Asset	Attack Surface [1]	Threat Description [2]	What could go wrong? [3]	Control	Impact [4]	Likelihood [5]	Control Effectiveness [6]	Inherent Risk Level Scale: 1 - 25 [7]	Residual Risk Level Scale: 0-25 [8]	Further Mitigation Warranted?	Action/Mitigation Plan	Mitigation Activity Owner
Internal Information	Google Drive	C,I loss through incorrect permissions.		Policy and auditing	2	3	4	6	2	No	Periodic audits.	
		C,I loss through compromised authN.		Policy and 2FA, Google 30 day retention policy	2	1	5	2	0	No		
		C,I,A loss through internal Google tampering.		Free markets	2	1	3	2	1	No		
	CTSC Uncontroled Media/Communicaitons	C loss through exposure.		CTSC Policy (need to formalize) & Local IT policies	2	1	3	2	1	Yes	Have formal infomation protection policy for CTSC Staff.	Adams
Approved Access Information	Google Drive	C,I loss through incorrect permissions.		Policy and auditing	4	3	4	12	5	Yes	Run audit checks more regularly as functionality of software improves.	Krenz
		C,I loss through compromised authN.		Policy and 2FA, Google 30 day retention policy	4	1	5	4	1	No		
		C,I,A loss through internal Google tampering.		Free markets	4	1	3	4	2	No		
	CTSC Uncontroled Media/Communicaitons	C loss through exposure.		CTSC Policy (need to formalize) & Local IT policies	4	1	3	4	2	Yes	Have formal infomation protection policy for CTSC Staff.	Adams
Engagement-related Information	Google Drive	C,I loss through incorrect permissions.		Policy and auditing	3	3	4	9	4	Yes	Run audit checks more regularly as functionality of software improves.	Krenz
		C,I loss through compromised authN.		Policy and 2FA, Google 30 day retention policy	3	1	5	3	1	No		
		C,I,A loss through Google internal tampering.		Free markets	3	1	3	3	2	No		
	CTSC Uncontroled Media/Communicaitons	C loss through exposure.		CTSC Policy (need to formalize) & Local IT policies	3	2	3	6	4	Yes	Have formal infomation protection policy for CTSC Staff.	Adams
Public Information/Tools	Google Drive	I loss through incorrect permissions.		Policy and auditing	3	3	4	9	4	No		
		I loss through compromised authN.		Policy and Google 30 day retention policy	3	1	2	3	2	No		
		I,A loss through internal Google tampering.		Free markets	3	1	3	3	2	No		
	CTSC Uncontroled Media/Communicaitons	C loss through exposure.		CTSC Policy (need to formalize) & Local IT policies	1	2	3	2	1	No		
TrustedCI Web Pages (Squarespace)		I loss through compromised authN.	Lose reputation due to hacked site	Web server's authN	3	2	2	6	5	No	See if 2FA is an option from squarespace.	
		A loss through DoS.		Free market	3	2	1	6	6	No	Current DDoS mitigation strategies require shifting the traffic through a 3rd party for filtering; these seem unwarranted for us, for now.	
Blog	Google Blogger	I loss through admin-level compromised authN.		blogger.com's authN (since Google, assuming 2F)	3	2	4	6	2	No		
		I,A loss through internal Google tampering.		Free markets	3	1	3	3	2	No		
		I loss through post-level compromised authN or egregious post.		Notifications on comments reviewed by staff before publishing	2	3	5	6	1	No		

Twitter identity		I loss through admin-level compromised authN.		Twitter's authN	3	2	3	**6**	**4**	No		
		I loss through post-level compromised authN.		Squarespace's authN	2	2	2	**4**	**3**	No		
		I,A loss through internal Twitter tampering.		None	3	1	1	**3**	**3**	No		
Domain Name Registrar	ghandi.net	I,A loss through compromised authN.		ghandi.net's authN	3	2	3	**6**	**4**	No		
		I,A loss through internal Ghandi tampering.		Free markets	3	1	3	**3**	**2**	No		
IU mailing lists		I,A loss through compromised authN.		IU's authN	1	1	3	**1**	**1**	No		
Teleconferencing services		I,A loss through compromised authN.		Conference services authN	1	1	2	**1**	**1**	No		
Adobe Connect		I,A loss through compromised authN.		Adobe Connect authN, Free market	2	2	4	**4**	**2**	No		
		Reputation loss through compromised flash plugin.		Rigourous patching, isolating the webinar process, but realistically, none	3	2	1	**6**	**6**	No	Explore another webinar platforms as discovered	
		A loss though service outage.		Free market	2	2	3	**4**	**2**	No		

[1] Identify the information system or portion/component thereof through which the threat would compromise the asset.

[2] Identify the risk. Think in terms of root cause, source, or threat, rather than outcome.

[3] Identify the possible outcome or effect of the risk occurring.

[4] If the risk were to occur, what would be the impact (of a single occurence)?
5 - Catastrophic
4 - Major
3 - Moderate
2 - Minor
1 - Insignificant

[5] What is the estimated frequency of occurrence?
5 - Constant, or extremely frequent
4 - Very frequent
3 - Somewhat frequent
2 - Infrequent
1 - Rarely, if ever

[6] What is the current effectiveness of controls over this risk?
5 - Extremely effective
4 - Very effective
3 - Moderately effective
2 - Minimally effective
1 - Ineffective

[7] Assessment of risk level not taking current controls into consideration.

[8] Assessment of risk level taking current controls into account.