

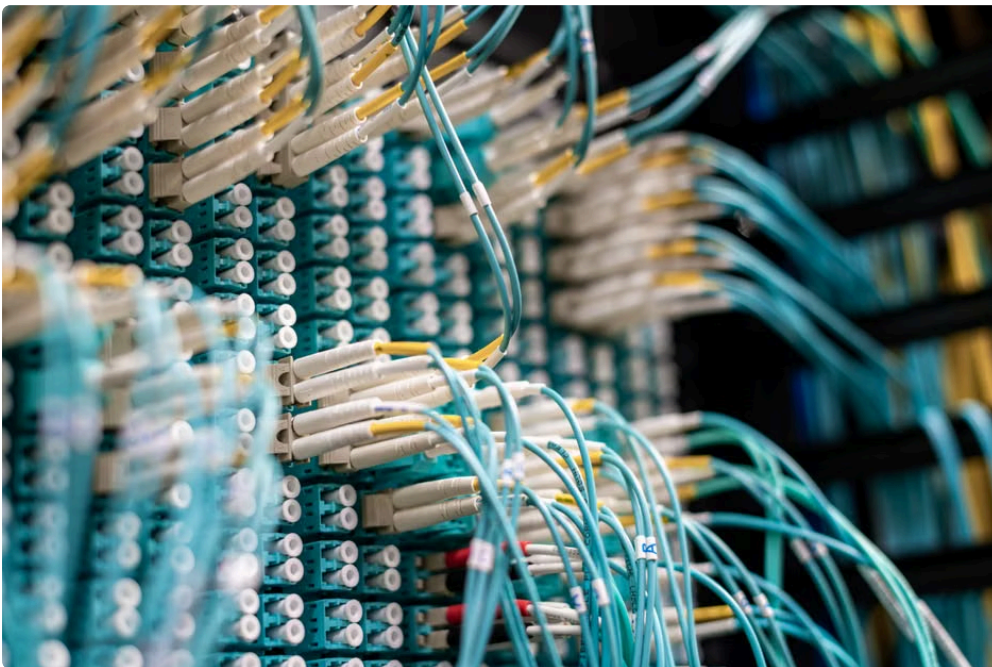
Firewalls, endpoint detection platforms and carefully designed access policies are essential security controls. But they cannot protect a network path they cannot see, or reliably enforce rules on a device that has been connected around them. When someone can reach network cabling, patch panels, cabinets or switches, physical access vectors can turn a well-intentioned logical design into something quite different.

This is not an argument against logical security. It is a reminder that logical controls depend on physical infrastructure. A network is built from devices, links and locations as well as rules and configurations. If those foundations are poorly protected, a logical control bypass may be as simple as changing which port connects to which device—or introducing an unapproved device into the path.

In office fit-outs, industrial environments and corporate networks, the warning signs can look mundane: exposed cable runs, unlabelled patch panels, an unmanaged switch tucked under a desk, or a connection that nobody is sure where it goes. Yet those are not merely housekeeping problems. They can create security blind spots, disrupt segmentation and make an incident harder to detect and contain.

Physical infrastructure is part of cybersecurity

It is tempting to treat cabling as “just plumbing”—the passive stuff that supports the important work done by firewalls and security software. That distinction does not hold up in practice. The cable is the path between a user, a switch, a server and the controls intended to govern their communications. If that path is changed, interrupted or extended, the security design may change with it.



Consider a network intended to keep visitors, corporate users and operational technology (OT) separate. The separation may rely on switch ports assigned to different virtual local area networks (VLANs), with routing rules and firewalls controlling traffic between them. If a person can access the relevant patching or switch ports, the physical arrangement may allow a device to be connected to the wrong segment, or an unauthorised device to be introduced. The firewall may still be operating exactly as configured. The weakness is that traffic has entered a different part of the network than the designers expected.

That is the core of a logical control bypass: the policy exists, but a physical change alters the route, access point or device to which the policy applies. The right response is to treat rooms, cabinets, outlets and cable routes as part

of the security boundary—not as background facilities work.

How physical access vectors undermine controls

Physical access does not automatically mean an attacker can take control of a network. Outcomes depend on the architecture, port configuration, authentication, monitoring and the access available. But reachable infrastructure can create opportunities that are absent from a purely remote attack. Common risk areas include:

- **Uncontrolled network ports:** A live outlet in a public or shared area may allow an unapproved device to connect, especially if port access is not restricted or monitored.
- **Accessible patch panels:** Unlocked cabinets and unclear labelling make it easier for authorised staff to make mistakes—and for unauthorised people to tamper with connections without attracting attention.
- **Unauthorised switches:** A small unmanaged switch can extend a connection to several devices, obscure what is attached and make it harder to apply or verify the intended port-level controls.
- **Changed or undocumented patching:** A move, addition or change can accidentally place a device in the wrong segment, or leave a connection in service after its business purpose has ended.
- **Accessible cable runs:** Cables routed through public areas, ceiling spaces or shared risers may be more exposed to damage, interference or unauthorised handling than the network owner realises.

Physical access vectors are not limited to malicious actions. A contractor may connect equipment to a convenient port without understanding its security implications. A rushed office move may reconnect a workstation to the nearest available outlet rather than its approved one. A fault may prompt a temporary workaround that remains in place for months. Good security design accounts for both deliberate tampering and ordinary human error.

Physical faults create outages and security blind spots

A damaged or poorly managed cable is first noticed as an availability problem: intermittent connectivity, packet loss, unexpected link changes or a complete outage. But the same fault can also degrade the quality of security monitoring. If a sensor, logging connection or security appliance loses connectivity, defenders may have less visibility precisely when the network is behaving unexpectedly.

Physical faults can also make network behaviour difficult to interpret. An undocumented switch might introduce additional links or devices. An incorrectly patched connection may cause traffic to traverse an unexpected route. A cable that is intermittently failing can produce repeated reconnects, making a legitimate fault look like a suspicious event—or concealing a meaningful change among a noisy stream of alerts.

This matters for incident response. Investigators need to understand what was connected, where it was connected, and what changed. If the patching is unlabelled and the topology exists only in somebody's memory, response teams can lose valuable time tracing the basics. When an incident is active, "which cable is this?" is not a question anyone wants to answer by pulling connections at random.

Physical faults can therefore create two related problems: service interruption and loss of confidence in the network picture. Resilience and security depend on the same discipline—documented layouts, controlled changes, sensible monitoring and equipment that can be identified quickly.

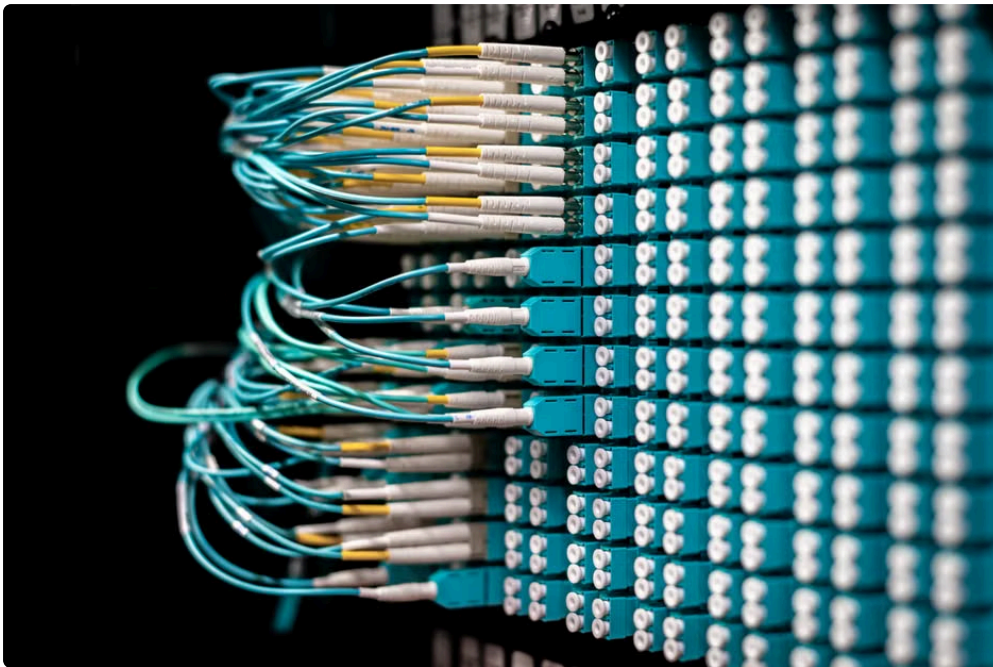
Segmentation depends on capable switching and correct design

Segmentation is often described in terms of VLANs, subnets and firewall rules. Those are important, but segmentation also depends on the switching infrastructure enforcing the design correctly. A network drawing that

shows separate zones is not proof that the deployed network actually keeps them separate.

Good design starts with clear requirements: which users and systems need to communicate, what should be isolated, and where traffic must be inspected. Those requirements then need to be reflected in the switch configuration, port assignments, routing, firewall policy and monitoring. The physical port and the device connected to it are part of this chain.

Capable, managed switching gives network teams the visibility and control needed to support that design. Features vary by platform, but may include port security, access control, VLAN enforcement, logging and controls for unused ports. These capabilities must be configured, tested and maintained. Buying capable equipment without establishing operational ownership is not a security strategy.



Vendors such as Cisco and MOXA operate in different parts of the networking market, including environments with differing performance, management and operational requirements. The important question is not the logo on the front of a switch. It is whether the selected equipment is suitable for the environment, can enforce the intended design, is supported, and can be monitored by the people responsible for it. In industrial settings, this assessment should account for availability, environmental conditions and the consequences of a change to production traffic.

For cable management and physical infrastructure, suppliers such as Garland may form part of a broader deployment. Regardless of supplier, the outcome depends on sound installation practice: protected routes, clear identification, appropriate cabinets, documented patching and controlled access. A neat cable tray does not create segmentation by itself, but a chaotic one can make mistakes and unauthorised changes much harder to spot.

Design element Security question Practical evidence Switching Can each port enforce its intended role? Approved configuration, port inventory and change records Patch panels Can a connection be identified and verified? Consistent labels that match current diagrams Cable routes Can unauthorised people reach or alter them? Protected routes and controlled access to risers and cabinets Monitoring Would an unexpected connection or link change be noticed? Switch logging, alerting and documented response procedures

How firewalls and endpoint detection fit in

Firewalls remain valuable for controlling traffic between zones and inspecting connections at defined boundaries. Endpoint detection platforms help identify suspicious behaviour on supported hosts. Neither should be expected

to solve every physical-layer problem.

A firewall can enforce policy only on the traffic that reaches it. If an unexpected connection changes the path or places a device on a segment with different controls, the firewall may not see the traffic it was meant to govern. Similarly, an endpoint detection platform can provide useful signals from managed, supported devices, but it will not necessarily detect an unmanaged switch or a physical change to a patch panel.

The strongest approach is layered. Physical safeguards reduce opportunities for tampering. Managed switching helps enforce and report network access. Firewalls control permitted communications between zones. Endpoint detection platforms add visibility on endpoints. Network monitoring and asset inventories help identify discrepancies across the whole environment. Each layer has a defined <https://www.cyberdaily.au/strategy/14271-why-physical-network-infrastructure-is-the-overlooked-foundation-of-your-cybersecurity-strategy> role, and none should be treated as a substitute for the others.

ACSC guidance needs solid network foundations

The Australian Cyber Security Centre (ACSC) publishes guidance intended to help organisations improve their cyber security. Applying such guidance effectively depends on the environment in which it is implemented. Controls that assume reliable asset knowledge, managed network access, appropriate separation and effective monitoring are difficult to sustain on top of an undocumented physical network.

That does not mean an organisation must perfect every cable before improving its security. It means the network foundation should be part of the implementation plan. Confirm what is connected, identify who owns each area, document the current topology, and address obvious exposure as controls are introduced. Where OT or other sensitive systems are involved, changes should be risk-assessed and coordinated with operational owners. A security improvement that causes an unplanned outage is not a successful outcome.

Guidance should be applied in context and checked against current ACSC publications and the organisation's requirements. The key point is straightforward: policies and technical controls need an infrastructure that can support them. If the underlying connectivity is unknown, the organisation cannot confidently demonstrate that the intended controls are working.

A practical programme for reducing risk

Start with the physical facts, then connect them to the logical design. A focused review can reveal issues before they become an incident:

1. **Inventory the network:** Record switches, patch panels, cabinets, outlets and critical cable routes. Identify equipment owners and the support status of each device.
2. **Trace and label connections:** Ensure labels are consistent at both ends and match diagrams. Retire mystery cables only after their purpose has been checked; guessing can create its own outage.
3. **Review physical access:** Assess who can reach communications rooms, cabinets, risers and exposed cable runs. Use proportionate locks, access records and visitor or contractor procedures.
4. **Check port controls:** Review unused ports, edge-port configuration, authentication and monitoring. Ensure exceptions are documented, time-bound where possible and approved by an owner.
5. **Find unmanaged equipment:** Look for unauthorised switches and other network devices. Remove them through a controlled process, and give staff a straightforward way to request approved connectivity.
6. **Validate segmentation:** Compare the intended architecture with live switch configurations, routing and firewall policy. Test expected and prohibited paths in a controlled manner.

7. **Connect physical events to response:** Define how teams will investigate unexplained link changes, cabinet access, new devices and reports of damaged or moved cables.

Ask the 2am question

Every network change should be assessed against a practical question: what happens at 2am when this fails? If a critical cable is damaged, can the right team identify it quickly? If a switch is added without approval, will anyone notice? If segmentation stops behaving as designed, can responders establish which devices and paths are affected?

The answers rely on more than a firewall rule or a diagram. They rely on accessible documentation, capable and managed equipment, clear ownership, and people who know how to make a safe change under pressure. A label maker in the laptop bag may seem low-tech, but accurate labelling can save time, reduce mistakes and give incident responders a better starting point.

Conclusion

Physical access to cables does not magically defeat every security control. It can, however, change the conditions those controls depend on. Exposed cable runs, accessible patch panels, unmanaged switches and undocumented connections can create a logical control bypass, weaken segmentation and obscure what is happening on the network.

Cybersecurity and physical infrastructure are not separate disciplines. Reliable segmentation, effective firewalls, useful endpoint detection and meaningful incident response all depend on a network whose physical layer is understood and controlled. Protect the routes, manage the switching, document the connections and test the design as it exists—not just as it appears on paper. Mystery cables are not merely untidy. They are a security smell worth investigating.