CISO EDGE

ADAPT

How to win Boards and influence the executive

Top 10 Tips for productive conversations

Ellie Warner
Global Head, Cyber Awareness, Standard Chartered Bank (Singapore)

CISO EDGE


WE NEED SOME NEW JARGON, THE PUBLIC ARE STARTING TO UNDERSTAND WHAT WE'RE TALKING ABOUT!
WHAT PART OF
$i\hbar\frac{\partial}{\partial t}\Psi(\vec{r},t) = \left(-\frac{\hbar^2}{2m}\nabla^2 + V(\vec{r},t)\right)\Psi(\vec{r},t)$
DON'T YOU UNDERSTAND?

Why the focus on executive engagement? Why now?

CISO EDGE

Elevated accountability, governance and oversight

Increase in regulatory requirements
Cyber as a business risk

High visibility data breaches (and some substantial fines)

The Marsh report: Cyber risk governance

CISO EDGE

7 Questions the board should be able to answer

- Have statutory / regulatory requirements been met?
- Have cyber exposures been qualified / financial resilience tested?
- Improvement plan in place to bring exposures within agreed risk appetite?
- Do regular board discussions take place with clear actionable MI?
- Are breach plans in place, exercised?
- Are roles clear and aligned to 3 LOD?
- Is there independent validation and assurance (testing/certification/insurance)?

Elements against which Boards can benchmark Cyber Risk Governance

- (Clarity on) Strategy
- (Extent of) Board ownership
- (insight into) Financial Resilience
- Executive Accountability
- Independent Assurance
- Board reporting

The Board's proactivity will be based on…

The Board's level of challenge will be based on…

Source: The City/UK Marsh report "Governing Cyber Risk"


58%
Intrusion Detected
Corporate directors at public companies believe that cyber-related risk is the most challenging risk

Let’s use our seat at the table


TOP 10

#1: Decide your key messages and asks

#2: Know your audience

#3: Build trust

#4: Adopt a framework

#5: Use relevant / external benchmarks

#6: Speak their language

Metrics

vs

KPIs

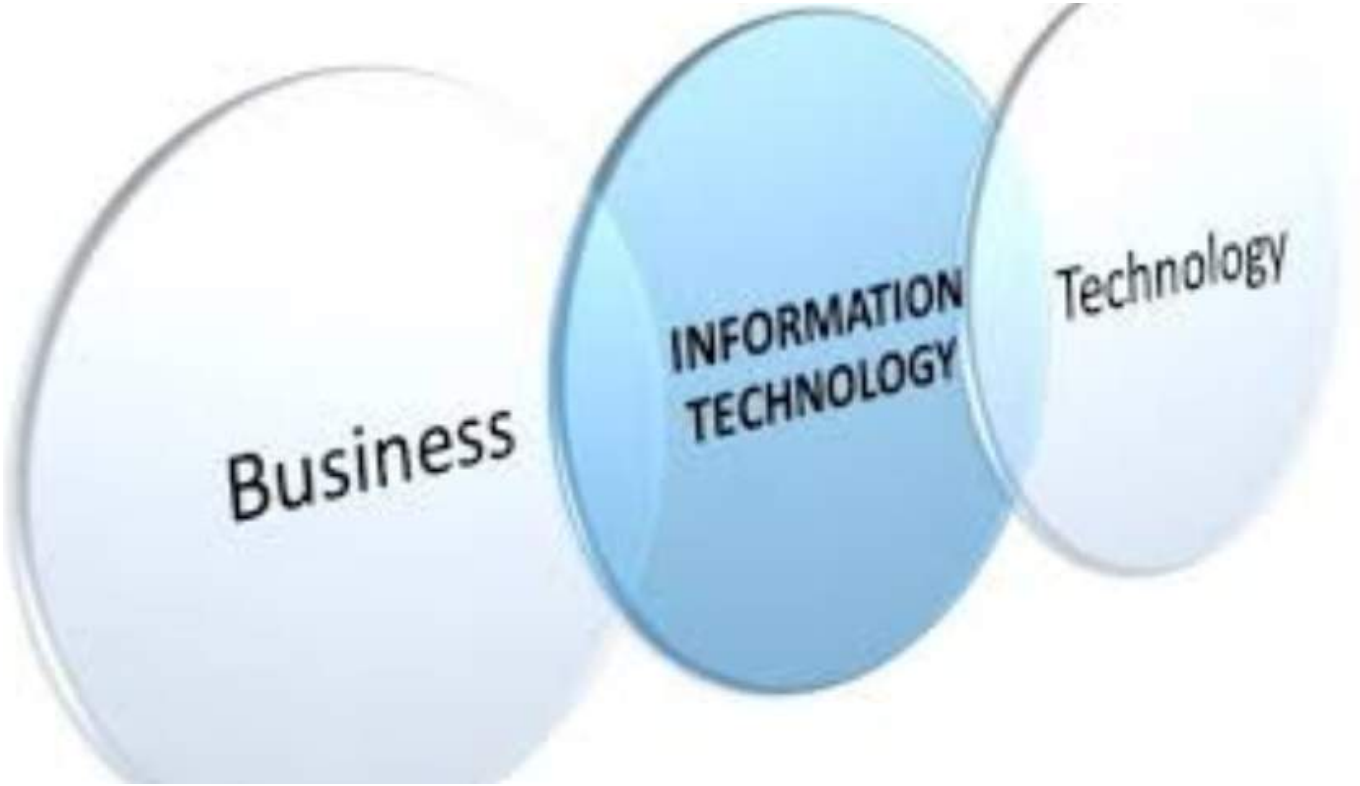
#7: Report on programme maturity vs operational metrics

Issues CISOs should be able to talk to

CISO EDGE

- Cyber Landscape, Actors, Impact/Likelihood
- Do we have a framework for managing ICS risk? Is our framework aligned to ERM/business and IT strategy?
- What is our plan to address the risks? How will we measure success? What is our risk appetite?
- Have we done any external benchmarking?
- Security Culture / Employee Risk management
- Can we qualify Third Party risk?
- Do we know where our information assets are? Are they appropriately protected?
- Do we have an incident response plan? Time to recover from an event?
- Can we use Cyber as a market differentiator / value add to customers?
- # High risk users / access to systems? Presence of / time to fix vulnerabilities

Source: The City/UK Marsh report "Governing Cyber Risk"



#8: Security as a business enabler

#9: Executive engagement as an iterative process

#10: Be Human!

CISO EDGE

ADAPT

My Closing Ask…

$28 trillion

What action will you take?

ADAPT

Thank you

CISO EDGE

Top 10 Tips

ADAPT

1. DECIDE YOUR KEY MESSAGES

What are the key messages you want to convey?

What specific actions do you want the executive to take?

Anticipate their questions and plan ahead

2. KNOW YOUR AUDIENCE

Board members have varying degrees of ICS knowledge

Start at high level

Avoid jargon, TLAs and shiny new toy speak

Do your research about the board

Be flexible

Know the rules

3. BUILD TRUST

Establish credibility early on

Balance between scaremongering and "green" washing

Acknowledge "when, not if"

Be transparent about the gaps

Outside speakers

4.ADOPT A FRAMEWORK

Use an industry framework such as NIST

Align your plan to the framework

Break it down. Clear path to green.

Consistently report progress / maturity by area

5. USE EXTERNAL BENCHMARKS / REPORTS

Peer to peer or industry benchmarks

Conduct an external assessment

Use eg: Marsh report to know "what good looks like"

Aim for a minimum standard of proactivity and challenge

CISO EDGE

Top 10 Tips

ADAPT

6. SPEAK THEIR LANGUAGE

Risk management

Establish a close partnership with the business

Align your messages with the business and IT strategy

What's the risk appetite

Explain the news

7. TALK PROGRAMME MATURITY VS METRICS/EVENTS

From metrics to forward looking reporting

Progress vs the plan

Vulnerability reduction

Avoid operational metrics / # events

Focus on business KPIs

8. POSITION IT AS PART OF THE SOLUTION

Security are often seen as the "no guys"

Show how "good security" can enable the business

Focus on solutions that address the gaps

Security as a competitive advantage

9. KEEP ENGAGED

Iterative process

Identify topics for the year eg: risks annually, maturity semi annually

Decide how often do you want to meet

10. BE HUMAN

Be approachable