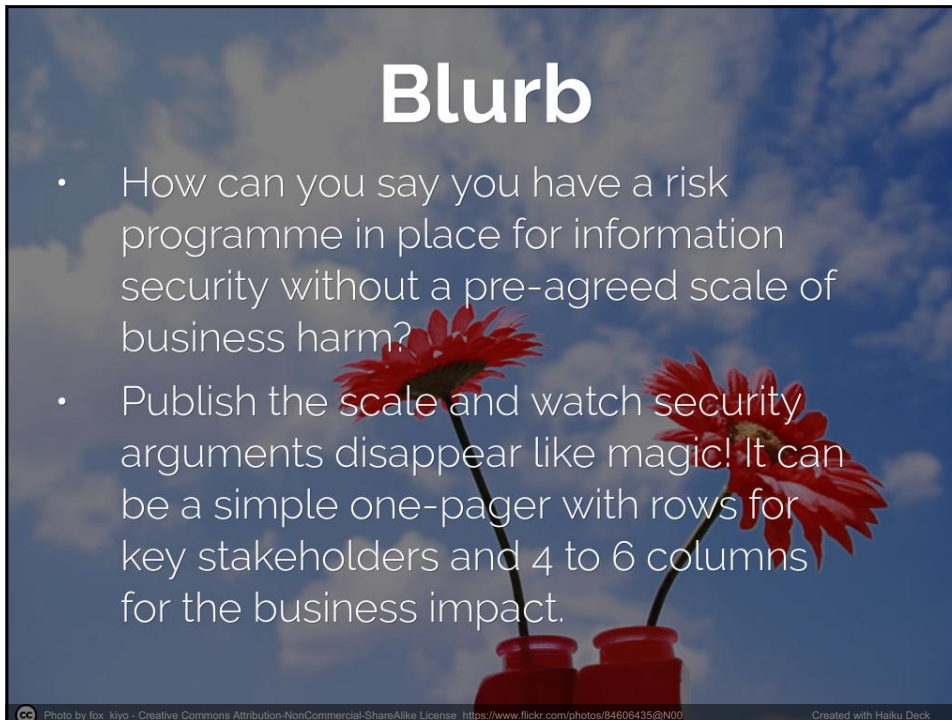




1



2

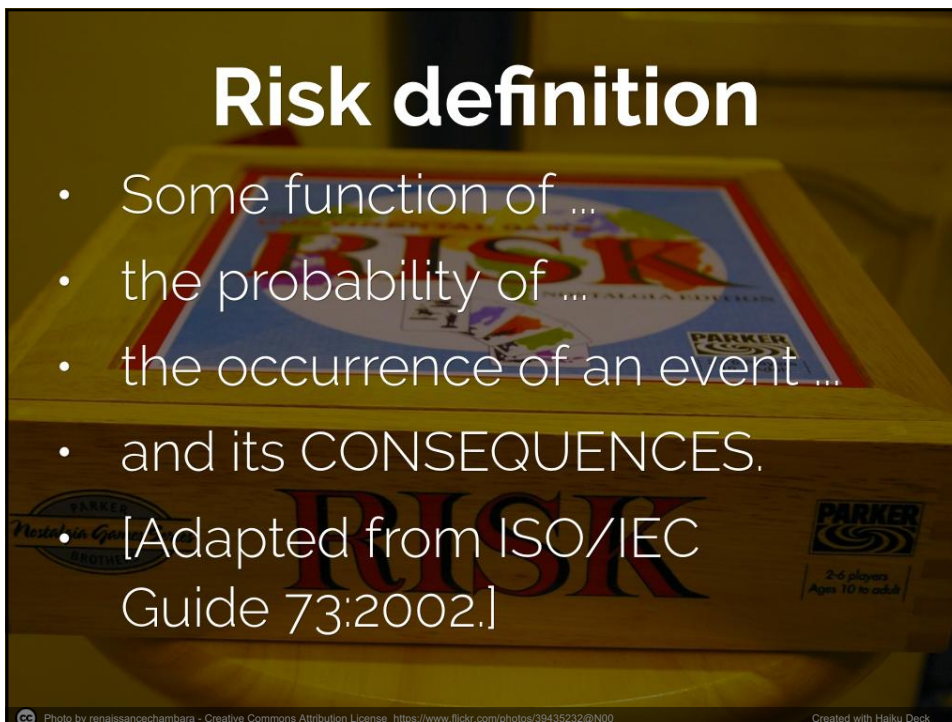


Blurb

- How can you say you have a risk programme in place for information security without a pre-agreed scale of business harm?
- Publish the scale and watch security arguments disappear like magic! It can be a simple one-pager with rows for key stakeholders and 4 to 6 columns for the business impact.

CC Photo by fox_kiyo - Creative Commons Attribution-NonCommercial-ShareAlike License https://www.flickr.com/photos/84606435@N00 Created with Haiku Deck

3



Risk definition

- Some function of ...
- the probability of ...
- the occurrence of an event ...
- and its CONSEQUENCES.

• [Adapted from ISO/IEC Guide 73:2002.]

CC Photo by renaissancechambara - Creative Commons Attribution License https://www.flickr.com/photos/39435232@N00 Created with Haiku Deck

4

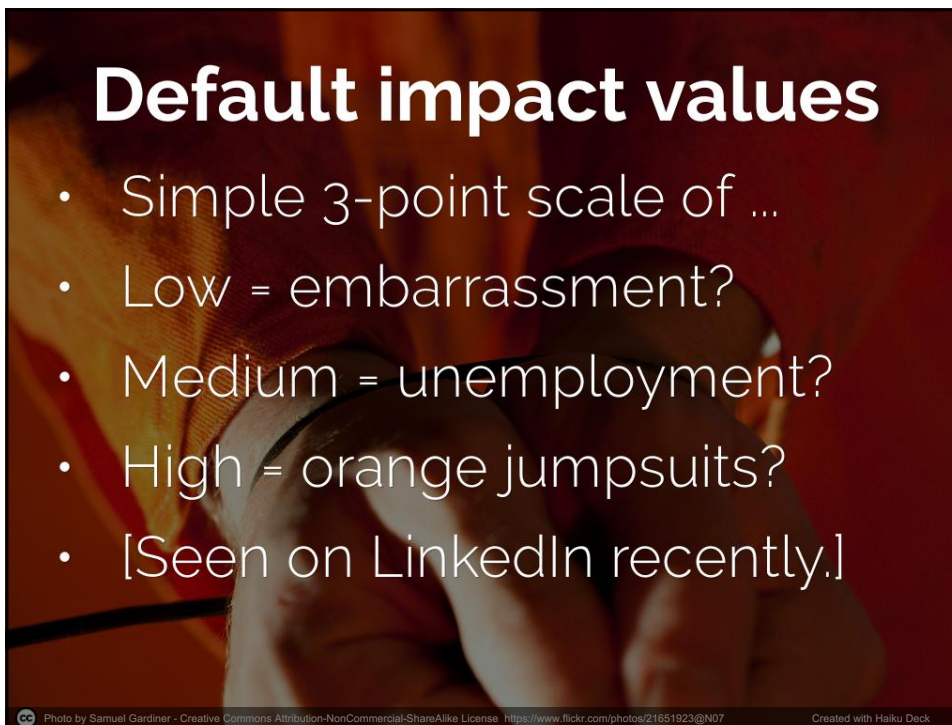


Consequences?

- Unwanted negative impacts
- Harm
- Losses

CC Photo by baryskeates - Creative Commons Attribution License <https://www.flickr.com/photos/31059504@N08> Created with Haiku Deck

5

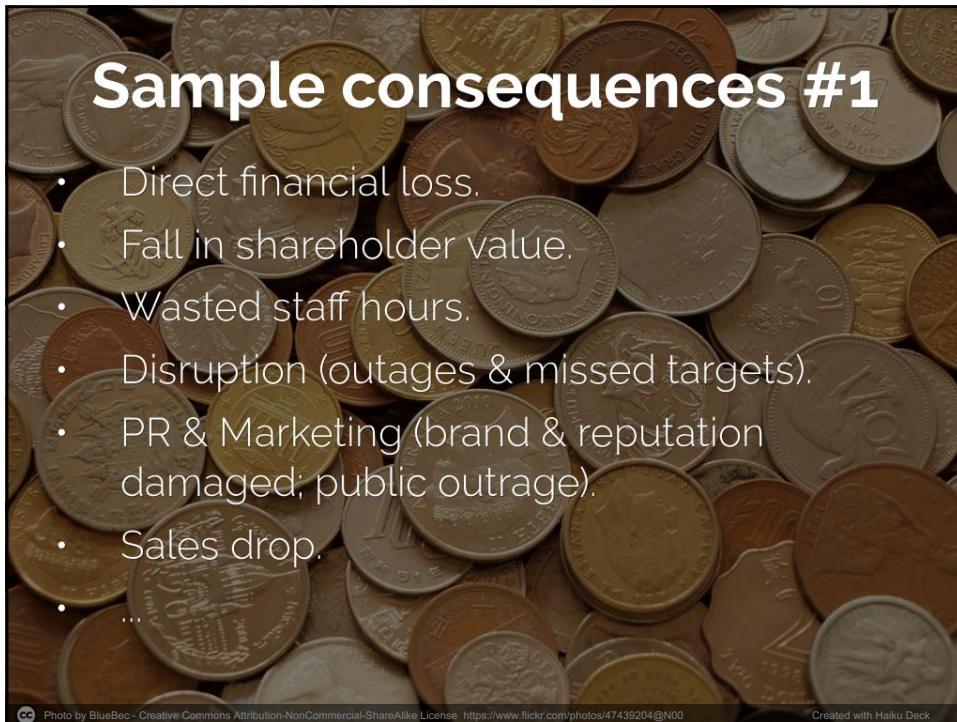


Default impact values

- Simple 3-point scale of ...
- Low = embarrassment?
- Medium = unemployment?
- High = orange jumpsuits?
- [Seen on LinkedIn recently.]

CC Photo by Samuel Gardiner - Creative Commons Attribution-NonCommercial-ShareAlike License <https://www.flickr.com/photos/21651923@N07> Created with Haiku Deck

6

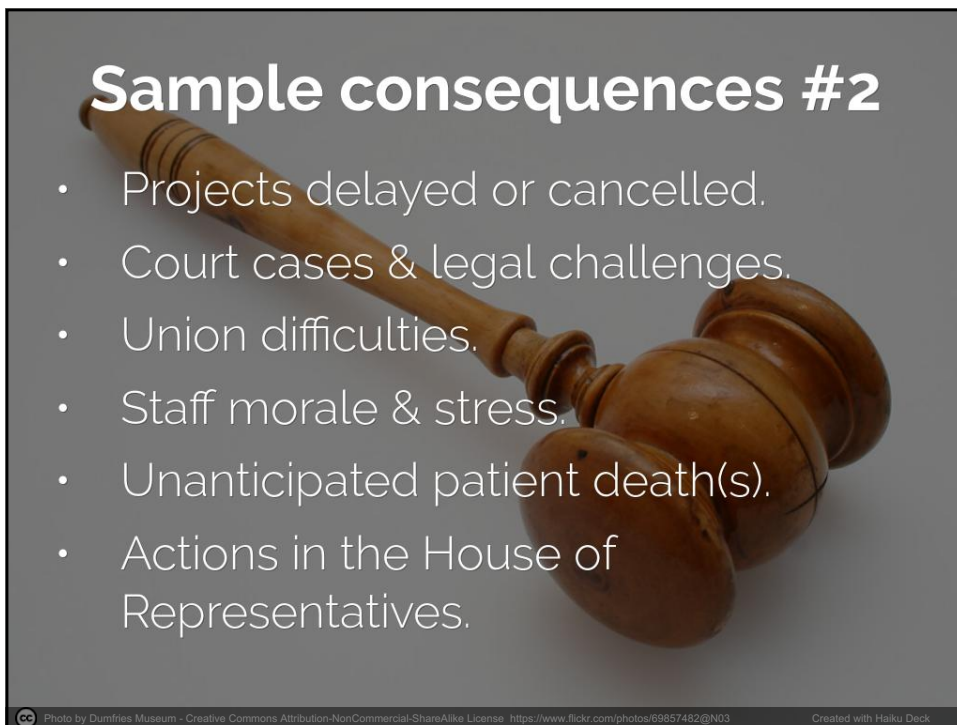


Sample consequences #1

- Direct financial loss.
- Fall in shareholder value.
- Wasted staff hours.
- Disruption (outages & missed targets).
- PR & Marketing (brand & reputation damaged; public outrage).
- Sales drop.
- ...

Photo by BlueBec - Creative Commons Attribution-NonCommercial-ShareAlike License. <https://www.flickr.com/photos/47439204@N00> Created with Haiku Deck

7

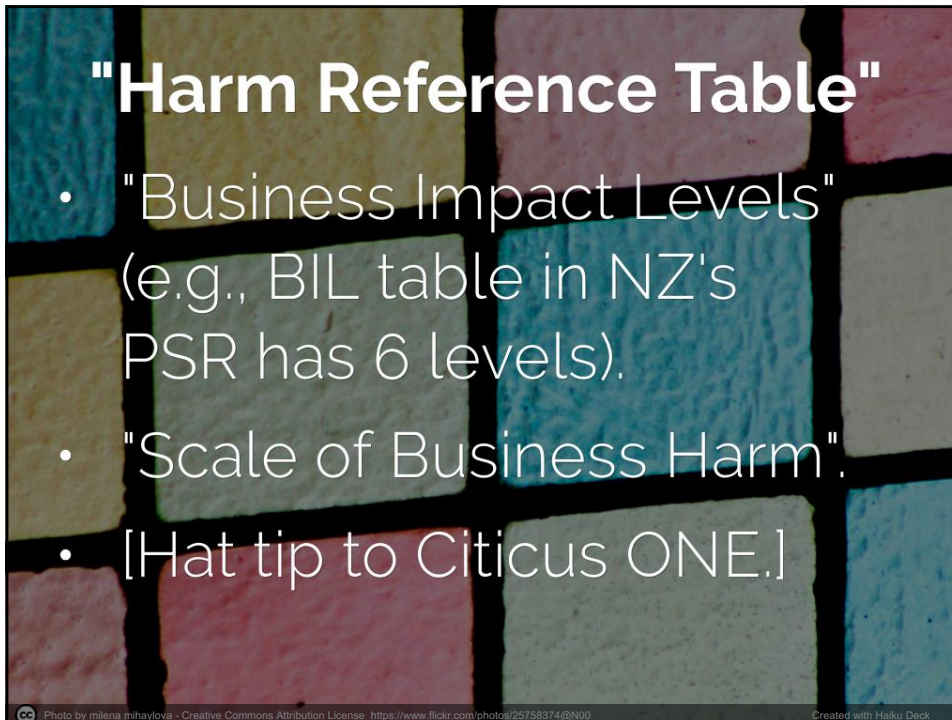


Sample consequences #2

- Projects delayed or cancelled.
- Court cases & legal challenges.
- Union difficulties.
- Staff morale & stress.
- Unanticipated patient death(s).
- Actions in the House of Representatives.

Photo by Dumfries Museum - Creative Commons Attribution-NonCommercial-ShareAlike License. <https://www.flickr.com/photos/69857482@N03> Created with Haiku Deck

8

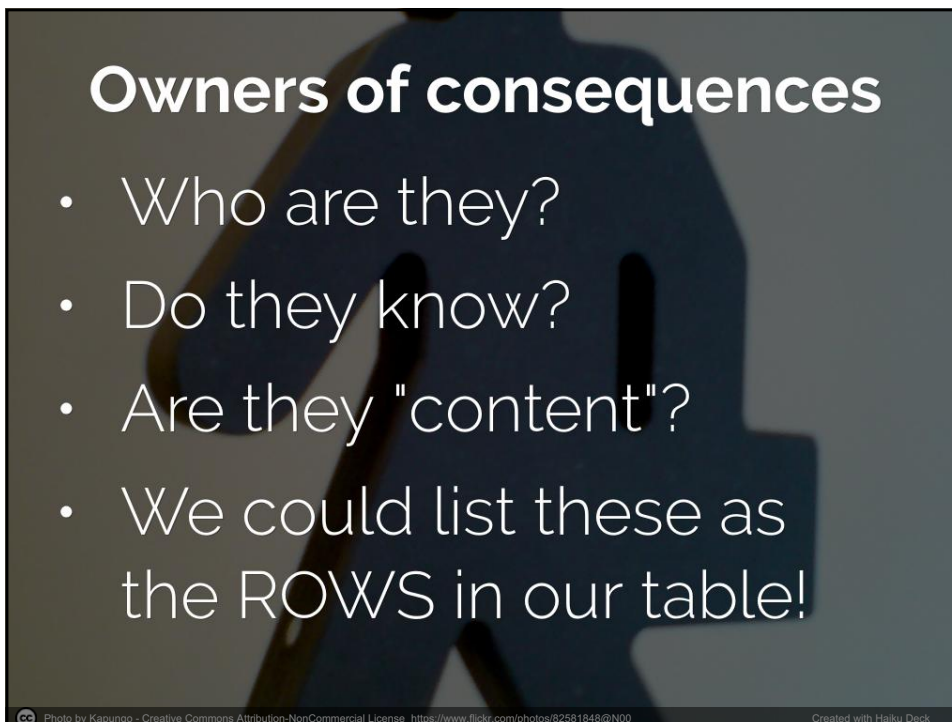


"Harm Reference Table"

- "Business Impact Levels" (e.g., BIL table in NZ's PSR has 6 levels).
- "Scale of Business Harm".
- [Hat tip to Citicorus ONE.]

Photo by milena mihaylova - Creative Commons Attribution License <https://www.flickr.com/photos/25758374@N00> Created with Haiku Deck

9



Owners of consequences

- Who are they?
- Do they know?
- Are they "content"?
- We could list these as the ROWS in our table!

Photo by Kapungo - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/82581848@N00> Created with Haiku Deck

10



Total Business Harm

- Primary Impacts (immediate harm).
- Secondary Impacts (longer-term harm to the business, over months or years).
- Total Business Harm = Primary + Secondary Impacts.
- We could rate these, using a 5-point scale, as the COLUMNS in our table!

11



OpenFAIR (quantitative)

1. Productivity loss.
2. Response costs.
3. Replacement costs.
4. Competitive advantage loss.
5. Fines & judgements.
6. Reputation damage.

12

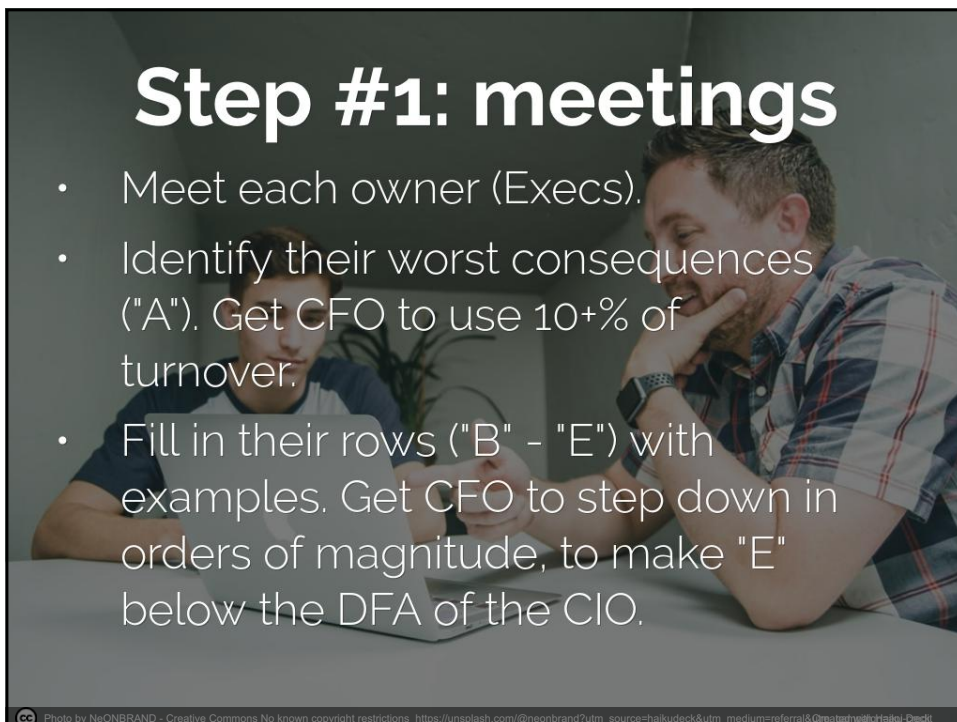


Scale (semi-quantitative)

- “A” ratings = worst-case impacts = human life, survival of the business.
- “B” & “C” ratings = major drop in sales due to damage to brand & reputation, or public outrage.
- “D” & “E” ratings = replacement equipment, overtime working, local news stories, inconvenience to customers or staff.

Photo by teachernz - Creative Commons Attribution-NonCommercial-ShareAlike License <https://www.flickr.com/photos/66893217@N00> Created with Haiku Deck

13



Step #1: meetings

- Meet each owner (Execs).
- Identify their worst consequences (“A”). Get CFO to use 10+% of turnover.
- Fill in their rows (“B” - “E”) with examples. Get CFO to step down in orders of magnitude, to make “E” below the DFA of the CIO.

Photo by NeONBRAND - Creative Commons No known copyright restrictions https://unsplash.com/@neonbrand?utm_source=haikudeck&utm_medium=referral&utm_campaign=haiku-deck

14

		LEVEL OF HARM				
NATURE OF HARM	MEASURE	A	B	C	D	E
		Extremely Serious Harm	Very Serious Harm	Serious Harm	Minor Harm	No Significant Harm
Financial Impact:	Direct financial loss	\$10+ million	\$1 - 10 million	\$100 thousand - \$1 million	\$10 - 100 thousand	\$0 - 10 thousand

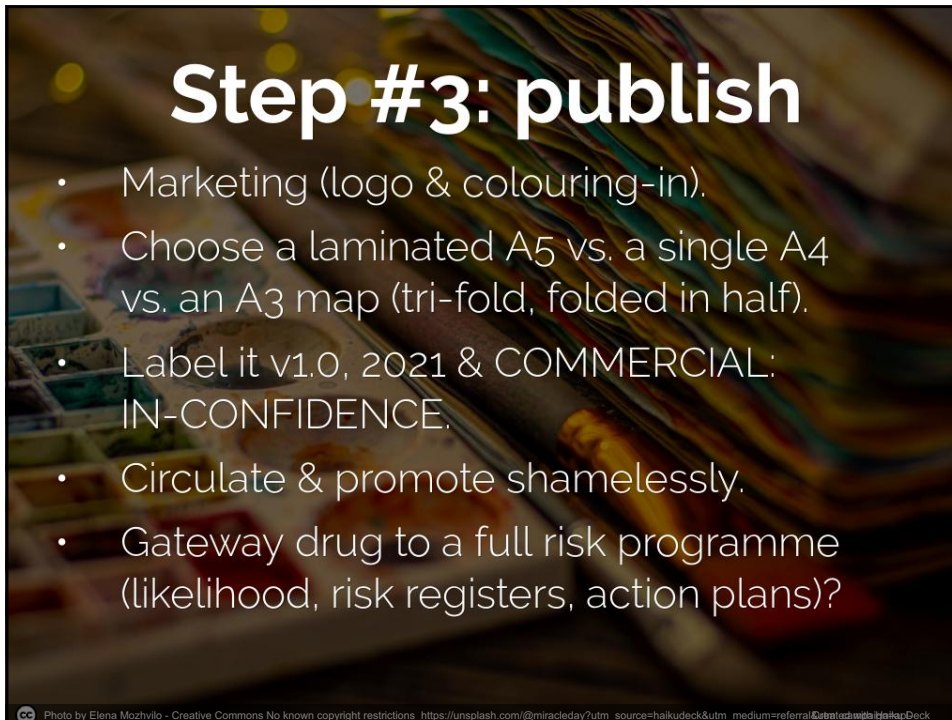
15

Step #2: workshop

- Align all 5 columns, "A" - "E".
- Give priority to Finance.
- Might need to use interim columns for "A+" or "F".
- Rework examples to fit.
- Sign-off (Execs).

Photo by Kelly Sikkema - Creative Commons No known copyright restrictions https://unsplash.com/@kellysikkema?utm_source=haikudeck&utm_medium=referral&utm_campaign=haikudeck

16

A slide titled "Step #3: publish" with a background image of a paint palette and brushes. The text is white and bold. Below the title is a bulleted list of five items. At the bottom left is a Creative Commons license icon and text. At the bottom right is the text "Created with Haiku Deck".

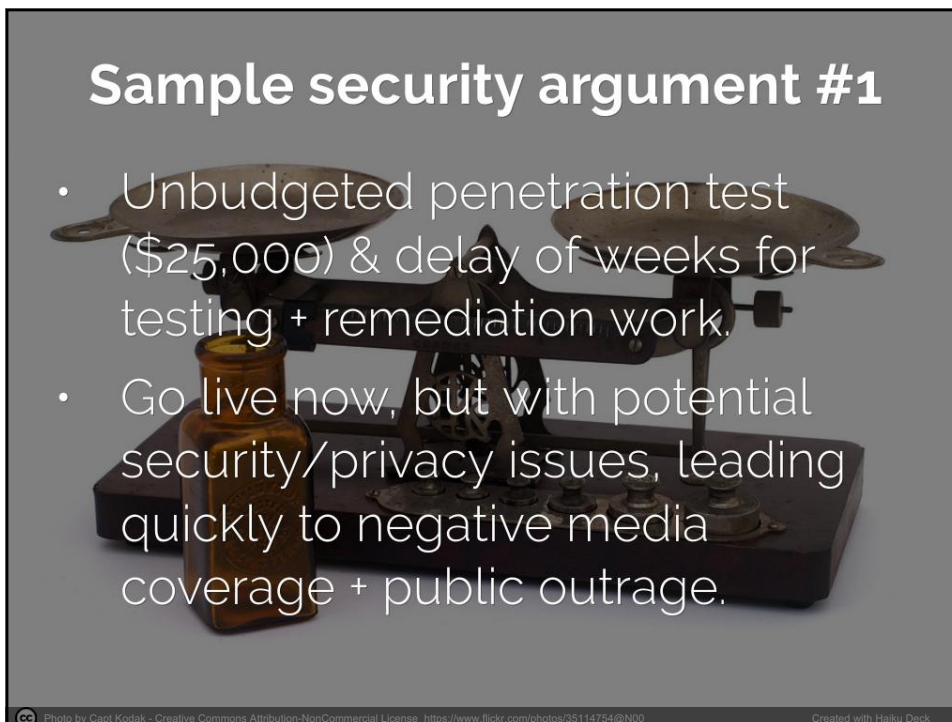
Step #3: publish

- Marketing (logo & colouring-in).
- Choose a laminated A5 vs. a single A4 vs. an A3 map (tri-fold, folded in half).
- Label it v1.0, 2021 & COMMERCIAL: IN-CONFIDENCE.
- Circulate & promote shamelessly.
- Gateway drug to a full risk programme (likelihood, risk registers, action plans)?

CC Photo by Elena Mozvilo - Creative Commons No known copyright restrictions https://unsplash.com/@miracleday?utm_source=haikudeck&utm_medium=referral&utm_campaign=haikudeck

Created with Haiku Deck

17

A slide titled "Sample security argument #1" with a background image of a balance scale and a glass bottle. The text is white and bold. Below the title is a bulleted list of two items. At the bottom left is a Creative Commons license icon and text. At the bottom right is the text "Created with Haiku Deck".

Sample security argument #1

- Unbudgeted penetration test (\$25,000) & delay of weeks for testing + remediation work.
- Go live now, but with potential security/privacy issues, leading quickly to negative media coverage + public outrage.

CC Photo by Capt Kodak - Creative Commons Attribution-NonCommercial License <https://www.flickr.com/photos/35114754@N00>

Created with Haiku Deck

18

		LEVEL OF HARM				
NATURE OF HARM	MEASURE	A Extremely Serious Harm	B Very Serious Harm	C Serious Harm	D Minor Harm	E No Significant Harm
Financial Impact:	Direct financial loss	\$10+ million	\$1 - 10 million	\$100 thousand - \$1 million	\$10 - 100 thousand	\$0 - 10 thousand
Operational Impact:	Disruption to significant project or new initiative	Project cancelled	Project scope reduced significantly	Project delayed by months	Project delayed by weeks	Project delayed by days
	Staff hours wasted	5000+ hours wasted	1000-5000 hours wasted	200-1000 hours wasted	40-200 hours wasted	5-40 hours wasted
Brand & Reputation:	Negative publicity	Featured on Fair Go; long-running news story; case study	Featured on TVNZ news; front page of the NZ Herald	Social media campaign; local news stories		
	Privacy Act 2020	Class Action	Compliance Notice	Increased IPP 6/7 requests		

19

Sample security argument #2

- Make developers work late into the night to fix/test /release this marketing change?
- Start promptly tomorrow morning to release before lunchtime?

Photo by Mauro Caleb - Creative Commons Attribution License <https://www.flickr.com/photos/69102917@N06>
Created with Haiku Deck

20

		LEVEL OF HARM				
NATURE OF HARM	MEASURE	A	B	C	D	E
		Extremely Serious Harm	Very Serious Harm	Serious Harm	Minor Harm	No Significant Harm
Financial Impact:	Direct financial loss	\$10+ million	\$1 - 10 million	\$100 thousand - \$1 million	\$10 - 100 thousand	\$0 - 10 thousand
	Disruption to significant project or new initiative	Project cancelled	Project scope reduced significantly	Project delayed by months	Project delayed by weeks	Project delayed by days
Operational Impact:	Staff hours wasted	5000+ hours wasted	1000-5000 hours wasted	200-1000 hours wasted	40-200 hours wasted	5-40 hours wasted
	Negative publicity	Featured on Fair Go; long-running news story; case study	Featured on TVNZ news; front page of the NZ Herald	Social media campaign; local news stories		
Brand & Reputation:	Privacy Act 2020	Class Action	Compliance Notice	Increased IPP 6/7 requests		

21

Your questions & comments?



s.coates@aurainfosec.com

Photo by Stefan Baudy - Creative Commons Attribution License https://www.flickr.com/photos/92454606@N00 Created with Haiku Deck

22