicole Pruden:
Amy - If you can share the slide and other resources with me I can load to our website for the event to get out to participants.

9:55:22 am - Michael Danielson:
SMS is no longer a secure MFA method.

9:57:36 am - Ryan Cloutier:
use a MFA solution to keep it a single pane of glass, also use app based not sms based MFA

10:00:09 am - Travis Rupp:
What's recommended for App MFA? Google Authenticator or what else?

10:00:18 am - Eric Simmons:
Thanks Amy and Dan!!

10:00:49 am - Nicole Pruden:
@Travis We've started exploring the FortiToken Mobile app because then you can MFA your Fortinet stuff as well as other accounts

10:01:04 am - Ryan Cloutier:

i like Duo and i use the MS and google Authenticator apps

10:01:14 am - Amy Diedrich:
We are also education the school board on this and the need to support cyber security efforts in their districts

10:01:22 am - Travis Rupp:
Ok, thanks Nicole and Ryan

10:01:55 am - Nicole Pruden:
Our biggest concern is not having multiple different apps for staff so we have less confusion or "user errors"

10:07:02 am - Brady Carstens:
Should we be concerned with using a 3rd party for MFA? Even though it gives another layer of security doesn't also add another layer of possible compromise?

10:08:51 am - Sumre Robinson:
Do the apps eliminate the need for a second device to receive any security codes? Huge road block to staff and student MFA enforcement is requiring users to use personal devices and how to manage it in environments where we might not don't personal devices on our network.

10:30:40 am - Nicole Pruden:
Book:
https://www.amazon.com/Learning-Continuity-Planning-Handbook-Universities-ebook/dp/B08RD45P3N

10:34:44 am - Nicole Pruden:
SnipeIT https://snipeitapp.com/

10:36:19 am - Mary Mehsikomer:
No shaming though! If you make it safe they will come to you and tell you what happened.

10:36:35 am - Nicole Pruden:
Very good point mary!

10:38:09 am - Mary Mehsikomer:
Chocolate is very powerful and should not be underestimated.

10:42:40 am - Nicole Pruden:
FYI - Marsh & McLennan Agency's resources are now available on the resources page of the summit site (summit.ecmecc.org/Resources)
There is the presentation and the cyber resiliency network information

10:43:19 am - Chris Lee:
named accounts, how likely is that with service providers with rotation/high turn over (ie HVAC, Printer Management, etc).

10:43:39 am - Nicole Pruden:
Amy also has said that she's more than willing to review your current policy and provide quotes. If

you're interested in that reach out to her at amy.diedrich@marshmma.com

10:46:58 am - Joseph Samek:
With most data living in cloud/web systems, does that change how we approach a local device incident?

10:51:12 am - Eric Simmons:
Our language is something like, "as soon as you suspect that personally identifiable or confidential data for which you are responsible might have been compromised."

10:54:31 am - Andrew Johannes:
IOMEGA ZIP BB

10:57:32 am - Nicole Pruden:
STIGS document library https://public.cyber.mil/stigs/downloads/

11:09:25 am - Nicole Pruden:
Wizer https://www.wizer-training.com/
ECMECC also has special pricing for InfosecIQ as a security awareness training and phishing platform https://securityiq.infosecinstitute.com/

11:11:26 am - Scott Antkowiak:
snickers are the best

11:11:39 am - Chris Lee:
Butterfinger BBs

11:12:18 am - You:
This is linked on the summit resources page too, but it is a great template for creating an incident response plan - in school language - it includes a template and a set of instructions to help you "make it your own" and implement.
https://www.incidentresponsetool.org/tools/incident-response/flowchart/

11:15:44 am - Mike Klun:
We delete their student network folders but we archive their google data. It becomes read only. Do we delete the graduating google accounts.

11:16:01 am - Nicole Pruden:
Nist 800-88 https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

11:17:00 am - Mike Klun:
If you use bitlocker and intune is that sufficient?

11:18:34 am - Jeffrey Johnson:
Can you provide your hardening guides?

11:19:16 am - Nicole Pruden:
CIS has some hardening guides https://workbench.cisecurity.org/benchmarks
I believe the STIGs Ryan mentioned are also hardening guides
https://public.cyber.mil/stigs/downloads/

11:19:51 am - Ryan Cloutier:
https://s2me.io

11:20:46 am - Nicole Pruden:
Also if you want to do a free assessment of your district you can do that here:
https://securitystudio.com/ecmecc/

11:21:17 am - Jennifer Ridgeway:
Thanks Ryan. Will someone include the chat notes with the recording?

11:21:22 am - Ryan Cloutier:
rcloutier@securitystudio.com

11:21:33 am - Nicole Pruden:
Yes we will get the chat!

11:22:02 am - Mary Mehsikomer:
Ryan - that was great as always!

11:22:16 am - James Hatz:
Fantastic session!

11:22:20 am - Ryan Cloutier:
Mike Klun for Encryption bitlocker is good, intune is good for managing devices i like them both.

11:23:28 am - Mary Mehsikomer:
Nicole is awesome! Call her up.

11:23:40 am - Nicole Pruden:
Aww shucks Mary!

11:24:48 am - Mary Mehsikomer:
Thank you Marc, Jenny, Nicole and Jon for this great event!

11:25:35 am - Nicole Pruden:
Here's that link again: https://securitystudio.com/ecmecc/

11:26:18 am - Susan Heidt:
Thank you EcMECC for coordinating this for us. Excellent sessions and resources.

11:26:28 am - Kimberly Briske:
Agreed. Thank you!

11:26:44 am - Cory Zimpel:
Thank you ECMECC and others!

11:26:48 am - Ryan Cloutier:
Thank you everyone! have a great rest of the conference!

11:27:06 am - Mike Dronen:
Thanks all!

11:27:13 am - Forrest Fosheim:
Well done guys. Thanks.

11:27:16 am - Tama Exsted:
Thank you

11:27:19 am - Tracy Benson:
thank you!

11:27:21 am - Justin LeClair:
That's everyone! Have a good one!

11:27:23 am - Dan Voce:
thanks Marc

11:27:29 am - Paul Brashear:
Thanks all.

11:27:44 am - Becky Coleman:
Thank you!