eHealth NSW

Taking a holistic approach when balancing cyber security risks in healthcare

Presenter:
Dr Peter Croll
Chief Security Information Officer (CISO)
NSW Health, Australia

NSW GOVERNMENT

eHealth NSW

NSW GOVERNMENT

Assumptions

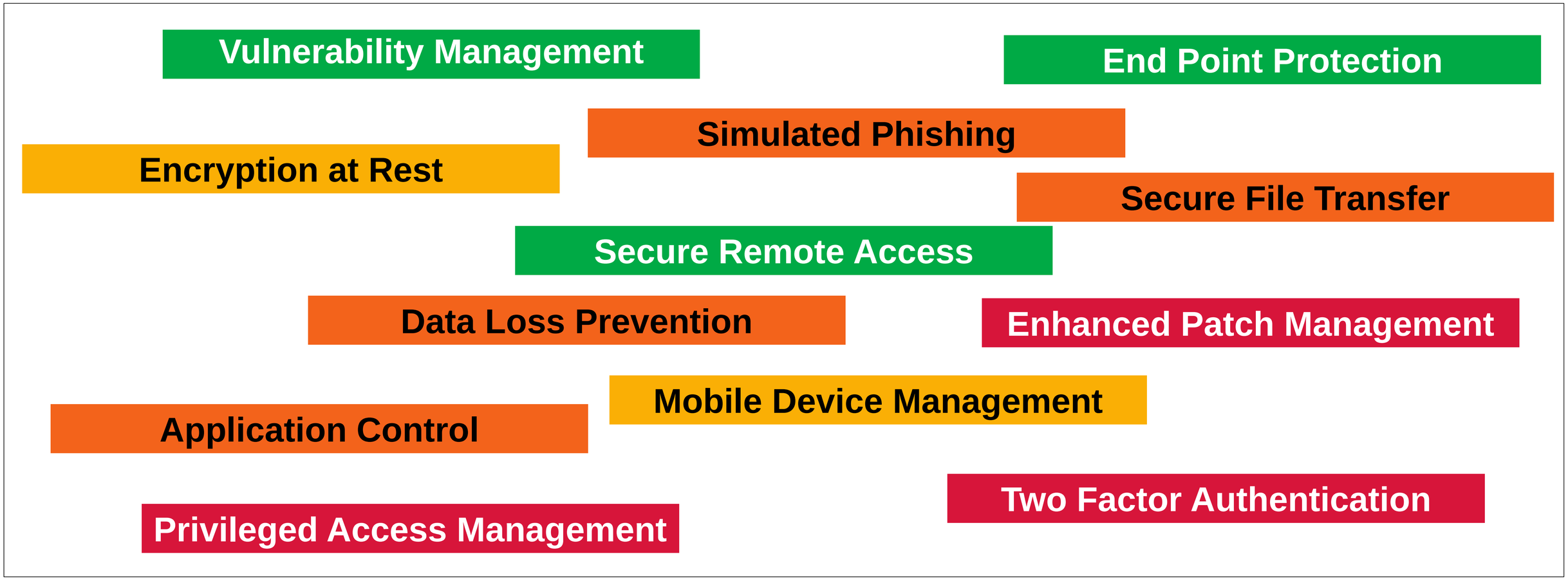
Your cyber security posture is not fully optimised

Your cyber security capability operates within a limited budget

Your organisation has special needs and expectations

Risk-based approach to meet priorities

Consider some mitigations



NOTE: these are just examples and do not represent the priorities or status of NSW Health

Prioritised by risk

- Enhanced Patch Management
- Privileged Access Management
- Two Factor Authentication
- Simulated Phishing
- Data Loss Prevention
- Application Control
- Mobile Device Management
- Encryption at Rest
- End Point Protection
- Vulnerability Management
- Secure Remote Access

Applying the risk matrix for the organisation

Likelihood Rating	Consequence Rating: Catastrophic	Major	Moderate	Minor	Minimal
Almost certain	A	D	J	P	S
Likely	B	E	K	Q	T
Possible	C	H	M	R	W
Unlikely	F	I	N	U	X
Rare	G	L	O	V	Y

Risk matrix key: Extreme (A – E) | High (F – K) | Medium (L – T) | Low (U – Y)

Can and should these be done in sequence?

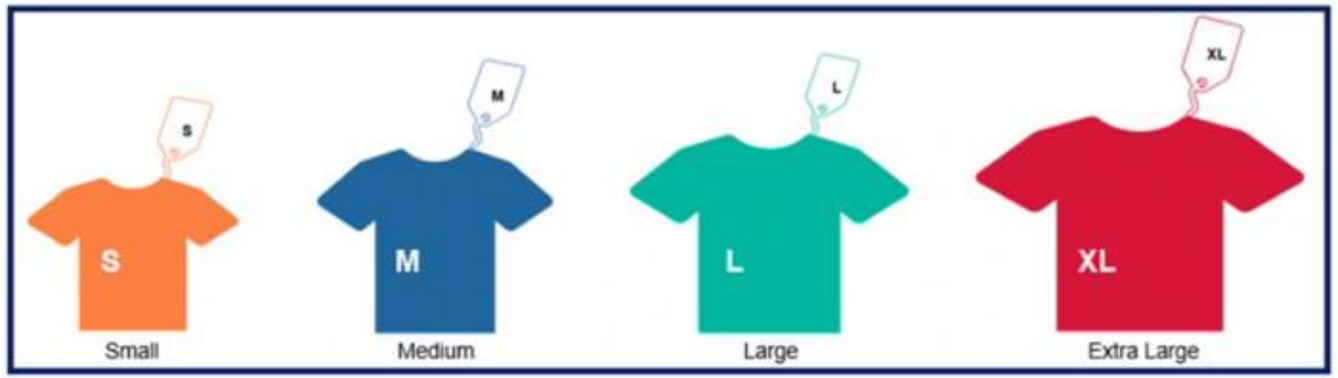
Scale – Effort – Complexity

Apply ‘T-Shirt’ sizing

- Enhanced Patch Management (M)
- Privileged Access Management (L)
- Two Factor Authentication (M)
- Simulated Phishing (S)
- Data Loss Prevention (L)
- Application Control (XL)
- Mobile Device Management (S)
- Encryption at Rest (M)
- End Point Protection (L)
- Vulnerability Management (XL)
- Secure Remote Access (M)

T-Shirt Size is used to assess Scale/Effort/Complexity

eHealth NSW uses 5 criterion to determine the amount of work/effort/complexity in front of them.



Size	Dependencies	Complexity	Duration	Effort	Governance*
Small	0	Existing applications / services	<3 Months	<479 Hours	Internal Stakeholder
Medium	1 - 2	Some existing applications / services. Request partially understood.	3 - 9 Months	480 – 1399 Hours	Design Working Group
Large	3+	No existing applications / services. Request not well understood.	+9 months	1400+ Hours	Whole Group Governance
Extra Large	Whole Group Governance*				
XXL	Whole Group Governance*				

Ranking by risk and complexity

- [2] Simulated Phishing (S)
- [3] Enhanced Patch Management (M)
- [3] Two Factor Authentication (M)
- [5] Mobile Device Management (S)
- [6] Privileged Access Management (L)
- [7] Data Loss Prevention (L)
- [8] Encryption at Rest (M)
- [10] Application Control (XL)
- [13] Secure Remote Access (M)
- [15] End Point Protection (L)
- [16] Vulnerability Management (XL)

	Risk	Ex	Hi	Med	Lo
Size	Weighting	1	2	5	9
S	0	1	2	5	9
M	2	3	4	7	11
L	5	6	7	10	14
XL	7	8	9	12	16

Ranking	Risk/Size	Weighting
1	Ex S	1
2	Hi S	2
3	Ex M	3
4	Hi M	4
5	Med S	5
6	Ex L	6
7	Hi L	7
8	Med M	7
9	Ex XL	8
10	Hi XL	9
11	Lo S	9
12	Med L	10
13	Low M	11
14	Med XL	12
15	Low L	14
16	Low XL	16

Cyber SHARP

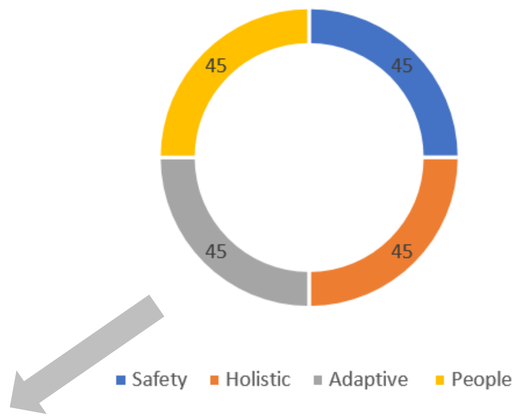
- **Safety:** at the core for digital healthcare solutions where harm can manifest in many ways
- **Holistic approach:** ensuring broad-range analysis capturing weak links
- **Adaptive:** since the cyber adversary and threats are in a state of constant change (simply being agile is not enough without building in risk-based continuous improvement)
- **Risk-based:** recognises that not everything can be covered with finite resources and should form the basis for continuing prioritisation
- **People-centric:** over process and technology to ensure usable, acceptable solutions

Your organisation has special needs and expectations

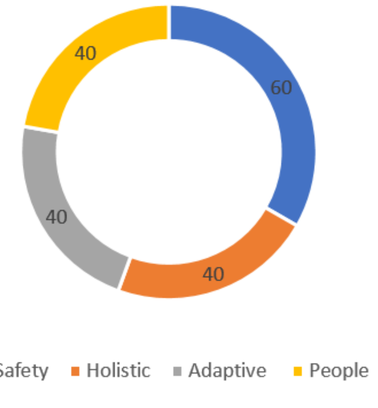
Balance those needs – organisational profile

Industry	Profile	Safety	Holistic	Adaptive	People
Healthcare (General)	An environment where safety is paramount, and quality is highly dependent on the people	60	30	30	60
Healthcare public hospital	As above plus a wide range of services	50	50	30	50
Technology startup	Needs to move with the market and will take some risks seeking new opportunities	30	60	60	30
Education	Very people oriented, needs to stay market focused, has a wide range of has many safety considerations.	45	45	45	45
Finance	Subject to fluctuations outside of their control, risk adverse, often focused, relies on customers	50	30	50	50
Transport	Safety is critical and measured, can be focused, relies on people, change is not rapid	60	30	30	60
Utilities	Safety is critical, very focused, change is not rapid, more technology than people focused	45	45	45	45

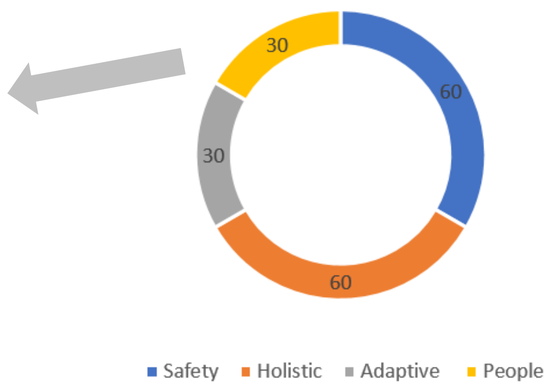
Balanced Criteria



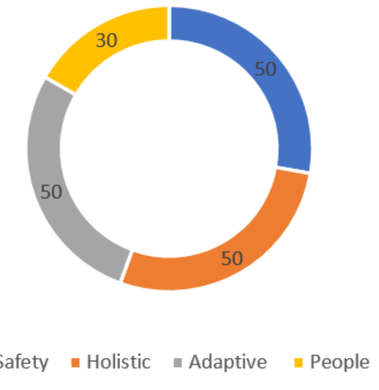
1 Priority Criteria



2 Priority Criteria



3 Priority Criteria



Apply to rolling roadmap

ROLLING ROADMAP FOR: Cyber Enhancements UPDATED 01-Jul-23 QRT 3

	This Month			Next Quarter	Following Quarter	
THEME	Jul	Aug	Sep	QTR 4	QTR 1 Next Year	FUTURE
Plan Simulated Phishing	Outline objectives, learning outcomes and targets	Check staff availability and timing			Leasons learnt for next event	Add more Cyber Awareness modules
Run Simulated Phishing exercise		Customise templates, Launch campaign	Monitor, track responses	Analyse, reporting		

SCORE CARD FOR: Cyber Enhancements UPDATED 01-Jul-23

THEME	Target	Score	CARRY OVER	QRT 1	QTR 2	QRT 3	QTR 4
SAFETY	60	60	Sim Phish (15)	Two Factor (20)	DLP (10)	Encryp Rest (10)	PAM (5)
HOLISTIC	30	50	Two Factor (10)	MDM (10)	DLP (15)	Encryp Rest (5)	Patch Man (10)
ADAPTIVE	30	25	MDM (5)	MDM (5)	DLP (5)	Encryp Rest (5)	PAM (5)
PEOPLE	60	40	Sim Phish (10)	Two Factor (5)	DLP (10)	PAM (15)	

Enter on score card

Conclusions

- Prioritising cyber security enhancements with limited budgets requires a ‘multi-staged’ risk-based approach
- Risk mitigations have to be prioritised against scale, effort and complexity to implement
- This can be achieved through use of a weighted ranking matrix
- The Cyber SHARP model ensures a focus is applied to meet the special needs and expectations of health organisations
- The key criteria are SAFETY, HOLISTIC, ADAPTIVE, RISK-BASED and PEOPLE-CENTRIC
- Keeping score against these criteria ensures the risk mitigations are appropriately applied
- This approach highlights what’s most important in healthcare and avoids being driven by technology and process.

Thank you

Dr Peter Croll, Chief Information Security Officer, NSW Health, peter.croll@health.nsw.gov.au