

When a security budget is under pressure, cabling can look like an easy item to defer. It is often tucked into a fit-out, a maintenance line or a general infrastructure refresh, while firewalls and endpoint detection platforms get their own visible place in the security plan. That distinction is understandable, but it is misleading.

Structured cabling, patching and switching are part of the environment those security controls rely on. If the physical network is unreliable, poorly documented or incapable of supporting sensible segmentation, security tools cannot deliver their full value. The right conversation with management is not “we need to tidy up cables”. It is “this infrastructure investment reduces operational and cyber risk, and gives our existing controls a dependable foundation”.

That is the risk explanation executives need: what can fail, what the consequences are, and how the proposed work changes the likelihood or impact. This is not an argument for spending money on cables for their own sake. It is an argument for treating the physical network as part of the organisation’s security architecture.

Start with the business risk, not the cable

Most managers do not need a technical tour of cable categories or switch features. They need to understand how a weakness affects service delivery, safety, compliance or recovery. Translate the network problem into outcomes they recognise:

- **Unplanned outage:** a damaged link, overloaded switch or undocumented patch change can interrupt a business-critical service.
- **Security blind spot:** a fault or workaround can disconnect a device from monitoring, logging or the intended security controls.
- **Loss of containment:** an inadequate switching design can make it harder to keep guest, corporate, operational technology and management traffic separate.
- **Slow incident response:** when nobody knows what a port connects to, responders waste time tracing connections instead of containing the incident.
- **Costly recovery:** emergency investigation, temporary equipment and after-hours labour usually cost more than planned remediation.

Use a specific example from your own environment. “The patch panel is untidy” is weak. “We cannot reliably identify which switch port serves the building-management controller, so a fault or suspected compromise could delay isolation and affect building operations” is a risk explanation. Keep it factual and avoid overstating what an attacker could do. Credibility matters more than drama.

Physical infrastructure is part of cybersecurity

Cybersecurity is often described in terms of software, identities and policies. But digital traffic still travels through physical links and equipment. A network port, patch lead, switch and cable pathway are not outside the security boundary simply because they are mounted in a cabinet or ceiling.

Physical access can create security consequences. Someone who can reach a network outlet or an unsecured communications cabinet may be able to connect an unauthorised device, disrupt a link or interfere with a service. Poorly controlled patching can also put a device on the wrong network. The precise risk depends on access controls, switch configuration and the services involved, but the principle is straightforward: physical infrastructure affects who can connect, what they can reach and whether activity can be observed.

This is why cabling should not be dismissed as “just plumbing”. A water pipe does not decide which department receives its contents; a network connection can determine which systems and data a device can communicate with. The physical path is part of the control environment.

Faults create outages and security blind spots

A physical-layer fault is commonly treated as an availability problem: a link drops, a port flaps or a device becomes unreachable. It can also create a security problem. When a connection is unstable, teams may introduce temporary workarounds, move devices to spare ports or bypass intended paths to restore service. Unless those changes are controlled and recorded, they can weaken segmentation and monitoring.

Faults can also make security telemetry incomplete. A security team may see a device disappear from an endpoint detection platform and assume it has been shut down, when in fact its network connection has failed. A sensor may stop receiving traffic, or a monitoring system may lose visibility of a part of the network. In an incident, that ambiguity makes it harder to distinguish a technical fault from deliberate interference.

The operational question is not only “does the link work?” It is “can we tell when it does not, identify what is connected, restore it safely, and confirm that security controls still apply afterwards?” Good records, clear labelling, appropriate testing and a maintainable design all help answer that question.

Segmentation depends on capable switching and correct design

Management may hear that the organisation needs network segmentation and assume it is primarily a firewall purchase. Firewalls are important, but segmentation is a design outcome, not a box you buy. It depends on understanding the traffic flows, choosing appropriate boundaries and configuring the switching and routing infrastructure to enforce them.

For example, separate networks for corporate users, guest access, servers and operational technology may require capable switches, correctly configured VLANs, controlled routing and suitable security policies. The cabling and patching must connect devices to the intended ports and locations. If ports are undocumented, equipment is unsupported or the topology is unclear, the design becomes harder to implement and maintain reliably.



That does not mean every organisation needs the newest hardware or a complicated architecture. It means the equipment must support the controls the organisation has chosen, and the design must be understood by the people operating it. A flat network where everything shares one broadcast domain is not automatically a breach,

but it can increase the potential reach of a compromised device and make containment more difficult. Segmentation limits unnecessary paths and helps teams apply controls where they matter.

Vendors such as Cisco, Garland and MOXA serve different parts of the networking market, including enterprise and industrial environments. The useful management discussion is not a brand comparison. It is whether the proposed equipment is fit for the operating environment, supportable over its lifecycle, compatible with the security design and documented well enough to manage at 2am when something fails.

ACSC guidance needs sound foundations

Australian organisations often use Australian Cyber Security Centre (ACSC) guidance as a reference point for improving cyber resilience. Guidance on areas such as network architecture, access control, asset management and incident response is much easier to put into practice when the underlying network is known, supportable and properly configured.

That does not mean [cyberdaily](#) ACSC guidance prescribes a particular cable type, switch brand or fit-out. It means practical security measures depend on reliable foundations. You cannot confidently manage network access if you do not know what is connected. You cannot consistently enforce separation if the switching design is unclear. And you cannot respond efficiently if the physical path from a device to the network is a mystery.

Present this as an enabler rather than a compliance shortcut. A cabling and switching project does not, by itself, make an organisation compliant or secure. It can remove obstacles that prevent security controls from being applied and verified.

Make the investment case measurable

A convincing security budget request connects the work to risk reduction and operational value. Avoid relying on vague claims such as “the network is old” or “best practice says we should upgrade”. Show what is known, what is uncertain and what the proposed investment will improve.

Management concern Evidence to provide Outcome to describe Service continuity Fault history, outage duration, unsupported components and critical links Fewer avoidable interruptions and a clearer recovery path Cyber exposure Unsegmented areas, unknown connections, unmanaged switches or gaps in monitoring Reduced unnecessary access and better visibility of connected assets Incident response Time taken to identify ports, devices and affected areas during tests or incidents Faster, more controlled investigation and containment Lifecycle cost Support status, repeat call-outs, temporary fixes and maintenance effort More predictable support costs and less dependence on emergency work

Where possible, include a baseline: number of unidentified outlets, switches without current support, repeat link faults, or time required to trace a connection. Then define what “done” means. That could include updated drawings, labelled patch panels, tested links, a switch inventory, documented network boundaries and a process for approving changes.

Separate essential remediation from optional enhancement. A damaged link serving a critical system may need immediate attention; a complete replacement of a functioning installation may be a longer-term lifecycle decision. Phasing the work can make the request easier to approve while ensuring urgent risks are not buried inside a large capital project.

Explain the cost of doing nothing fairly

“Do nothing” is still a choice, but it should be compared honestly. Estimate the likely operational impact using the organisation’s own data: previous outage costs, recovery hours, service-level commitments and the value of staff time. Include uncertainty rather than presenting a speculative breach figure as fact.



Also consider the cost of repeated small fixes. A handful of unlabeled patch leads may appear harmless, but across a site they can add time to every fault investigation and increase the chance that a rushed change affects the wrong service. I keep a label maker in my laptop bag because the label often saves more time than the tool. More seriously, mystery cables are a security smell: they indicate that the organisation may not know what its network is carrying.

Unmanaged switches in production deserve particular attention. They can make the topology harder to see and limit the organisation’s ability to apply or verify controls consistently. The response is not necessarily to replace every device at once. First establish where they are, what they support and whether a controlled alternative is required.

A practical way to present the request

Keep the management paper brief enough to read, but specific enough to decide. A useful structure is:

1. **State the business objective.** For example, maintain critical services while improving the organisation’s ability to contain and investigate network incidents.
2. **Describe the current exposure.** Use verified findings: undocumented connections, recurring physical faults, unsupported switching or limits on segmentation.
3. **Explain the consequence.** Link each finding to availability, visibility, containment, recovery time or a relevant operational obligation.
4. **Set out the proposed work.** Define the sites and services in scope, the standards of documentation and testing, and any required switching changes.
5. **Show the options and trade-offs.** Compare urgent fixes, phased remediation and full replacement, including operational disruption and lifecycle support.
6. **Measure the result.** Agree how you will verify the work: test records, updated diagrams, port labels, inventory accuracy and successful segmentation checks.

Bring it back to resilience

The strongest case for cabling as a security spend is not that every old cable is a cyber threat. It is that physical infrastructure determines whether the organisation can connect systems safely, maintain availability, enforce network boundaries and see what is happening.

Good infrastructure investment makes firewalls and endpoint detection platforms more effective by giving them a network that can be understood and operated. It supports the practical application of ACSC guidance without pretending that cabling alone solves cybersecurity. And it helps staff respond when something breaks, whether that is an accidental fault, a failed component or a suspected incident.

So frame the decision around risk, evidence and resilience. Ask what the organisation needs to keep running, where the current network makes that difficult, and what a safer, supportable design will change. Then make sure the result is tested, labelled and documented. Because at 2am, when a critical link fails, nobody wants to start by asking where the other end of the mystery cable goes.