



THINK FORWARD

**How OT leaders are tackling
visibility, legacy risk and
uptime-first security**

How OT leaders are navigating visibility, legacy risk and operational resilience

What does it take to protect critical systems without disrupting the operations they support?

That was the central question at Lock It Down: An OT Security Power Lunch, hosted by RES. Business IT and Fortinet in Brisbane. The closed-door event brought together senior technology and operational leaders from asset-intensive sectors such as mining, manufacturing, food production and agriculture for a candid, peer-led discussion: What's working, what's breaking, and what's next in OT security?

THIS REPORT DISTILLS THE INSIGHTS INTO FOUR STRATEGIC FOCUS AREAS:



Ownership and visibility

How teams are bridging responsibility gaps across IT and OT



Availability and safety

Why uptime often overrides risk controls and what to do about it



Legacy risk

How to contain inherited vulnerabilities without disrupting production



Collaboration and resilience

Why trust, process and shared capability matter most



Ownership and visibility: Why clarity is the foundation of OT security

Visibility and accountability are the foundation of secure OT environments, but both are often missing. As OT systems become more connected, ownership is quietly shifting to IT without formal handover or structure. The result is a growing number of blind spots across critical infrastructure.

Incomplete asset inventories, flat networks and vendor-installed equipment make it difficult to see where risk begins or ends. Leaders shared how fragmented responsibility slows response, weakens oversight and turns basic questions like “who owns this?” into roadblocks.



Insights and trends

Responsibility for OT systems is increasingly falling to IT, but the transition is rarely structured. In many cases, there is no documentation, no formal handover and no defined accountability. Control is often shared informally across internal teams, engineering groups and third-party vendors. This creates confusion about who is responsible when something goes wrong.

That uncertainty directly impacts visibility. Without clear ownership, asset inventories are often incomplete. New devices may be added without proper configuration or change control. Flat networks and ageing infrastructure make it harder to understand how systems are connected or where risks may lie. In many environments, visibility only improves after something breaks, or when compliance or audit requirements force the issue.

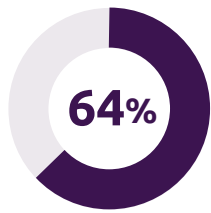
Even when risks are known, response is often delayed by fragmented oversight. Vendors can bypass internal processes, and instrumentation teams may retain control of specific assets. These overlaps make coordination harder and slow decision-making. The result is more than technical debt. It is a lack of shared awareness that increases risk across the board.



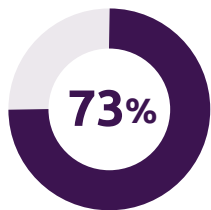
“One of the biggest challenges is getting people comfortable with bringing IT and OT together. There’s often this fear that if you connect the two, something will break, but it’s not true. We need people who’ve done it before, who can walk in and show that it’s possible to run both on one platform safely and effectively. It does work, and the world doesn’t end when you do it.”

– LUKE SMITH,
PRINCIPAL - IT INFRASTRUCTURE LEAD,
HARMONY AUSTRALASIA

Visibility by the numbers



64% of organisations lack visibility across their network of connected OT assets and systems, leaving critical blind spots in ageing and fragmented environments.



73% of organisations experienced a cyber intrusion that impacted OT systems in 2024 (up from 49% in 2023)



45% of OT cybersecurity service engagements reveal a lack of visibility across networks, complicating accountability and response in multi-vendor setups.

KEY TAKEAWAY

Clarify ownership before you secure.

Visibility without ownership leaves organisations exposed. A secure OT environment starts with a shared understanding of what exists, how it operates and who is responsible for its protection.



RES RECOMMENDS

Start with an OT systems register. It does not have to be complex, but it should include the essentials:

- ✓ A list of key systems and how they are connected
- ✓ Internal owners and third-party vendors
- ✓ Interfaces such as telemetry, remote access or reporting feeds
- ✓ Support arrangements and escalation points

This simple step creates clarity. It helps identify blind spots, strengthen accountability and support faster decision-making. From there, visibility can grow into shared responsibility and more structured risk management.



Availability and safety: Making OT security operationally viable

Security in OT environments has to respect a simple rule. If a control threatens uptime or safety, it will not be implemented. Cyber risks are well understood, but operational disruption is not an acceptable trade-off.

This session highlighted a key challenge. Security must be delivered in a way that aligns with how these environments actually run, not just how frameworks are written.



Insights and trends

During the discussion, leaders kept returning to a clear reality: if a control risks uptime or safety, it will not be implemented. Operational disruption is not an acceptable trade-off, even when the cyber risk is understood.

Patching is one of the first things to fall behind. Some environments only allow it once or twice a year, and even then, only if the business case stacks up. That delay leaves known vulnerabilities unaddressed.

Backup and recovery processes follow a similar pattern. Teams can assume they're covered, but testing is often infrequent. Several attendees noted that maintaining consistent backups across systems has been challenging – and, as a result, recovery processes have sometimes been delayed when needed.

On top of this, security frameworks like the Essential Eight are often referenced, but not strictly followed. Many prescribed controls are viewed as incompatible with legacy systems. In response, teams are adopting more pragmatic strategies – prioritising monitoring, detection, and containment to reduce risk while maintaining operational continuity.

The message was consistent: OT security must be shaped around availability, not the other way around.



“In OT environments, cybersecurity must focus on availability and safety above all, ensuring systems stay online and human lives are protected, as downtime or failures have immediate, critical impacts beyond mere data concerns.”

– JOSHUA ALCOCK,
OT SECURITY AND THREAT INTELLIGENCE MANAGER,
FORTINET

Operational risk by the numbers



86% of major cyber incidents in 2024 resulted in operational downtime, reputational damage, or financial loss, emphasising the high stakes of maintaining availability in OT environments.



75% of observed ransomware cases against industrial organisations in 2024 involved some degree of operational disruption, reinforcing the need for non-intrusive resilience strategies like monitoring over aggressive patching.



94% of OT professionals avoid security controls that risk disrupting operations or safety, even when risks are known.

KEY TAKEAWAY

Design security around uptime.

Availability is the priority in OT. Security must be implemented in ways that maintain continuity, minimise disruption and align with operational constraints.



RES RECOMMENDS

Start with practical steps that improve resilience without impacting system availability:

- ✓ Enable system logging and monitor for anomalies
- ✓ Use allowlisting where patching is not viable
- ✓ Review and secure vendor remote access pathways
- ✓ Apply time-bound user accounts and least privilege access
- ✓ Test backup restores regularly, even if only partially
- ✓ Incorporate security awareness into daily operations

Controls that work quietly and reliably are the most effective in OT. Build around what is possible now, not what is ideal later.



Legacy systems and the path to secure integration

Most OT environments still depend on systems that were never built to be connected. These legacy assets often run on outdated platforms with limited support and minimal security, yet remain critical to operations. As exposure grows, teams are shifting focus. Rather than waiting for large-scale upgrades, they are isolating high-risk systems, improving visibility and designing controls that contain risk without disrupting production.



Insights and trends

Legacy systems were a recurring topic throughout the lunch, as leaders explored the risks of securing infrastructure that was never designed to be connected. Many environments still rely on unsupported operating systems or ageing hardware, where patching can introduce instability, void warranties or require downtime that operations cannot accommodate.

That challenge is often compounded by network design. Flat, unsegmented environments remain common, allowing a single compromise to spread quickly without containment. Without clear boundaries between systems, even minor incidents can escalate.

In many cases, the devices themselves offer limited protection. Features like encryption, access controls and logging are often missing or insufficient. Segmentation and isolation become critical to reducing exposure without disrupting operations.

To address this, teams are beginning with visibility. Mapping dependencies, understanding traffic flows and securing access pathways are helping organisations design targeted controls that work within the constraints of legacy environments.



“Legacy OT systems, often unpatchable due to operational constraints, require layered security approaches like network segmentation and strict access controls to mitigate risks while maintaining production continuity.”

– JOSHUA ALCOCK,
OT SECURITY AND THREAT INTELLIGENCE MANAGER,
FORTINET

Legacy incidents by the numbers



Over 50% of OT environments rely on legacy systems for at least half their infrastructure, exposing critical operations to unpatchable vulnerabilities and unsupported hardware.



43% of organisations experienced a cyber incident targeting legacy OT systems in the past year, often due to flat networks and absent security features like encryption.



75% of OT attacks originate as IT breaches, underscoring the risks of unsegmented convergence and the need for isolation strategies in legacy setups.

KEY TAKEAWAY

Contain risk, don't chase perfection.

Legacy systems may be difficult to modernise, but they are not impossible to protect. Containment, monitoring and segmentation allow organisations to manage risk while continuing to rely on critical infrastructure.



RES RECOMMENDS

Many legacy systems are connected to provide better telemetry and operational data. While that connectivity enables new insights, it also increases exposure. Start by taking stock of your environment:

- ✓ Map traffic flows and understand how systems interact
- ✓ Block both inbound and outbound internet access where feasible
- ✓ Apply time-of-day access rules to reduce attack windows
- ✓ Use segmentation to limit the blast radius of a compromise
- ✓ Check current operating system support and patch levels
- ✓ Consult vendors (where possible) for configuration guidance

You do not need to solve everything at once. A clear understanding of system dependencies and exposure is the first step toward sustainable risk reduction.



Building operational resilience through collaboration and capability

Technology alone won't solve the challenge of securing operational environments. One message came through clearly during the discussion: resilience hinges on how well teams align around risk, responsibility, and response.

When communication breaks down between IT and OT, so does progress. Security decisions stall. Gaps persist. But when teams collaborate with clear roles and shared context, they create the conditions needed to manage complexity and strengthen day-to-day resilience.



Insights and trends

Aligning IT and OT remains one of the most persistent roadblocks to operational resilience. Each team is driven by different priorities. IT focuses on reducing risk, while OT is responsible for keeping systems online. Without shared objectives, even well-designed strategies struggle to take hold.

Leaders at the lunch shared how they're addressing this disconnect through more deliberate collaboration. Joint playbooks, shared reporting and scenario planning are helping create a common language and a clearer path to action.

This alignment becomes even more important when internal capability is stretched. In these cases, the right external support can bring both operational awareness and technical depth that neither team can fully provide alone.

Convergence literacy is also gaining ground. Teams that understand both the operating environment and the threat landscape are better positioned to design security controls that are not just technically sound, but operationally practical.



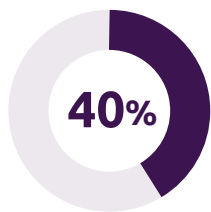
“When OT and IT actually sit down and work through scenarios together, you get a shared understanding. You start seeing gaps not as blame points but as opportunities to build trust. That’s what resilience really looks like.”

– BEN HOPPER,
MANAGING DIRECTOR,
RES. BUSINESS IT

Collaboration and resilience by the numbers



52% of organisations overhauled their IT security collaboration processes in 2024, focusing on cross-functional alignment to bridge IT/OT silos and build shared resilience.



40% fewer security incidents occur in OT environments among organisations with collaborative IT and OT teams, demonstrating the impact of cross-functional alignment on shared priorities and response.



62% fewer disruptive security incidents are reported by organisations that effectively connect IT and OT teams through cross-training and joint planning, enhancing overall operational resilience.

KEY TAKEAWAY

Align people before technology.

Resilience is shaped by culture as much as capability. The organisations that succeed in securing OT environments are the ones that invest in alignment across people, priorities and process.



RES RECOMMENDS

Most operational environments have developed over time. There is rarely a clean slate or ideal moment to begin. Progress depends on steady, collaborative effort rather than perfect conditions.

- ✓ Build alignment by clarifying roles and expectations early
- ✓ Run cross-functional exercises to test coordination and response
- ✓ Encourage ongoing dialogue between technical and operational teams
- ✓ Identify where capability gaps exist and bring in trusted support
- ✓ Make business priorities central to all decision-making
- ✓ Focus on incremental improvements that build momentum

Operational resilience is a long-term commitment. It starts with trust, continues through collaboration and becomes sustainable through consistent action.

Resilience in focus: Progress through trust, clarity and control

The session confirmed a familiar truth: securing operational environments isn't about perfection. It's about progress. As systems grow more complex and risks evolve, resilience comes from clear visibility, shared accountability and decisions that balance security with real-world constraints.



“These conversations are essential. It can feel isolating managing these environments day to day, so hearing how others are approaching the same challenges helps you think differently and move forward.”

– BEN HOPPER,
MANAGING DIRECTOR,
RES. BUSINESS IT

Five principles for strengthening OT security	1. Build alignment by clarifying roles and expectations early	2. Focus on controls that support uptime, not just compliance
	3. Isolate and monitor legacy systems instead of rushing to replace them	4. Clarify roles between IT and operations to close visibility gaps
		5. Prioritise small, continuous improvements over big-bang projects



LOOKING AHEAD

While operational environments may never be simple, securing them doesn't need to be overwhelming. This roundtable highlighted the value of practical conversations. Not just about technology, but about the people, processes and decisions that drive change.

RES. Business IT will continue to support these conversations and the organisations leading them, helping clients take meaningful steps forward with clarity, confidence and control.

Cyber and ICT services for OT environments

Protect your critical infrastructure with a technology partner that understands operational risk. RES helps businesses improve visibility, reduce complexity and secure their OT environments without compromising uptime.





RESIT.COM.AU

- ✉ sales@resit.com.au
- ✉ support@resit.com.au

☎ (07) 3513 8900

📍 2A, Level 2, 50 McDougall St
Milton, QLD 4064

CONTRIBUTORS

Ben Hopper – RES Business IT
Paul Black – RES Business IT
Eloise Pearce – RES Business IT
Tim Gray – Unique Metals Laser
Des Woolfield – Australian Country Choice
Luke Smith – Harmony Gold

Beau Millhouse – Reward Hospitality
Simon Scully – Sealy Australia
Jarad Gibson – Priestley's Gourmet Delights
Josh Alcock – Fortinet
Matt Harrison - Ellerslie Farms