

Avoiding Common Pitfalls in Cybersecurity Transformation Projects

A Practical Playbook

PROACTIVE[™]
Enhancing Digital Experience



You don't fix your roof when it rains.
You fix it when the sun is out.

If Your Transformation Project Needs a Rescue Plan, Read This
Before You Spend Another Rupee

Cybersecurity programs fail silently. Not because they lack funding, but because they ignore execution. You bought the licenses. You deployed the tools. You even got a compliance certificate. But six months later, your Nagpur plant is running the same flat VLAN. Your VPN logs still overwhelm your SOC. And your CFO still asks what ROI cybersecurity delivers.

Transformation without clarity is expense. This playbook draws from real experiences across Indian enterprises, those that stumbled and those that recalibrated successfully.

1. Pitfall: Skipping the Audit Before Going Zero Trust

Raj Malhotra, the Head of IT Infrastructure at a Pune-based manufacturing group, launched a Zero Trust pilot last April. The objective was to harden east-west traffic and remove implicit trust from the factory network. But 30 days into implementation, a security incident revealed that several OT devices had been left out of the scope. These devices, unpatched, unmanaged, and undocumented, were connected to the same VLANs as user endpoints. The remediation cost ran into tens of lakhs.

Fix: Define response ahead of detection.

You cannot modernize what you have not mapped. Most cybersecurity programs jump to vendor shortlists before assessing their own environment. This leads to blind spots: shadow assets, unmanaged SaaS usage, third-party API calls, and legacy OT infrastructure that has never been catalogued.

Start with a Zero Trust maturity audit. This gives you a clear view of where trust is implicit, which identities are over-permissioned, what data flows are uncontrolled, and which devices are not governed. Skip this, and you are building Zero Trust on unverified ground.

2. Pitfall: Overlooking Business Context in Threat Models

Meera Srinivasan, CISO at a Bengaluru pharma company, ran a textbook threat modelling exercise. Yet, when ransomware hit their export logistics platform, it exploited a completely ignored workflow that passed data to third-party clearing agents via FTP. The model had not considered real-world business exceptions.

Fix: Align security threat models to operational flows.

Security teams often treat threat modelling as a checkbox exercise. Diagrams are clean, but real workflows are messy. You need to capture edge cases, third-party workflows, unmanaged devices, and tribal practices.

Conduct threat modelling in the presence of business teams. Map actual data flows, not just system diagrams. Include supplier integrations, outdated protocols, and nonstandard user behaviours.

3. Pitfall: Assuming Compliance Equals Coverage

Ajay Verma, IT Lead at a Delhi-based auto parts supplier, had proudly secured ISO 27001 certification across all plants. Policies were printed, audits were clean, and leadership was confident. But during a surprise internal red team test, attackers breached the ERP interface through expired credentials issued to contract employees. None of it showed up in the compliance report.

Fix: Treat compliance as a milestone, not an end-state.

Compliance frameworks focus on policies and process hygiene. They don't measure how well those policies hold up under actual threat behaviour. Real-world attacks exploit gaps between what's documented and what's practised.

You need active validation built into your cybersecurity operations:

- Run adversary simulations quarterly to test real resilience
- Use red teaming to uncover what compliance audits miss
- Track operational metrics like Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), not just audit checklists
- Audit controls in production environments, not just on paper

Your goal isn't a certificate. It's readiness.

4. Pitfall: Buying Platforms Without Integration

Vikram Shetty, Security Head at a Hyderabad-based BPO, signed off on a multi-crore security stack last year. The pitch was compelling: best-in-class SIEM, EDR, and XDR solutions, each with its own console, dashboards, and analytics.

By quarter two, Vikram's SOC team was drowning in alerts from six tools, all flagging anomalies but failing to link events. During an actual breach attempt, correlation took so long that the attacker had already exfiltrated data before containment even began.

Fix: Focus on interoperability from day one.

Most enterprises buy top-tier security platforms only to discover later that their tools do not talk to each other. One system detects lateral movement, another flags a suspicious login, but no layer joins the dots. The result: alert fatigue, fragmented visibility, and delayed containment.

Security telemetry must be stitched at ingestion. Signals from the network, identity, SaaS, and endpoints must align in real time. Choose solutions that prioritise native integrations, shared context, and open APIs. Correlation should be built-in, not bolted on.

What You Should Do:

- Consolidate detection signals early. Choose a SIEM that can natively ingest logs from identity, endpoint, and network layers.
- Design for shared context. Ensure user identity, device state, and network location flow through a common metadata layer.
- Test end-to-end visibility. During your POC, simulate a cross-layer breach to validate how fast your tools correlate alerts.

- Prioritize open platforms. Tools with restrictive APIs or closed ecosystems slow down response time and increase TCO.

Think like an adversary. They don't care what tools you own. They only care whether your telemetry systems talk to each other before the breach reaches critical mass.

5. Pitfall: Deploying MFA But Ignoring Credential Hygiene

Reena D'Souza, CIO at a Tier 2 auto parts exporter in Aurangabad, had deployed MFA across all employee endpoints. Audit reports looked great. But during a phishing simulation exercise, six users clicked on a fake invoice link and entered credentials, bypassing MFA via session hijack. Her team realized they had underestimated human error and weak password habits.

Fix: Harden your identity layer beyond MFA.

MFA alone is not a silver bullet. If employees reuse passwords, store them insecurely, or share credentials across apps, attackers will still find their way in. A malicious actor doesn't bypass your MFA, they just find a user who reused their password on a compromised site.

- Promote enterprise-wide adoption of password managers
- Monitor for credential reuse and unsafe storage practices
- Enforce periodic rotation of high-privilege credentials
- Pair MFA with conditional access and device posture checks

Good authentication hygiene closes the door on the softest attack vectors.

6. Pitfall: Leaving OT and Legacy Assets Unsegmented

Arvind Balan, CTO of a legacy textile machinery firm in Coimbatore, thought his plant was well-insulated from external threats. His team had implemented standard firewalls and endpoint detection in IT environments. But when a ransomware attack halted production for three days, the root cause was traced to an unmonitored PLC system in the OT network communicating with internet-facing devices. The incident made one thing painfully clear: his legacy systems were the weakest link.

Fix: Microsegment and monitor OT environments.

Legacy assets, from old PLCs to decade-old SCADA systems, often remain invisible to standard IT monitoring. They run outdated firmware, are rarely patched, and typically operate in flat networks with little or no segmentation. This makes them prime targets for attackers looking to move laterally or cause operational disruption.

You cannot secure what you do not see. A full asset discovery is the starting point. Use passive network monitoring to map communication patterns. Identify devices that talk unnecessarily to broader systems. Prioritize crown jewels such as production line controllers and isolate them.

- Deploy next-generation firewalls with deep packet inspection tuned to OT protocols like Modbus and DNP3
- Place unidirectional gateways at the boundary of critical control zones
- Use anomaly detection based on historical OT traffic, not generic IT heuristics
- Implement jump servers and dedicated access points for contractors, with strict session logging

Most importantly, work with operations teams. Security will only succeed in OT when it respects uptime, latency, and safety constraints. Think of segmentation as a safety valve, not just a compliance checkbox.

7. Pitfall: Focusing on Detection Without a Response Playbook

Nandita Kapoor, CISO of a mid-sized electronics OEM in Noida, discovered during a breach simulation that while her SOC could detect anomalous behaviour quickly, no one knew what to do next. Her team escalated the incident to senior leadership without clarity on roles, approvals, or technical steps. The confusion wasted precious minutes, and in a real-world scenario, the delay could have proven fatal.

Fix: Define response ahead of detection.

Detection is just the first half. Response is where the breach stops or spreads. Without predefined playbooks, teams scramble, escalate late, and act inconsistently.

- Draft attack-specific workflows covering ransomware, account takeover, and insider threats
- Assign roles, backups, and escalation thresholds
- Run quarterly tabletop drills with technical and non-technical stakeholders
- Pre-approve containment steps, so no one waits for legal or leadership sign-off

A mature SOC thinks in workflows, not alerts.

8. Pitfall: Underestimating SaaS Security Complexity

Deven Arora, CTO at a digital marketing firm in Ahmedabad, believed their SaaS footprint was secure because everything was behind SSO. But during a routine audit, they discovered over 200 unauthorized SaaS tools being used by different departments, many with full access to customer data. Worse, some tools had been granted OAuth access months ago and never reviewed.

Fix: Treat SaaS apps like internal systems.

SaaS apps bypass traditional perimeter controls. Most come with excessive permissions, weak sharing policies, and silent OAuth creep.

- Deploy CASB or SSPM solutions to audit SaaS risk posture
- Limit scope of third-party integrations through strict OAuth governance
- Apply zero-trust policies to SaaS access - user identity and device health both matter
- Enforce usage policies for sensitive actions such as file sharing or app installs

What runs in the browser can still compromise your network.

9. Pitfall: Ignoring Change Management in Large User Bases

Sonal Reddy, Head of IT Ops at a global shared services center in Chennai, deployed endpoint protection tools across 7,000 users in three weeks. The tech worked, but support tickets spiked 200 per cent. Teams complained about slow devices, blocked apps, and unknown alerts. The backlash forced her to roll back features and delay phase two by a quarter.

Fix: Bake change management into every rollout.

Users don't hate security. They hate surprises. Deploying tools without prep results in pushback, workarounds, and shadow IT.

- Communicate early with end-user groups. Explain the why before the how
- Offer opt-in pilots and use feedback loops to improve rollout
- Use internal champions to drive adoption in specific departments
- Track sentiment and incident data to validate adoption

Security outcomes improve when people don't feel like obstacles.

10. Pitfall: Neglecting Endpoint Visibility Across Contract Workers

Prakash Menon, CIO at a Bengaluru-based logistics company, assumed their endpoint security was solid until a contractor's device, used briefly at a remote warehouse, introduced malware that travelled through VPN tunnels and reached the billing system. The post-mortem revealed that third-party devices were never part of their visibility scope.

Fix: Extend endpoint visibility everywhere.

Your contractors, partners, and gig workers access the same apps and data. But do their devices meet your hygiene bar?

- Apply NAC or ZTNA policies that inspect device posture before access
- Issue containerised workspaces or VDI to untrusted devices
- Track every endpoint accessing sensitive data, regardless of ownership

- Review third-party access logs weekly, not quarterly

Endpoints are the new perimeter. Don't leave yours porous.

Final Word: From Insight to Impact

Most enterprises don't fail because of technology. They fail because execution breaks down in the middle. If this playbook exposed familiar gaps in your environment, you're not alone. Proactive has helped manufacturers, logistics majors, and ITeS companies across India harden their cybersecurity programs with clarity, speed, and measurable impact. Let's talk.

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us
at pro@proactive.co.in

 www.proactive.co.in

PROACTIVE[™]
Enhancing Digital Experience