

Practical Approach to OT Risk – Hype or Reality?

Exploring Holistic and Practical
Strategies for Critical
Infrastructure Security

Trevor Goldman

15th July 2024



Introductions



Brief overview of the session's objectives



Importance of OT security for critical infrastructure



The gap between traditional IT security controls and OT needs

Cost-Effective Initial Assessment



"WHAT DO YOU HAVE
ALREADY?" – INITIAL
ASSESSMENT



ASSURANCE APPROACH TO
DETERMINE THE CURRENT
SITUATION



EMPHASIS ON COST-
EFFECTIVENESS AND
LEVERAGING EXISTING
RESOURCES

Stakeholder Engagement



Importance of talking to stakeholders



Understanding their perspectives and desired outcomes



Building a collaborative environment for security improvements

Leveraging Existing Frameworks



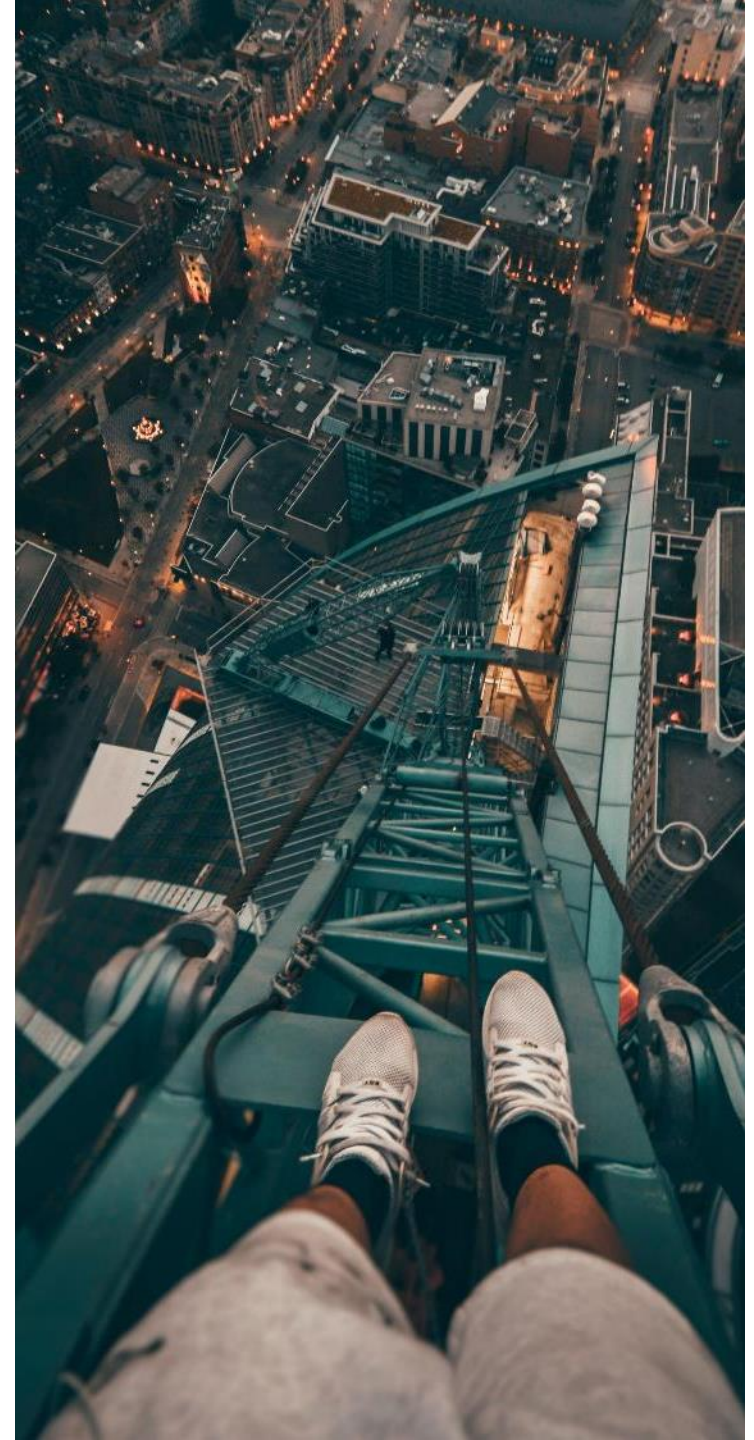
IEC 62443 and SOCI Act



Tailoring the frameworks to meet specific organizational needs

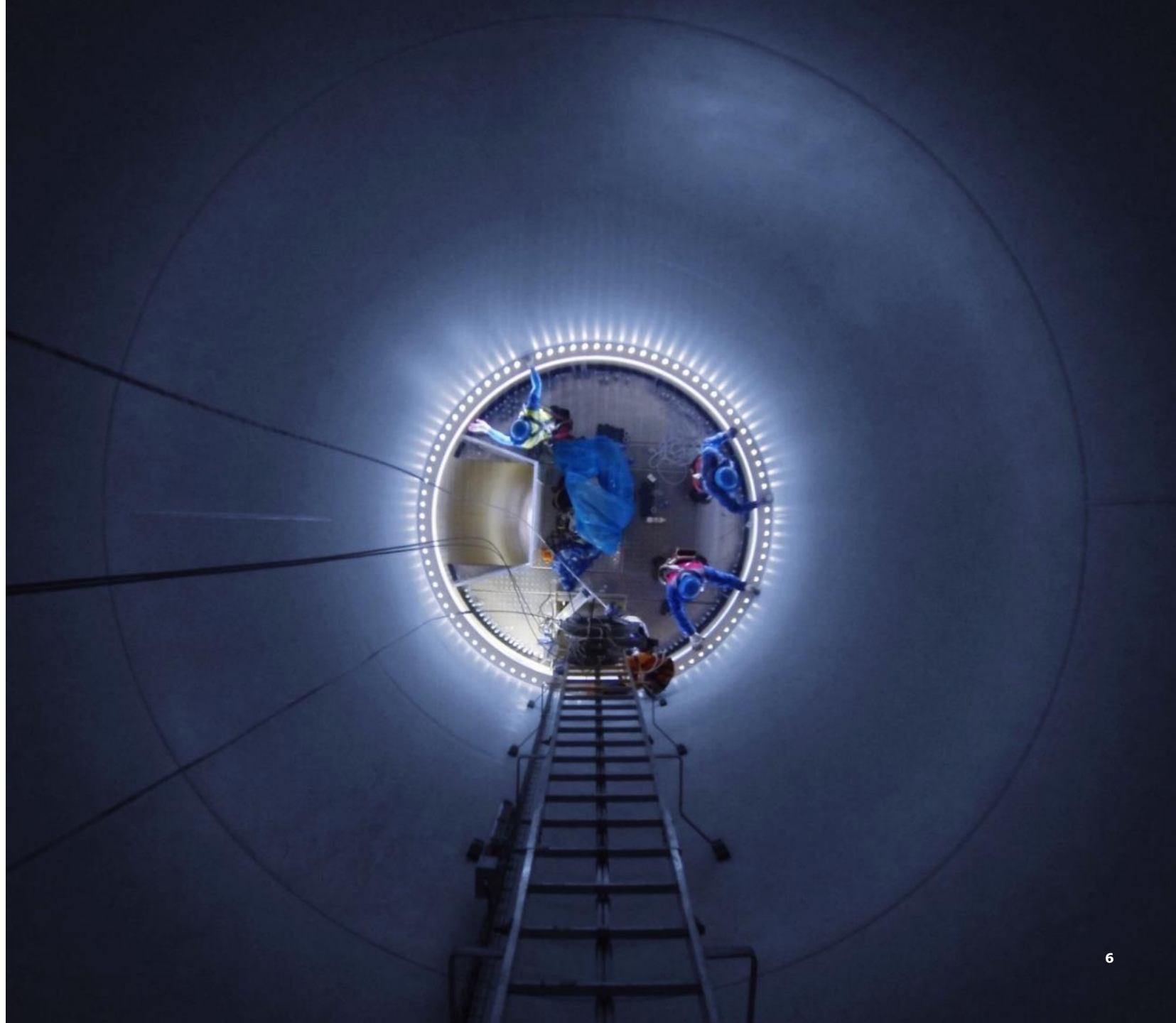


How these frameworks guide the security strategy




Developing a Phased Approach

1. Creating a phased plan of action based on initial assessment
2. Prioritizing actions based on risk and impact
3. Example of a phased implementation strategy



Practical Implementation Strategies



Steps to implement a
practical OT security
strategy

Case studies or examples
of successful
implementations

Key practices to ensure
ongoing effectiveness

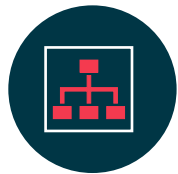
Mitigating Third-Party Risks



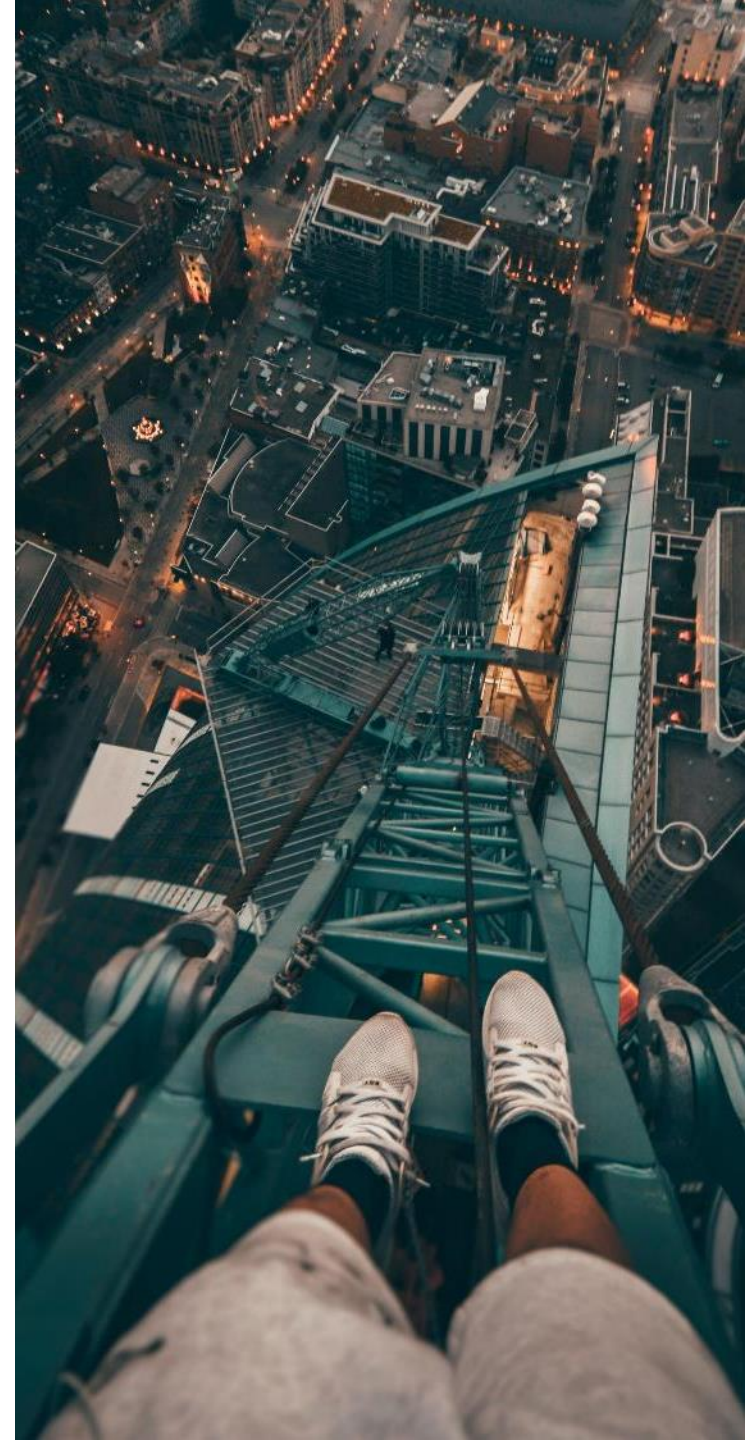
Importance of managing third-party risks in OT environments



Strategies to assess and mitigate third-party risks



Success Stories



Communication and Coordination



The role of collaboration
between different teams
(business, IT, OT)



Effective communication
strategies for cross-
functional teams



Tools and frameworks to
facilitate collaboration

Measuring Success and Continuous Improvement

Incident Reduction:
Fewer and less
severe security
incidents

Compliance Rate:
Adherence to IEC
62443 and SOCI
Act

Vulnerability
Management:
Faster identification
and mitigation

Downtime
Reduction: Less
downtime from
breaches

Response Time:
Improved incident
response times

Continuous
Improvement
Practices

Regular
Assessments:
Periodic reviews
and updates

Training: Ongoing
staff education

Feedback Loops:
Incorporating
incident lessons
and stakeholder
input

Tech Updates:
Keeping systems
current

Policy Reviews:
Updating policies
for new threats

Learning from
Incidents

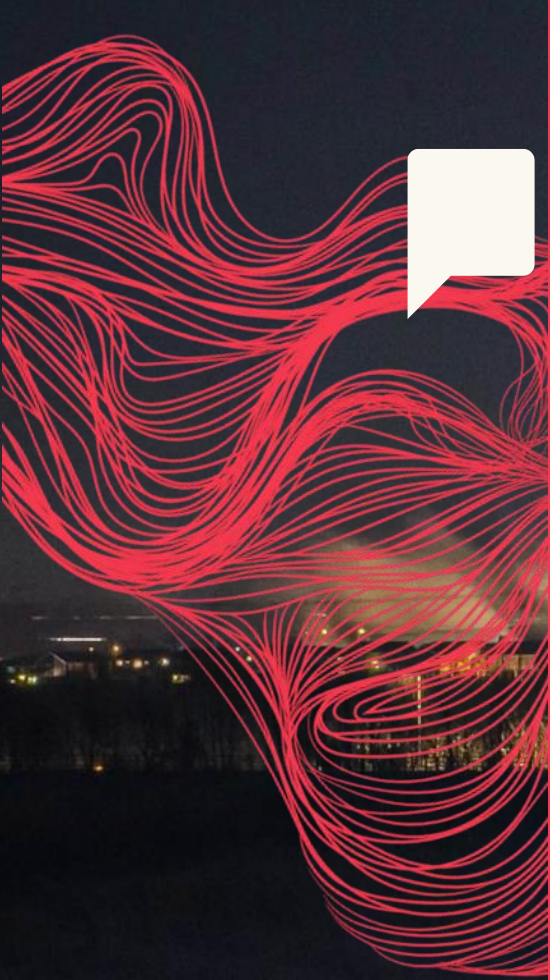

Incident Analysis:
Identify root
causes

Lessons Learned:
Document and
share findings

Benchmarking:
Compare with
industry best
practices

Adaptation: Evolve
strategies for new
challenges



- 
- 
1. Recap of key points discussed
 2. Final thoughts on the practicality of a holistic OT security approach
 3. Call to action for critical infrastructure owners and operators

CONCLUSION





Open the floor for questions and answers



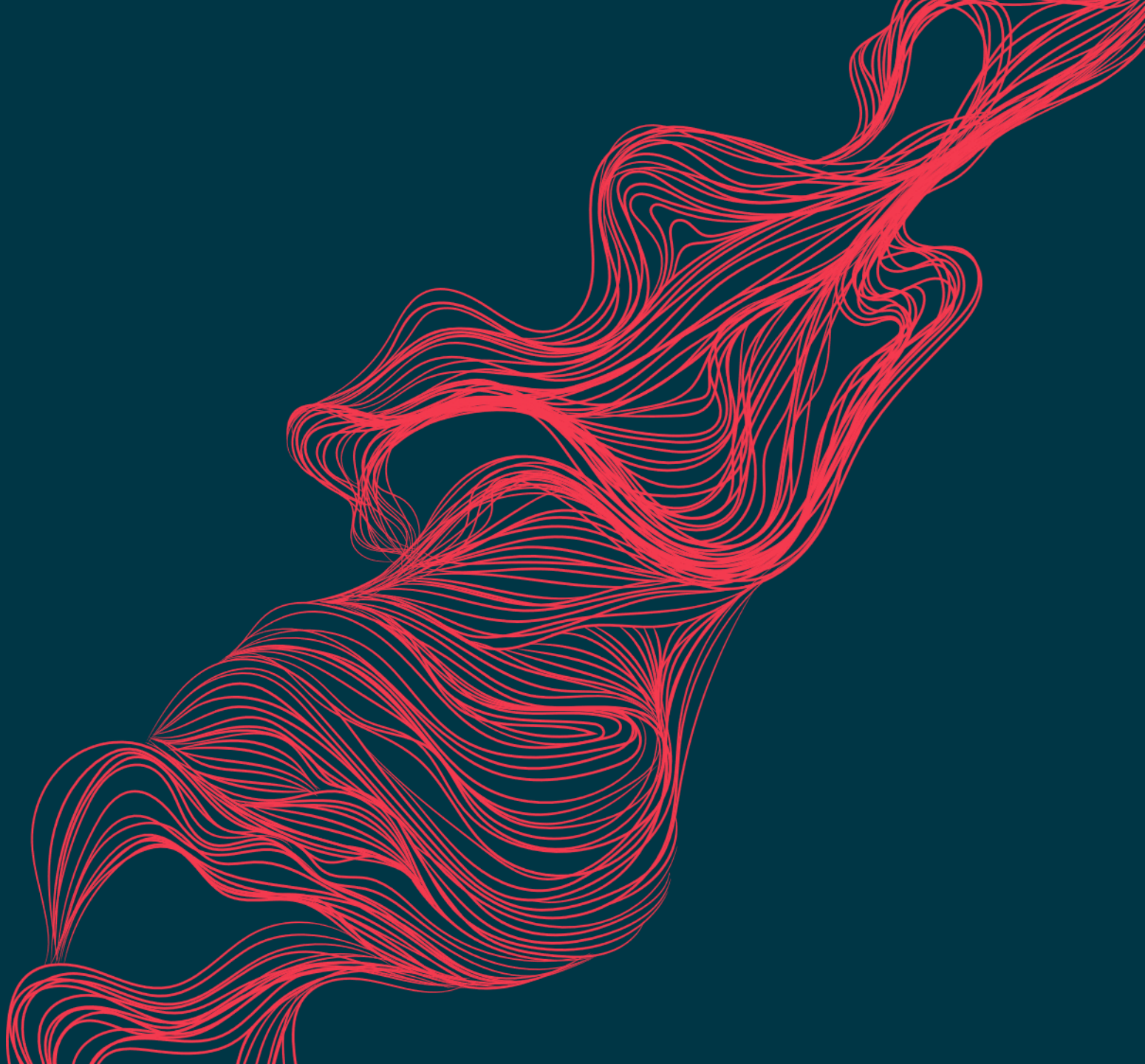
Contact Us:

N: Trevor Goldman – Technical Director – OT Cybersecurity

T: +61 449 845 449

E: trevor.goldman@worley.com

worley.com



Disclaimer

This presentation has been prepared by a representative of Worley.

The presentation contains the professional and personal opinions of the presenter, which are given in good faith. As such, opinions presented herein may not always necessarily reflect the position of Worley as a whole, its officers or executive.

Any forward-looking statements included in this presentation will involve subjective judgment and analysis and are subject to uncertainties, risks and contingencies—many of which are outside the control of, and may be unknown to, Worley.

Worley and all associated entities and representatives make no representation or warranty as to the accuracy, reliability or completeness of information in this document and do not take responsibility for updating any information or correcting any error or omission that may become apparent after this document has been issued.

To the extent permitted by law, Worley and its officers, employees, related bodies and agents disclaim all liability—direct, indirect or consequential (and whether or not arising out of the negligence, default or lack of care of Worley and/or any of its agents)—for any loss or damage suffered by a recipient or other persons arising out of, or in connection with, any use or reliance on this presentation or information.

