PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 11 • ISSN: 3136-2729

EDITORIAL

Cybersecurity as a National Infrastructure Problem, Not Just an IT One

When a bank, a power utility, and a hospital network all stumble in the same week from the same class of attack, the postmortem can't stop at "patch the servers." It has to ask why cybersecurity was ever treated as somebody else's department.

Keywords: Cybersecurity; Critical Infrastructure; National Security; Digital Policy; Pakistan

By **Junaid Haseeb Malik** | **Ontario,** Canada | Published: July 2026
editorial@paktechtoday.com | Position: Cybersecurity Expert

Introduction

In the space of a single year, Pakistani banks have paused card transactions after a suspected breach, a major telecom operator has confirmed a data leak, and provincial hospitals have reported ransomware locking up patient records. Each incident was handled the same way: quietly, defensively, and by the technology department. None of them should have been treated as an IT problem alone.

That instinct — route the crisis to IT, patch what broke, issue a brief statement, move on — made sense when computers were back-office tools that processed payroll and stored files. It makes far less sense today, when software runs the electricity grid, the payments system, the water utilities, the ports, and the hospitals that keep a country functioning. A ransomware operator does not need to blow up a substation to cause a blackout; disabling the software that manages load balancing will do.

Pakistan is not unique in facing this shift, but it is unusually exposed to it. Rapid digitisation of banking, the rollout of e-government services through platforms tied to NADRA, and heavy reliance on a small number of telecom and cloud providers have concentrated risk faster than institutions have built the capacity to manage it.

> ***A breach in a power-distribution control system is not an IT ticket — it is an outage, a public-safety event, and potentially a diplomatic incident, all at once.***

Why "Call IT" Is the Wrong Reflex

Treating a cyberattack as an IT incident assumes the damage is contained to servers and data. But critical systems today run on what security engineers call OT — operational technology: the industrial control systems that open valves, route electricity, and manage rail signals. Much of this equipment was built decades ago, designed for reliability and physical safety, not for a world of remote attackers. Bolting modern IT networks onto it, for the sake of efficiency and remote monitoring, has quietly connected control-room equipment to the internet without giving it the internet's defences.

The interdependencies compound the problem. A prolonged power outage does not just switch off lights; it can take down water pumping stations, mobile network towers, and the data centres that banks depend on. An

attack that starts in one sector rarely stays there. Pakistan's own experience with load-shedding has already shown how failure in one utility cascades into hospitals, factories, and telecom infrastructure — a cyber-triggered version of the same failure would spread just as fast, and with less warning.

Add to this a supply chain problem: much of the hardware and software running Pakistani infrastructure, from network switches to SCADA systems, is imported, and few buyers have the leverage or expertise to independently audit it for security. A vulnerability discovered in a vendor's product overseas can sit unpatched in a Pakistani substation or bank for months, because no single IT department owns responsibility for tracking it.

The Cost of Getting This Wrong

Global incidents offer a preview of what infrastructure-grade cyberattacks look like. The 2021 ransomware attack on the Colonial Pipeline in the United States shut down fuel supply along the East Coast for days, not because the pipeline's physical machinery was destroyed, but because the billing and scheduling systems it depended on were taken offline. Ukraine's power grid has been the target of at least two attacks explicitly designed to cause blackouts through control-system manipulation, not conventional weapons.

For Pakistan, the equivalent exposure sits in its financial sector, which has already absorbed the reputational and operational cost of high-profile breaches at major banks; in its telecom backbone, which now carries both consumer traffic and government service delivery; and in energy-sector infrastructure tied to CPEC investments, where any disruption carries a diplomatic as well as a domestic dimension. Industry estimates consistently put the global cost of cybercrime in the trillions of dollars annually — a burden that falls hardest on economies with the least redundancy built into their systems.

The deeper cost is one of trust. Once citizens stop believing that digital banking, e-government portals, or hospital record systems are safe to use, the years of investment in digitising those services start to unwind — pushing people back toward slower, less transparent, and more corruption-prone paper processes.

What's Next?

Fixing this requires treating cybersecurity the way countries treat electricity, water, or food supply: as critical infrastructure with its own regulatory home, its own minimum standards, and its own budget line — not a cost centre buried inside each ministry's or company's IT department. A national critical-infrastructure protection framework, with mandatory incident reporting and baseline security requirements for power, telecom, banking, and health-sector operators, would be a starting point.

That framework needs teeth: a properly resourced national CERT with the authority to coordinate response across sectors during an incident, rather than each operator managing its own crisis in isolation. It also needs people — a sustained pipeline of OT-security talent, since the skills needed to secure a power grid's control systems differ from those needed to secure a bank's website, and Pakistan currently trains far more of the latter than the former.

None of this is glamorous work, and none of it will show up in a product launch or a quarterly earnings call. But the alternative is finding out, during an actual blackout or bank outage, that the responsibility for stopping it was never clearly assigned to anyone. Cybersecurity stopped being an IT problem the day critical infrastructure went digital; policy, budgets, and accountability structures need to catch up to that fact before an adversary forces the issue.

About the Author

The Junaid Haseeb covers information security, technology policy and digital infrastructure of many tech setups in Canada.