RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **RMG-R09V**

How to Tell the Right Cyber Story to Executives and Board Members

Ian Yip

Chief Executive Officer
Avertro
@ianyip

Context

I have had over 100 conversations on this topic to learn about what good looks like and delivered countless engagements for organisations to address this issue.

These insights come from the discussions and resulting lessons.

I have not used production data points in the following sections and avoided the use of graphics that could compromise the anonymity of those involved.


“It (the NotPetya cyber incident) cost us between $250 to $300 million. It is time to stop being naive when it comes to cybersecurity.”
Jim Hagemann Snabe
Chairman, A.P. Moller Maersk


100% of enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually by 2020.
–Gartner-
But there is a communication disconnect between the cyber team and everyone else, particularly at the executive layer

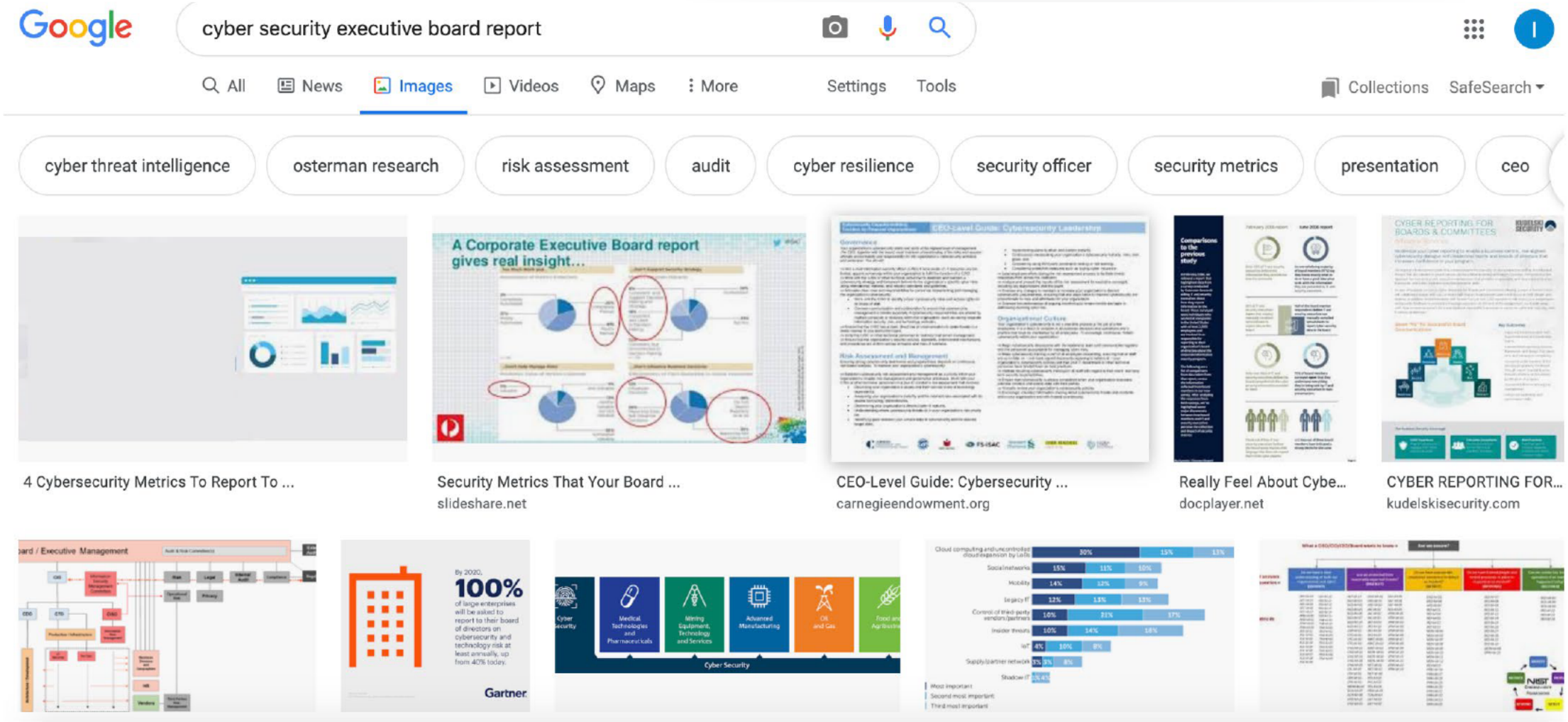
RSAConference2020 APJ

A Virtual Learning Experience

Cybersecurity Today

A Different Language

How do we do better when it's not easy to find examples?



Some common security KPIs: these are too technical

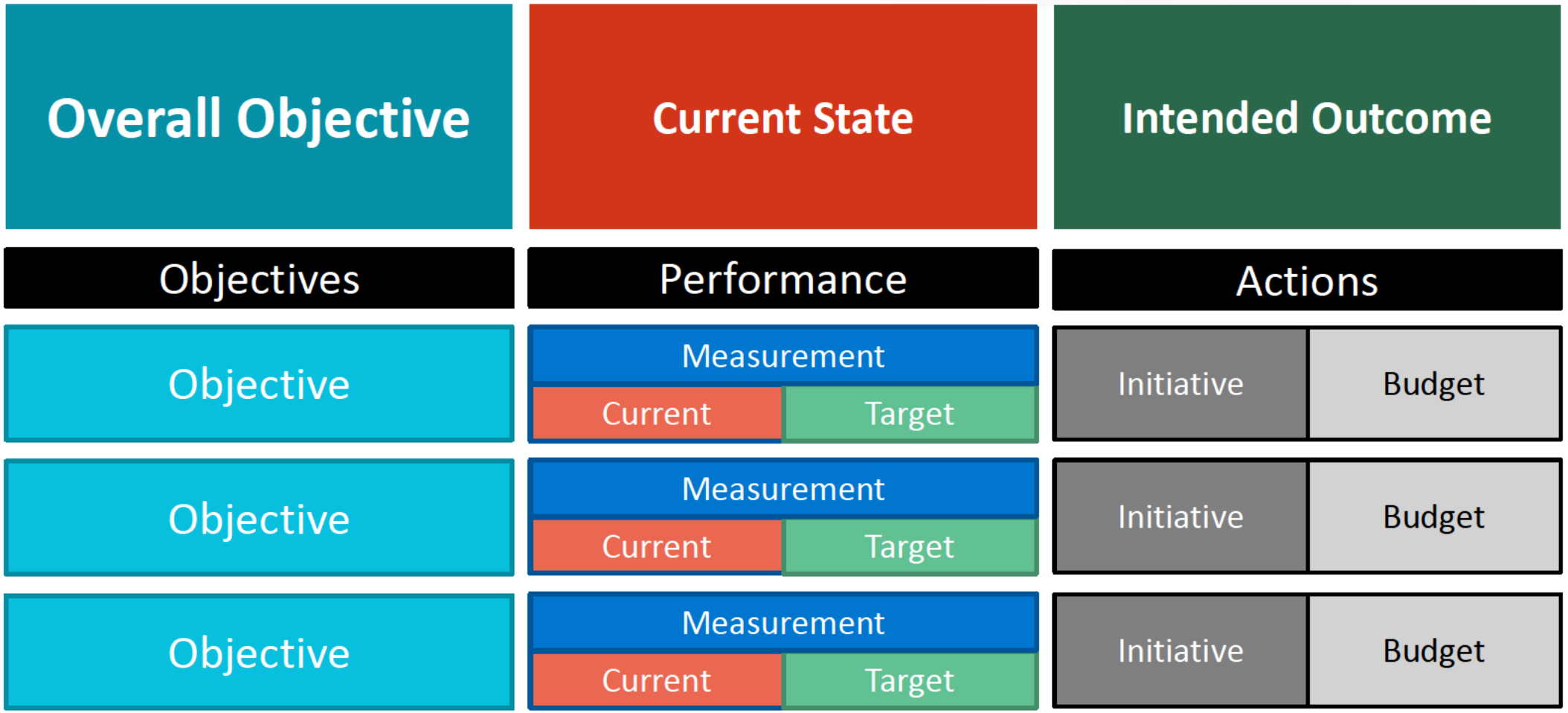
- Intrusion Attempts
- Number of Security Events and Alerts
- Number of Vulnerabilities Found
- Mean Time to Detect (MTTD)
- Mean Time to Resolve (MTTR)
- Mean Time to Contain (MTTC)
- Patching Cadence
- Vendor Risk

RSAConference2020 APJ
A Virtual Learning Experience

What Executives and Boards are Used to

Balanced Scorecards

Balanced scorecard



Balanced scorecard example

Increase Customer Retention	Current	Target
	50% customer retention ▲ **$1,000** customer lifetime value ▲	**80%** customer retention **$2,000** customer lifetime value

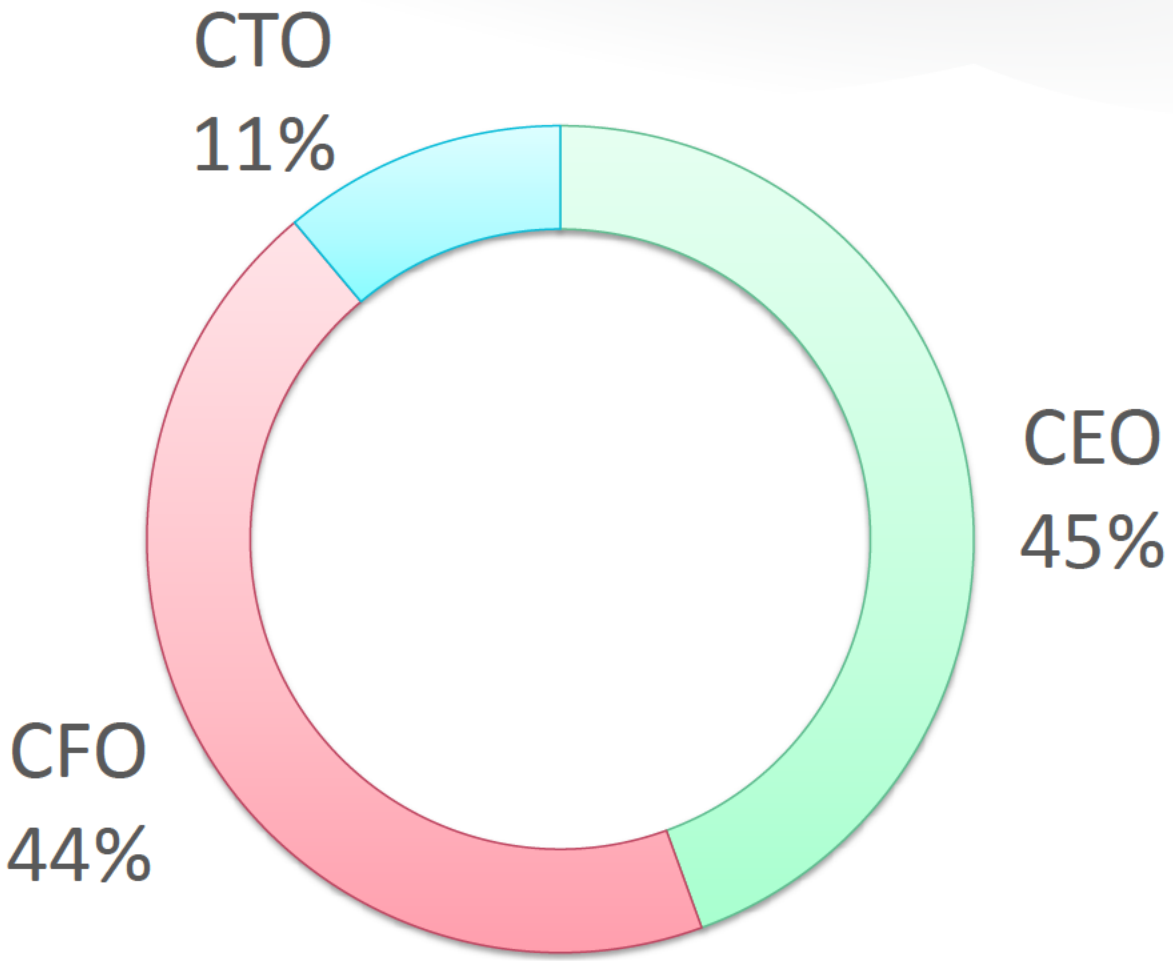
Objectives	Performance		Actions	
Improve customer experience ●	Average user session duration		UX refresh ●	$150,000
	5 minutes ▲	Target: 15 minutes		
Increase customer satisfaction ●	Customer satisfaction rating		Customer success program ●	$200,000
	2 stars ▲	Target: 4 stars		
Improve product quality ●	Average support calls per week		QA process improvement ●	$100,000
	250 ▲	Target: 50		

RSAConference2020 APJ
A Virtual Learning Experience

What Executives and Boards Want in Your Cyber Story

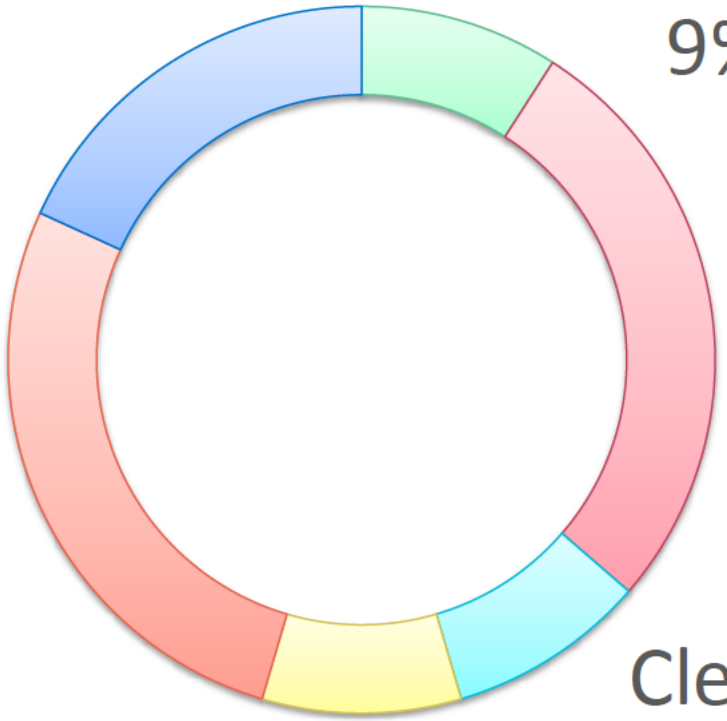
Understanding Their Language

Which C-level executives are least concerned about cyber risk?



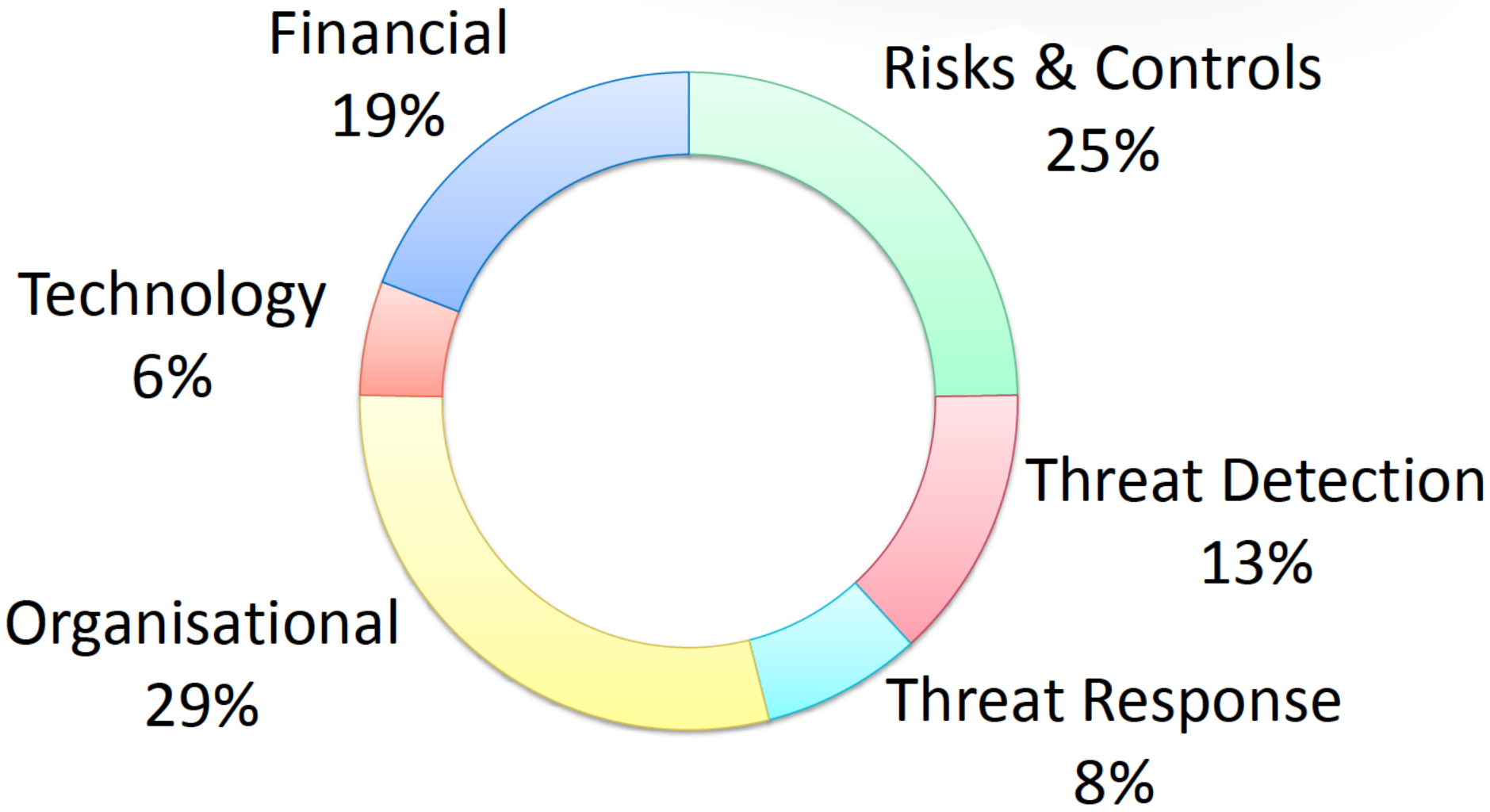
Source: McAfee Cyber Responsibility study 2018

What are the main reasons for this?



Source: McAfee Cyber Responsibility study 2018

Important metrics for the C-level and board



Source: McAfee Cyber Responsibility study 2018

Most important factors in improving understanding of cyber risk at the C-level and board

1. Being able to articulate threats and impacts in plain language
2. Keeping things brief and targeted
3. Being able to articulate the financial impacts and costs
4. Providing an independent view

Source: McAfee Cyber Responsibility study 2018

Things executives and board members needs answers to

Why and What

- Why do we care about cyber risk?
- What are our key assets?
- What are our cyber risks?
- What are our cyber capabilities?
- What are our goals and desired outcomes?
- What are the gaps?

How and When

- How are we measuring cyber?
- How are we currently doing and is it enough?
- How are we going to close our gaps?
- How do we know we are spending the right amount?
- How will we know when we get there?
- When will we get there?

RSAConference2020 APJ
A Virtual Learning Experience

What Executives and Boards are Being Told

Executive and Board Cyber Education

AICD Cyber for Directors Course

What can you expect?

Over the course of the day, you will undertake interactive working sessions facilitated by a director experienced in the challenges of cyber.

CLOSE

The Cyber for Directors course is a one-day session covering:

- Cyber Governance for Directors
- Cyber Risk for Directors
- Cyber Strategy and Innovation for Directors

Source: https://aicd.companydirectors.com.au/education/courses-for-the-director/short-courses/cyber-for-directors

AICD Cyber for Directors Course

What will you learn?

Participants will gain an understanding of the key terms and concepts of the cyber landscape, the fundamental roles and responsibilities of the board as they relate to cyber and learn tools for managing cyber risks and opportunities.

CLOSE

Upon completion of the Cyber for Directors program, you will be able to:

- understand key terms and concepts of the cyber landscape;
- outline the roles and responsibilities of the board in cyber governance, enabling you to discharge your duties through effective governance methods;
- identify cyber risks, threats and opportunities ensuring the organisation is prepared; and
- direct your organisation's cyber strategy, balancing cyber threats with innovation.

Source: https://aicd.companydirectors.com.au/education/courses-for-the-director/short-courses/cyber-for-directors

National Association of Corporate Directors Guidance

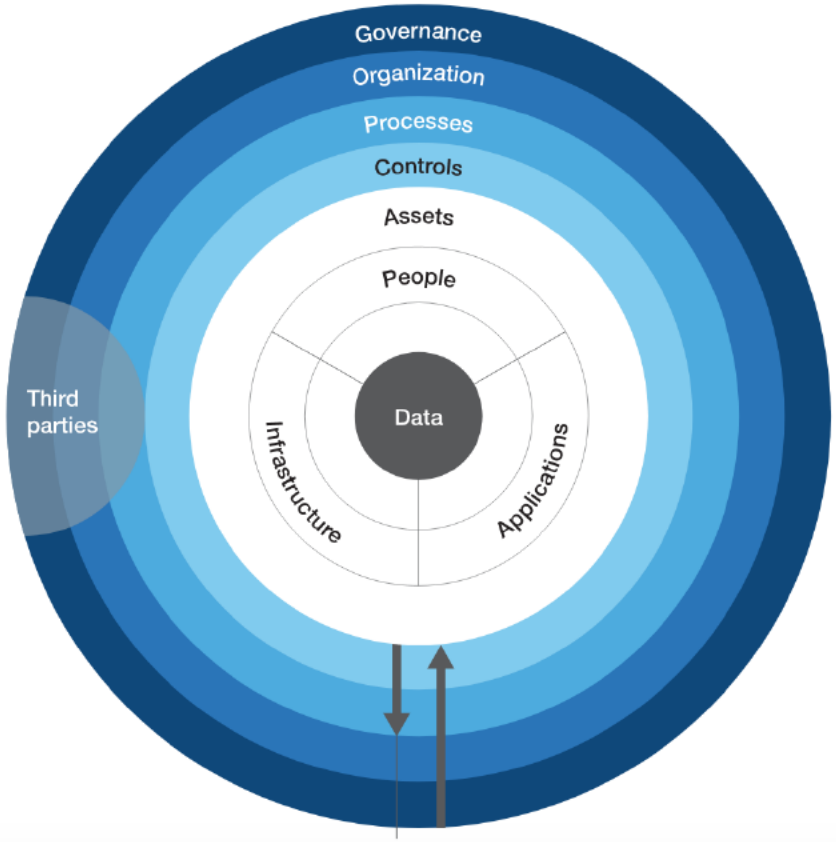
Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
IT Risk Management	IT risks are not identified	M	9	5	▲
	IT risks are not managed to acceptable levels	M	5	6	▲
Physical & Environmental Security	Physical perimeter controls at information processing facilities are not established	L	14	4	■
	Plans and operational controls to support power contingency mechanisms are not defined	M	3	13	▲
Organization Security and Awareness	Users do not perform their security responsibilities	M	5	1	■
	Users do not understand their security responsibilities	H	30	11	▼

Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
Information Security Program Management	The information security program is not aligned with business requirements	M	3	13	▲
	Policies and procedures have not been established for information security	L	2	11	■
Third Party Security	Security risks are not identified with third-parties	H	1	18	▲
	Security risks are not managed to acceptable levels with third-parties	M	4	13	▲
IT Operations	Information security practices are not integrated into IT operations	L	5	2	■
	IT operations are not performing their information security responsibilities	M	7	4	■

ILLUSTRATIVE

The holistic approach, according to a consulting firm

Holistic cyber risk–management approach



Assets. Clearly defined critical assets

Controls. Differentiated controls to balance security with agility

Processes. State-of-the-art cybersecurity processes focused on effective responses

Organization. Right skills, efficient decision making, and effective enterprise-wide cooperation

Governance. Investments in operational resilience prioritized based on deep transparency into cyber risks

Third parties. Coverage of the whole value chain, including third-party services

Source: https://www.mckinsey.com/business-functions/risk/our-insights/cyber-risk-measurement-and-the-holistic-cybersecurity-approach

RSAConference2020 APJ
A Virtual Learning Experience

The Right Cyber Story

Setting Yourself Up for Success

Goals

- Align the board and executives with the cyber mission to ensure its success
- Illuminate the strategic value of a cost centre by bringing business concepts to the cyber discussion
- Prove you are doing cybersecurity right

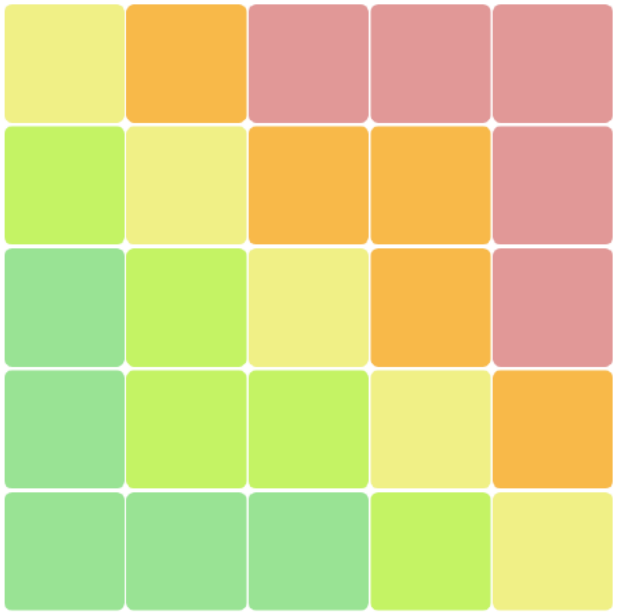
Elevate your cyber game

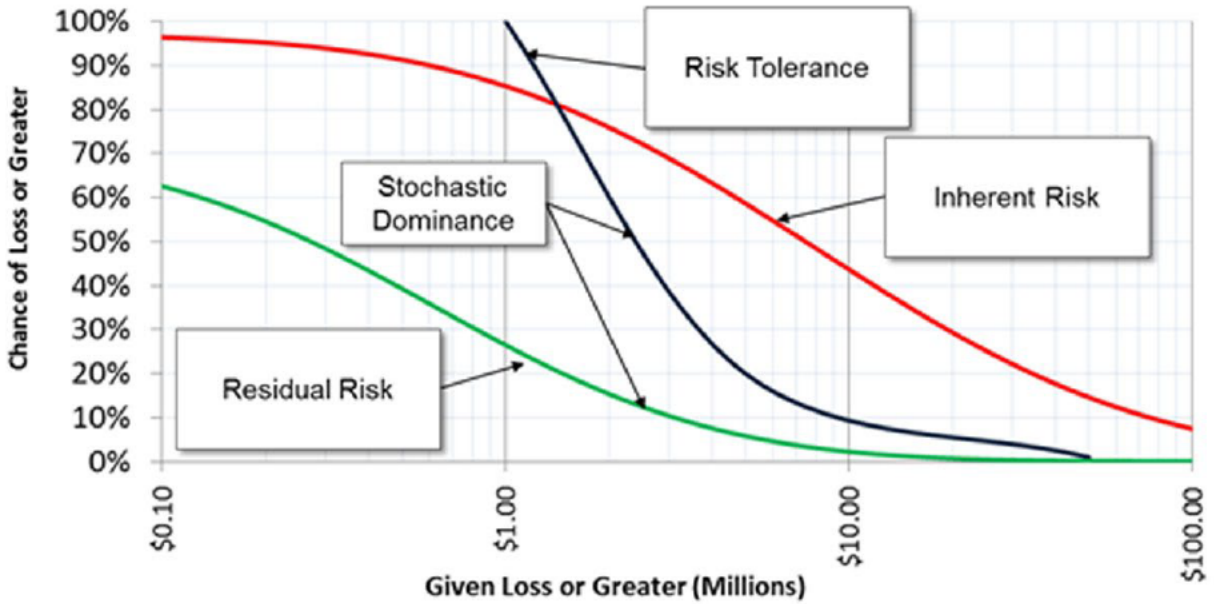
- Answer the “why” and “so what” questions
- Explain everything to stakeholders in plain language
- Avoid detail unless it adds to the story
- Forecast your cyber journey
- Justify and right-size spend
- Validate your strategy

Make the team the heroes in the story

- CISO: Strategic alignment with the business
- Governance & Risk: Continuous risk visibility
- Procurement: Better third-party risk management
- SecOps: Appreciated for being cyber ninjas

The language of the c-suite and board is risk





Source: How to Measure Anything in Cybersecurity Risk – Hubbard & Seiersen

Cyber risks at the executive level are not technical

There are 500 vulnerabilities in our cloud infrastructure that need to be addressed.

Is this a business or technical risk?

Cyber risks at the executive level are not technical

Our fleet of servers in the data centre have not been patched for 3 months.

Is this a business or technical risk?

Always ask: “so what?”

- There are 500 vulnerabilities in our cloud infrastructure that need to be addressed.
  - So what? Answer: This technical risk increases the following business risk.
    - Exfiltration of sensitive data stored in our cloud resulting in regulatory fines.
- Our fleet of servers in the data centre have not been patched for 3 months.
  - So what? Answer: This technical risk increases the following business risk.
    - System unavailability as a result of a malicious cyber attack resulting in the inability to process customer financial transactions.

Executives and board members only care about the business risks

- **Data Breach Risk:** Exfiltration of sensitive data stored in our cloud resulting in regulatory fines.
- **System Availability Risk:** System unavailability as a result of a malicious cyber attack resulting in the inability to process customer financial transactions.

NOT

- There are 500 vulnerabilities in our cloud infrastructure that need to be addressed.
- Our fleet of servers in the data centre have not been patched for 3 months.

RSAConference2020 APJ

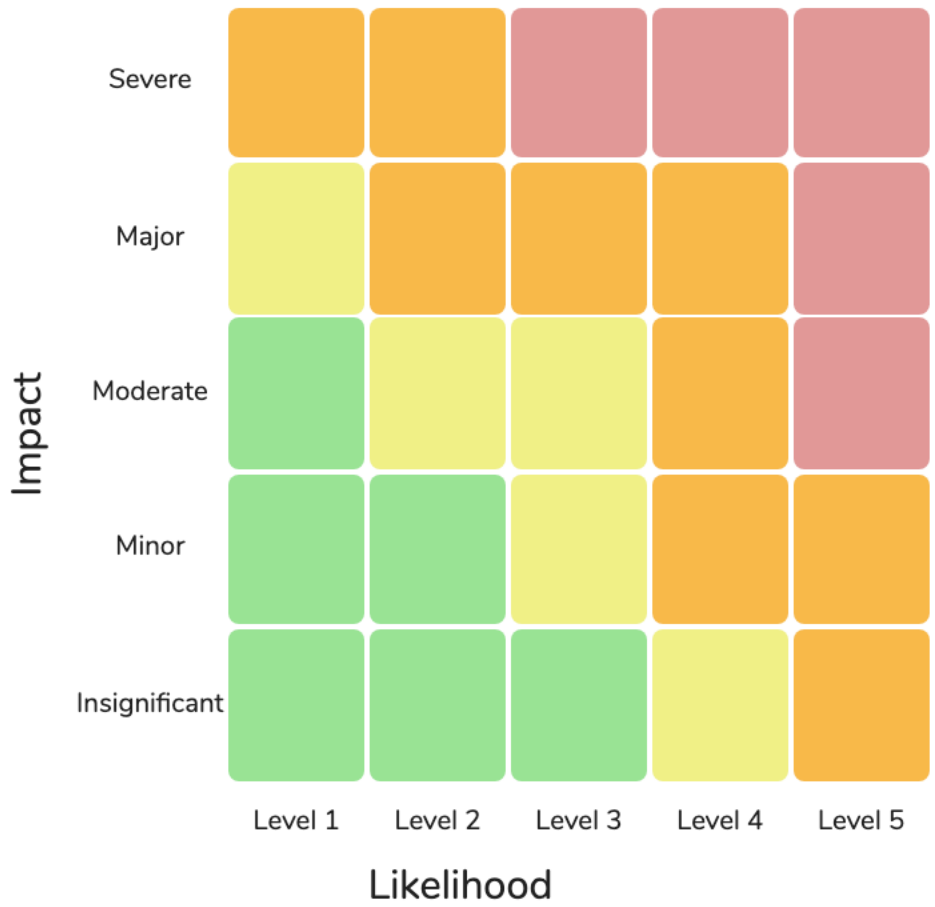
A Virtual Learning Experience

The Right Cyber Story

Do Your Homework

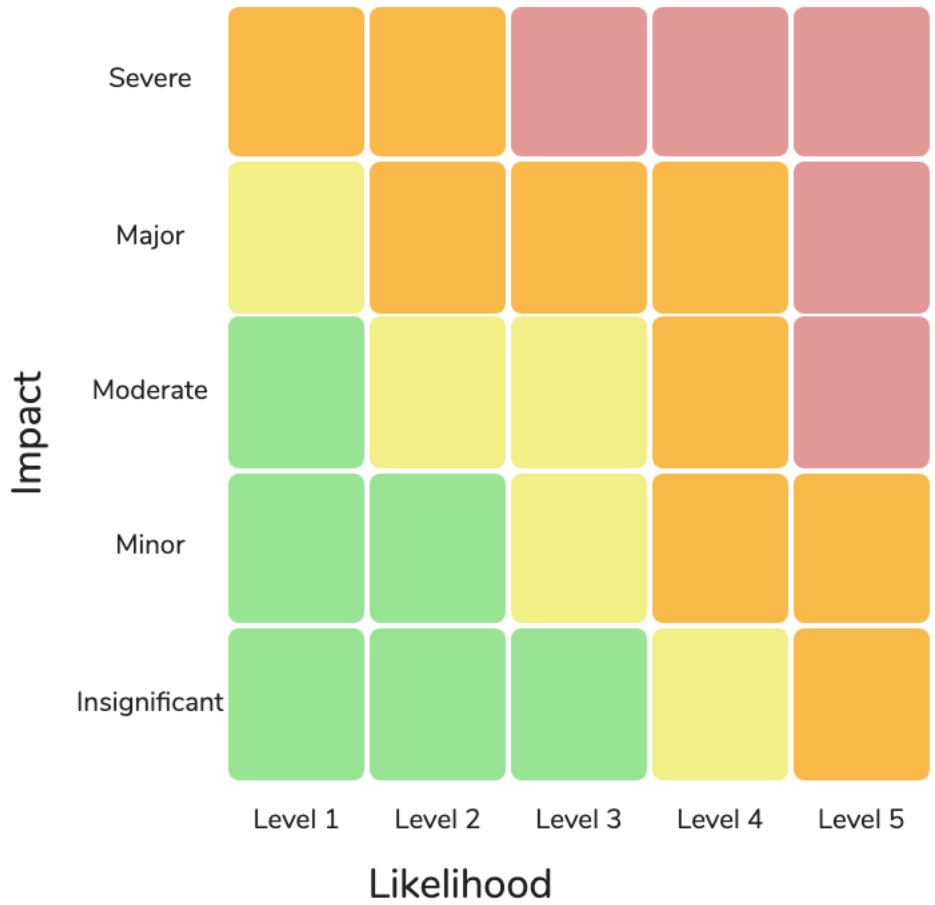
Determine your risk tolerance (appetite) levels

Risk Event Type	Tolerance Level
Data Breach	Low
System Availability	Low
Data Integrity/Tampering	Medium
System Misuse	Medium
Defacement	High
Malicious Damage	Medium
Fraud	Low
Extortion	Medium



Determine the financial impact of cyber risks

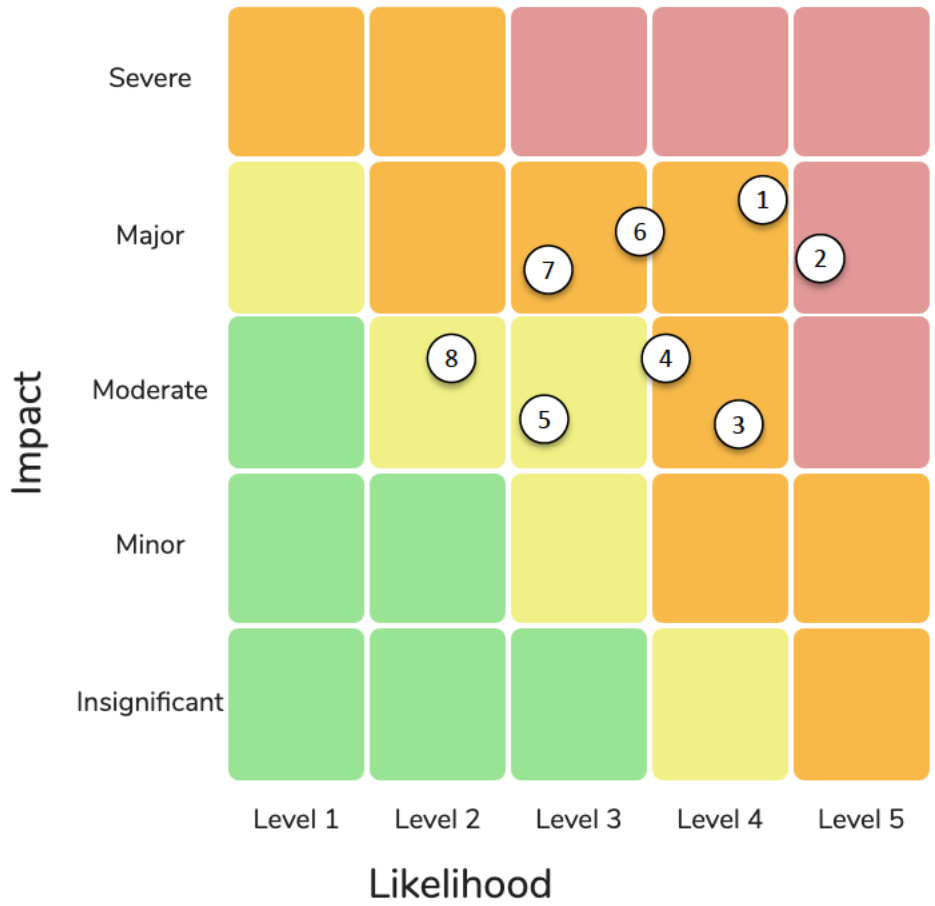
Risk Event Type	Financial Impact	
Data Breach	Major	$10m - $30m
System Availability	Major	$10m - $30m
Data Integrity/Tampering	Moderate	$5m - $10m
System Misuse	Moderate	$5m - $10m
Defacement	Moderate	$5m - $10m
Malicious Damage	Major	$10m - $30m
Fraud	Major	$10m - $30m
Extortion	Moderate	$5m - $10m



Determine where you stand in terms of risk exposure

Risk Event Type

1. Data Breach
2. System Availability
3. Data Integrity/Tampering
4. System Misuse
5. Defacement
6. Malicious Damage
7. Fraud
8. Extortion



Understand your cybersecurity capabilities

A. Asset Management
B. Business Environment
C. Governance
D. Risk Assessment
E. Risk Management Strategy
F. Supply Chain Risk Management

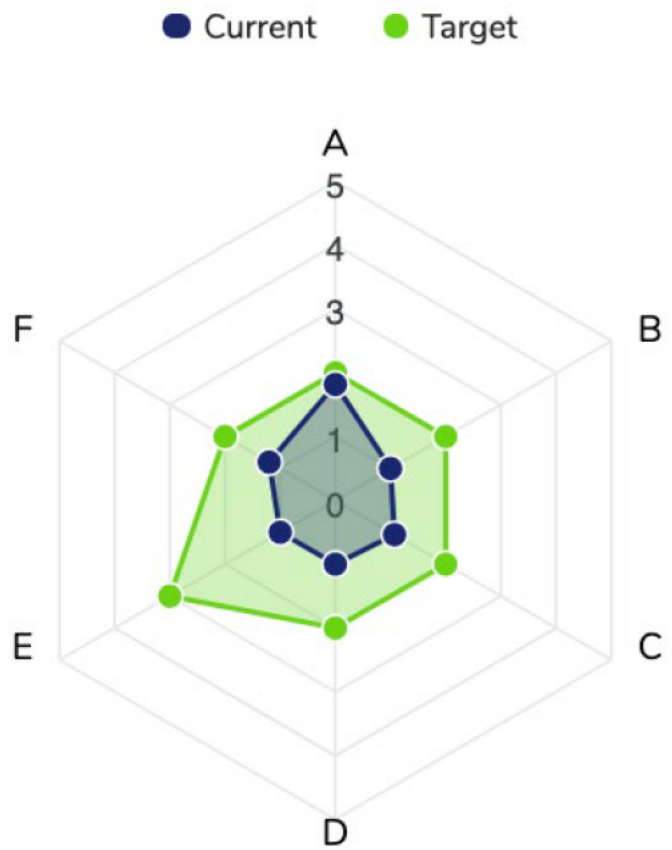
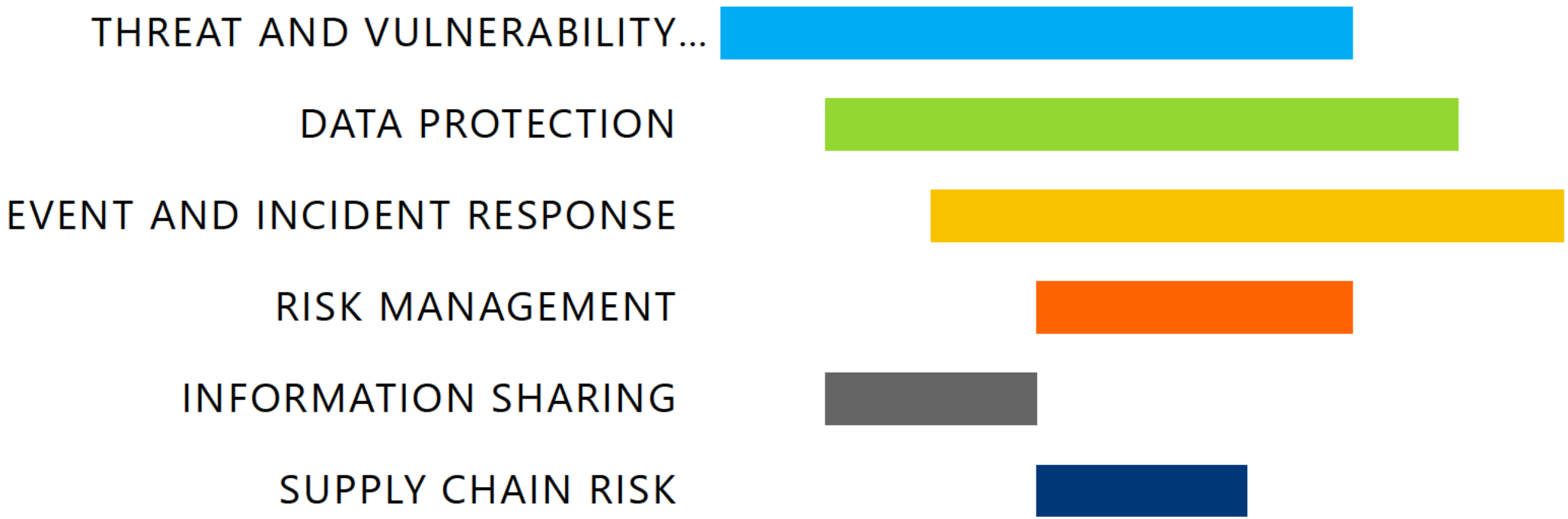
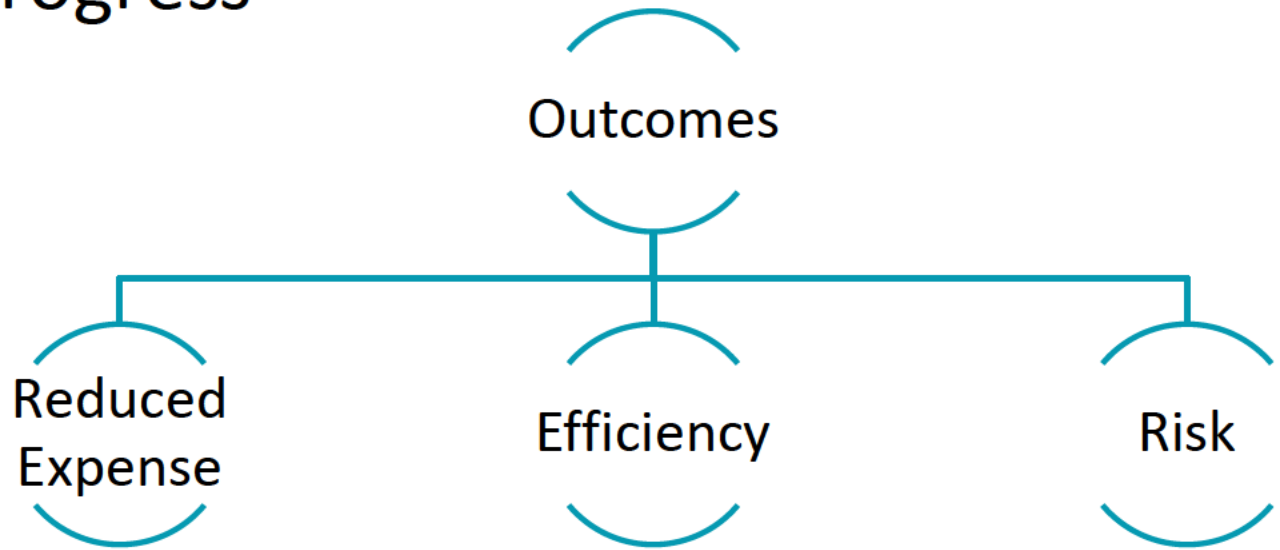


Figure out how you are going to close the gaps



More than that, create a business case for change

1. Align to business goals
2. Right-size spend by aligning to outcomes
3. Monitor and report progress



Use a simple metric to quantify how you are doing overall

- While the purists may argue this unfairly trivialises the team's hard work, the reality is that often, executives and board members just don't have time to look at all the detail
- But you need the detail ready, if you are asked to explain the "why" and "so what"

Make the way you do this repeatable

Focus on the business representation of cybersecurity and build a permanent bridge to translate cyber in a normalised way

RSAConference2020 APJ

A Virtual Learning Experience

Telling the story

Game Day

Considerations

The steps outlined are the standard way you go about things.

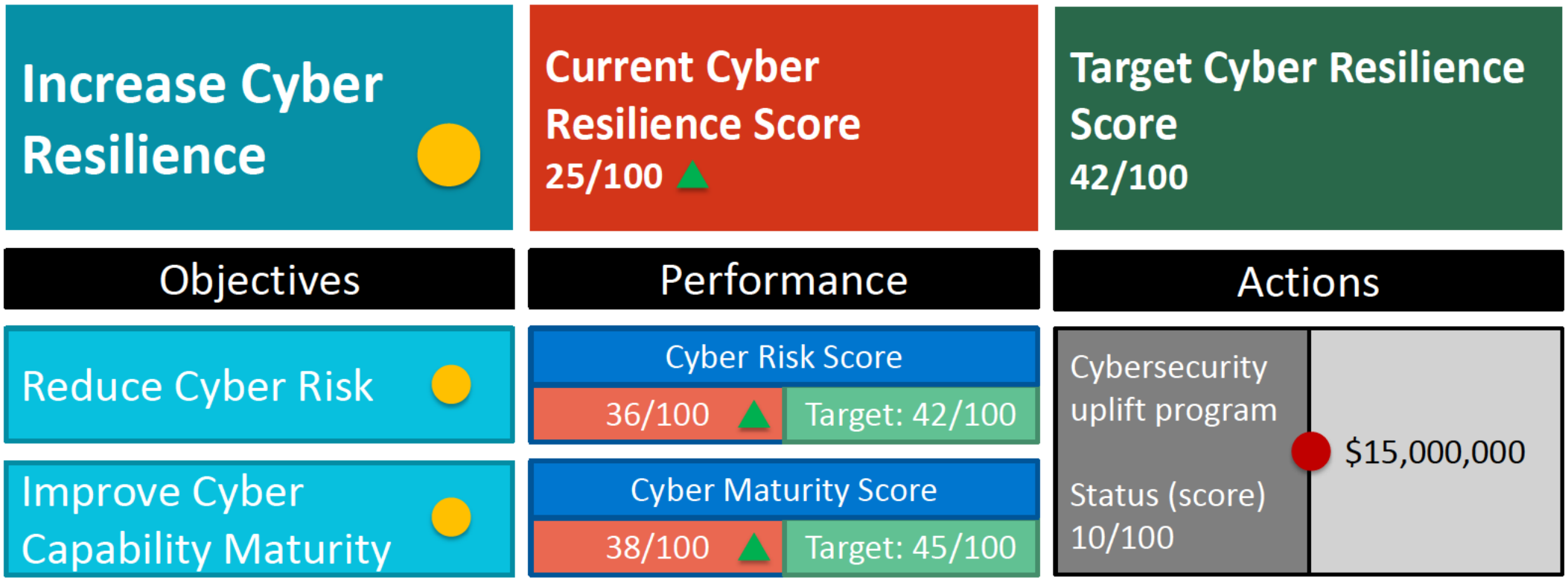
From time-to-time, you may need to front the executive committee and board because of a significant cyber incident.

Due to the tailored nature of the conversation when such incidents occur, this does not cover what you should do in those cases.

Your delivery and ability to present will get you very far

- If you aren't a confident presenter, get trained in the art of presenting; it really does help.
- Script your delivery.
- Practise. Practise. Practise.
- Make sure the content looks good. Get help if your superpower isn't in creating content for executive audiences.
- **Treat it like you are about to deliver a keynote at a large conference and embrace it.**

Have your 1-page ready if that's all you have time for



Key story elements

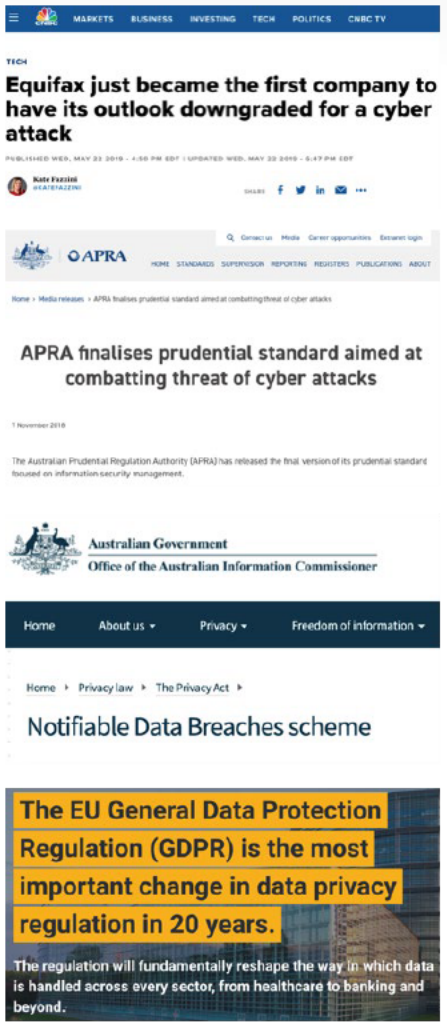
1. Industry update
2. How are we doing?
3. Where are we trying to get to?
   - Is it enough?
   - When are we going to get there?

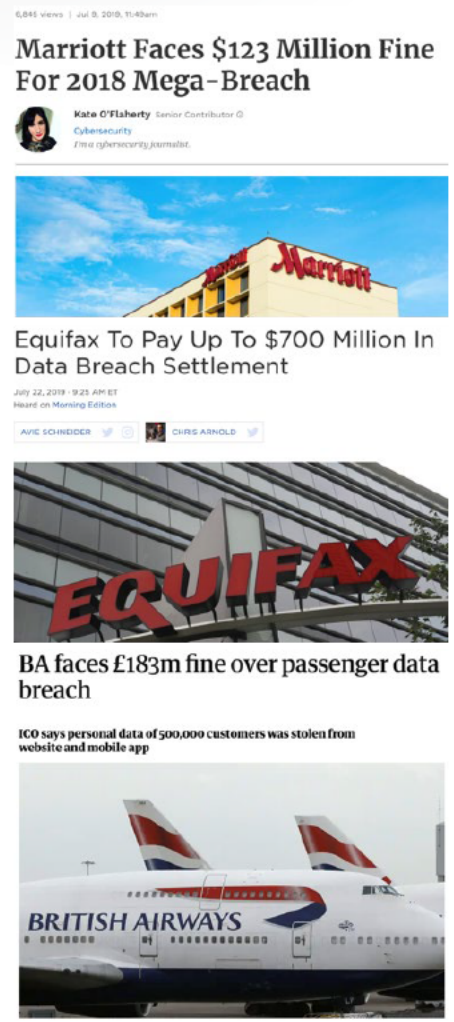
Remember: Keep things at a high level. Have the detail ready, but only go there if asked.

Industry update

This is your chance to show what a compelling storyteller you are, but go easy on the FUD:

1. Explain as objectively and as calmly as possible the key events that have occurred since the last update.
2. Explain which ones are relevant to the organisation.
3. Tell the story of how you handle things should they occur. They need to know you've "got this".





How are we doing?

Our cyber resilience posture needs work

Key wins: reduction in Defacement risk, improvement in Detect (DE) capability, and 6 program activities completed

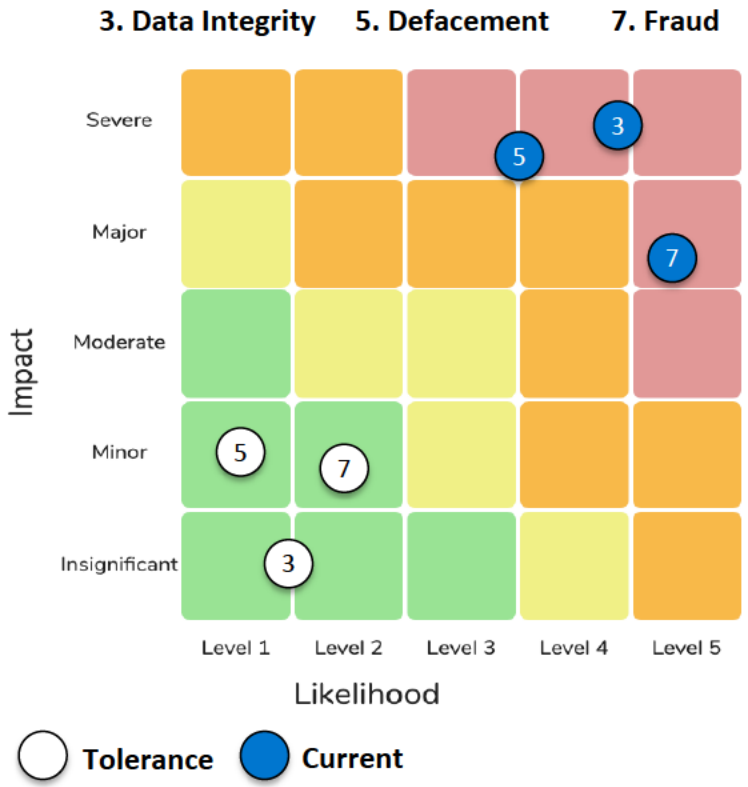
Risk	Defacement	62.5%	35.2%	▼
Maturity	Detection	2.2	1.9	▲
Program	Activities Completed	6	5	▲

Key concerns: least improvement in System Misuse risk, least increase in Protect (PR) capability, and 2 program activities completed late and over budget

Risk	System Misuse	65.2%	31.8%	▼
Maturity	Protect	1.2	0.5	▲
Program	Activities Over Budget	2	1	▲

How are we doing?

Top 3 risks outside of tolerance levels are: Data Integrity, Defacement, and Fraud



Exposure to Defacement, Data Breach, and Data Integrity risks were reduced by the largest margins

Defacement	62.5%	35.2%	▼
Data Breach	62.9%	34.6%	▼
Data Integrity	64.1%	33.8%	▼

How are we doing?

Protect, Identify, and Recover capabilities improved

Capability	Current	Target	Increase/ Decrease
Protect	1.3	3.2	1.3 ▲
Identify	2.1	3.8	1.6 ▲
Recover	1.9	2.9	1.9 ▲

6 program activities were completed, mostly over budget and/or behind schedule

Project Activities	Over Budget	On Budget	Under Budget
Behind Schedule	2	2	0
On Schedule	0	0	0
Ahead of Schedule	2	0	0

Where are we trying to get to?

At the completion of our program, our cyber resilience posture will be at a score of 42/100

Question: Is this an acceptable score? Why?

Where are we trying to get to?

Program is on track to finish ahead of time but will likely be over budget by $2,636,897

Program completed	86%
Planned end date	31 Jan 2021
Planned budget	$3,640,000
Projected end date	15 Sep 2020
Projected cost	$6,276,897

Question: Is is acceptable that we will be ahead but over budget?

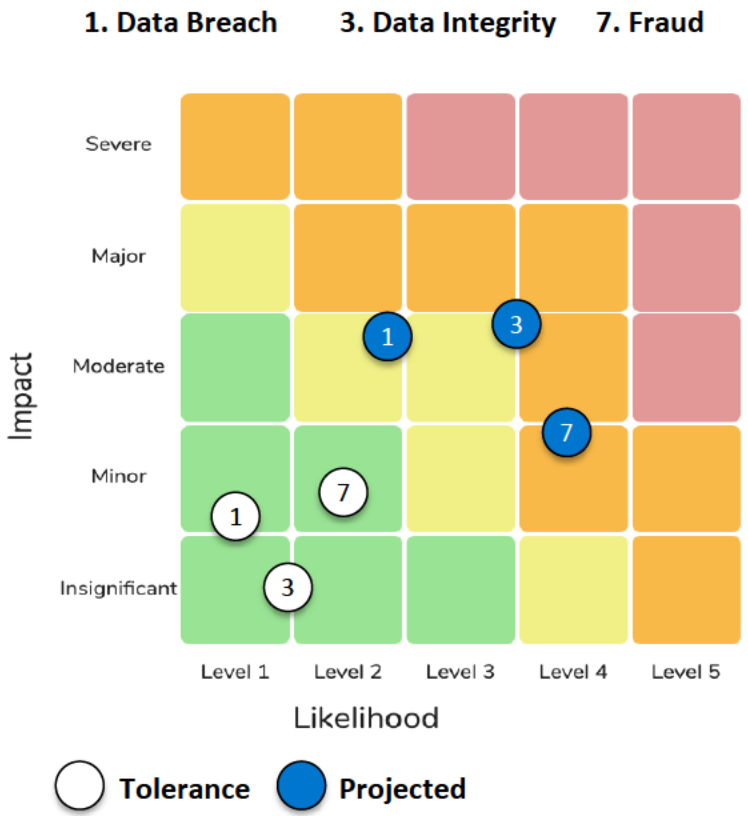
24 program activities will be completed, mostly on budget and on time, or better

Project Activities	Over Budget	On Budget	Under Budget
Behind Schedule	6	0	0
On Schedule	1	0	1
Ahead of Schedule	5	9	2

Where are we trying to get to?

Question: Is it acceptable that we will not get to our risk tolerance levels?

Data Breach, Data Integrity, and Fraud risks will still be outside of tolerance



We will have reached the cyber capability targets currently defined

Capability	Projected	Target
Identify	2.8	2.5
Protect	2.9	2.5
Detect	3.2	2

Where are we trying to get to?

Summary

- We will get to a score of 42/100.
- We will not get to our cyber risk tolerance levels.
- We will finish our program ahead of time but be $2 million over budget.
- How can we meet our cyber capability targets, but not get to our risk tolerance levels? Are we not aiming high enough?

Questions:

- Should we adjust our risk tolerance levels?
- Should we adjust our strategy?
- Do we need to spend more?

What if we need to spend more?

Build your business case:

1. Determine the additional activities that need to be added to your strategy, including scope, costs and duration.
2. Clearly articulate the outcomes each helps to achieve.
   - E.g. Spending an additional $500K on a data protection program that takes 6 months will reduce the likelihood of a data breach by 25% when it is done.
3. Present options and the associated outcomes (i.e. risk reduction and capability improvement) of each.

RSAConference2020 APJ

A Virtual Learning Experience

Conclusion

Summary

- Use the language of risk, business impact, capabilities, and outcomes.
- Technical security risks are not the same as cyber (business) risks, but they are related.
- Manage progress against a strategic, defensible plan.
- Investment is driven by regulatory requirements, risks, key industry trends, audit findings, and business/financial impacts.
- There must be logical, defensible ties between (and to) the key cyber risk metrics being tracked and reported on.

Apply

- Next week you should:
  - Determine if you can articulate your key cyber risks, tolerance levels, and current cybersecurity capabilities.
  - If not, make a plan to address this.
- In the first three months following this presentation you should:
  - Define the outcomes you are trying to achieve: cyber risk tolerances, cyber capability targets.
  - Assess if your cyber strategy will get you to the outcomes.
  - Adjust your cyber strategy as required.
- Within six months you should:
  - Operationalise how you track and report on your cyber risks, capabilities, strategy; this should be embedded into your team's day-to-day.