Wired Together

The Case for Cross-Training in Networking and Cybersecurity

Executive Summary

This report examines the critical convergence of Networking and Cybersecurity, outlining the operational challenges that arise from this integration. With 75% of professionals now viewing these domains as integrated, cross-training has emerged as a strategic solution. Developing professionals with dual expertise is crucial for organizations to improve threat detection, streamline operations, reduce costs, and foster innovation.

Table of Contents

The Convergence Reality

The Integrated Landscape

Gone are the days when Network Engineers and Security Analysts could work in isolation. Today, these once-distinct domains have become inextricably linked—A reality confirmed by our recent industry survey, where **75% of professionals described Networking and Cybersecurity as either "completely integrated" (29%) or "highly interconnected" (46%). Just 7% still view them as separate disciplines.**

This convergence didn't happen overnight. Over the last decade, the boundary between these fields has steadily eroded. Cisco's 2025 Cybersecurity Readiness Index found that 88% of organizations plan to deploy network security solutions in the next two to three years. Several forces have driven this shift:

- **Widespread cloud adoption**
- **Remote work acceleration**
- **The explosion of IoT devices connecting to corporate networks**

The traditional network perimeter hasn't just changed—it's virtually disappeared, replaced by complex distributed systems where **security must be woven into the very fabric of the network.**

Key Organizational Challenges

Despite widespread acknowledgment of this new reality, organizations continue to struggle with its practical implications. INE conducted a survey of nearly 1,000 Networking and Cybersecurity professionals worldwide, and uncovered several pain points where Networking and Cybersecurity collide:

01 Knowledge gaps remain pervasive

Nearly one in five professionals (18%) identified knowledge gaps as their primary challenge—they simply lack adequate cross-functional expertise.

02 Threat landscape complexity continues to grow

Keeping pace with evolving threats presents a significant hurdle as each new attack vector requires coordinated responses across both domains.

03 Operational friction persists

The classic tension between security and operational needs remains unresolved, with 15% reporting difficulties aligning security policies with network performance requirements.

04 Resource constraints limit progress

Limited resources force tough choices between security investments and networking infrastructure upgrades, often resulting in compromises to both.

05 Talent shortages exacerbate problems

A persistent talent shortage makes it difficult to find professionals comfortable working across domain boundaries.

06 Organizational and communication barriers compound issues

Perhaps most telling, nearly a quarter of respondents pointed to organizational misalignment and communication breakdowns between departments, suggesting structural barriers to effective integration.

These findings point to a clear conclusion:

This report examines where Networking and Cybersecurity intersect most critically, explores the concrete benefits of cross-domain expertise, and provides practical guidance for building a more versatile technical workforce equipped to handle today's complex digital environment.

Organizations must break down the silos between Networking and Cybersecurity through strategic cross-training initiatives. Those that invest in developing professionals who can speak both languages will gain tangible advantages:

- **More effective threat detection**
- **Streamlined operations**
- **Reduced interdepartmental friction**
- **More resilient infrastructure**

The Challenge

Interconnectedness

Okay, They're connected.
So what?

Understanding that Networking and Cybersecurity are interconnected domains is only the starting point.
The real challenge emerges in daily operations where these fields continually intersect and occasionally collide, creating significant implications for:

- Organizational efficiency
- Security posture
- Business continuity

How Ready Are We?

Are professionals prepared to navigate where networking and cybersecurity collide?

33%
Very well / Extremely well prepared
Strong foundation for cross-domain collaboration and security

41%
Moderately well prepared
At risk of inefficiencies and slower incident response

26%
Slightly well / Not at all prepared
Major risk to org efficiency, security posture, and business continuity

Collision Points

When Network Engineers make **configuration changes without security considerations**, vulnerabilities emerge

When **Security Teams implement controls without understanding network architecture**, performance suffers

These **daily friction points impact everything** from routine maintenance to emergency incident response

According to IBM's 2023 Cost of a Data Breach Report, organizations with high levels of security/IT complexity face breach costs averaging $1.2 million higher than those with streamlined, integrated environments.

From a Security Professional's Perspective

Security professionals face these networking-related challenges:

01 Threat Surface Analysis
Must understand network architectures to identify vulnerable entry points

02 Traffic Analysis
Need networking fundamentals to distinguish between legitimate anomalies and threats

03 Implementing Controls
Without network engineering knowledge, they often propose controls that create bottlenecks

04 Forensic Investigation
Network evidence is crucial during incidents but requires appropriate skills

05 Vulnerability Assessment
Must identify risky network configurations

From a Networking Professional's Perspective

Security considerations impact virtually every aspect of network operations:

01 Configuration Management
Face numerous security implications with each change

02 Troubleshooting
Must distinguish between network problems and security control interventions

03 Network Design
Need to incorporate zero-trust principles and micro-segmentation from the planning stages

04 Compliance Requirements
Changes require verification against standards like PCI-DSS and HIPAA

05 Incident Response
Must rapidly implement containment measures during security incidents

Areas with Most Significant Overlap

Our survey identified these critical convergence points:

Network Monitoring

For Networking Professionals: Primary tool for tracking bandwidth, bottlenecks, and service availability

For Security Professionals: Reveals potential compromises through unusual traffic patterns

Cross-training benefit: Quickly distinguish between normal anomalies and genuine security incidents

Configuration Management

For Networking Professionals: Ensures performance, reliability, and operational stability

For Security Professionals: Represents potential vulnerability points when implemented incorrectly

Cross-training benefit: Configurations that maintain both security and functionality from day one

Security Monitoring

For Networking Professionals: Helps implement changes that don't trigger unnecessary alerts

For Security Professionals: Forms frontline defense but requires network knowledge

Cross-training benefit: Context-aware monitoring reduces investigation time from hours to minutes

Detection

For Networking Professionals: Understanding baseline behavior creates the foundation for spotting anomalies

For Security Professionals: Recognizing attack patterns requires translating indicators into impacts

Cross-training benefit: Sophisticated detection rules with fewer false positives

Firewalls

For Networking Professionals: Critical traffic control points affecting connectivity and performance

For Security Professionals: Primary enforcement mechanism for security policies

Cross-training benefit: Establishes ground rules that protect assets while maintaining necessary business flows

Access Control

For Networking Professionals: Ensures authorized systems can communicate effectively

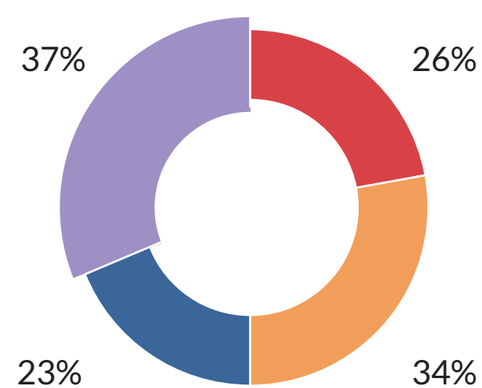
For Security Professionals: Prevents unauthorized access and limits attack surface

Cross-training benefit: Balance between protection and productivity

The Goal

Reduced Operational Friction Between Cybersecurity & Networking Teams

Our survey results reveal the current state of collaboration between these interconnected disciplines. This data paints a clear picture—while most organizations recognize the need for cross-functional cooperation, genuine integration remains elusive. The majority of professionals still operate in partial silos, creating inevitable friction points where these domains intersect.



Frequency of Cross-Specialty Collaboration Among Professionals

- Most of the time/Always
- About half the time
- Sometimes
- Never

Why Cross-Training Reduces Operational Friction

The persistent friction between networking and security teams creates tangible business problems that affect your bottom line. Cross-training addresses these challenges by transforming how these teams interact on four critical fronts:

01
Common Language, Faster Execution

Business Impact

Projects deploy faster with fewer delays. Changes are implemented correctly the first time, reducing rework cycles. Your organization brings new services to market more quickly with higher quality and fewer security compromises.

Problem

Networking and security professionals speak fundamentally different languages. Network engineers focus on throughput, latency, and routing protocols, while security teams discuss threat vectors, vulnerabilities, and attack surfaces. This terminology gap causes misunderstandings, delayed projects, and implementation errors.

Solution

Cross-trained professionals serve as translators between these worlds. They understand that a security concern about "lateral movement" translates to specific routing and segmentation requirements. They create documentation that both teams can interpret correctly the first time.

02
Balanced Decisions, Enhanced Reliability

Business Impact

System reliability and availability metrics improve dramatically. Unplanned outages decrease as changes succeed the first time. Emergency changes and rollbacks become the exception rather than the rule, preserving both business continuity and team resources.

Problem

Siloed decision-making creates a perpetual cycle of implementation, breakage, and emergency fixes. Security teams implement controls without understanding network impacts. Network teams make changes that inadvertently create vulnerabilities.

Solution

Cross-trained professionals anticipate the downstream effects of technical changes before implementation. They evaluate both security and performance implications simultaneously, breaking the implement-break-fix cycle.

Why Cross-Training Reduces Operational Friction (cont.)

03
Streamlined Operations, Cost Efficiency

Business Impact

Operational costs decrease through more efficient use of technical talent. Meeting time and coordination overhead reduce substantially. Teams spend more time innovating and less time firefighting, creating measurable financial benefits while accelerating security improvements.

Problem

Organizations waste countless hours on emergency remediation, failed implementations, and endless interdepartmental meetings. Technical resources spend more time navigating organizational boundaries than solving actual problems.

Solution

When teams understand both domains, the change management process transforms. Network changes arrive with security considerations already addressed. Security patches come with clear network implementation plans. Review cycles shrink dramatically.

04
Collaborative Culture, Talent Retention

Business Impact

Improved job satisfaction leads to better retention of experienced professionals. Team productivity increases as organizational friction decreases. Your organization develops greater resilience and adaptability, responding faster to emerging threats and opportunities without being paralyzed by internal silos.

Problem

Constant tension between security and networking creates toxic work environments, contributing directly to burnout, reduced engagement, and talent loss. Security teams feel ignored when recommendations aren't implemented correctly. Network teams grow frustrated when security requirements impede service delivery.

Solution

Cross-trained teams focus on collaborative problem-solving rather than blame assignment. Professionals with broader skill sets experience greater autonomy and effectiveness, solving problems holistically without endless handoffs.

The Solution

Cross-Training
Cross-Training Benefits

Cross-training professionals in both Networking and Cybersecurity delivers four key advantages that directly impact business outcomes:

01
Enhanced Threat Detection and Response

The Value

- **Comprehensive visibility** across network architecture and security implications
- Faster threat identification with **fewer false positives**
- Significantly **reduced incident response times**
- Improved **ability to contain threats** before they spread

Real-World Impact

"The average cost of IT downtime is $5,600 per minute - or $336,000 per hour."

- Gartner Research

Break down security silos with cross-tool integration

Cross-trained teams can act faster and more decisively

02
Operational Excellence

The Value

- Streamlined workflows with **fewer handoffs** between specialized teams
- More efficient change management with **reduced review cycles**
- Dramatically **fewer failed implementations** and **emergency rollbacks**

By the Numbers

Organizations with cross-functional teams report significant reductions in deployment delays

Emergency fixes and rollbacks decrease substantially with proper cross-domain expertise

Technical projects are completed on time and on budget more consistently

03
Cost Savings

The Value

- **Reduced downtime** from security incidents
- More **flexible staffing capability** across technical domains
- **Decreased reliance** on expensive emergency consultants

The Impact

Research from IBM shows that security system complexity was the top factor in increasing the cost of a breach

Cross-trained teams can help reduce these costs through more efficient incident response and remediation

Organizations report significant reductions in third-party emergency support costs

04
Innovation & Adaptability

The Value

- **Faster adoption** of emerging technologies that blend Networking and Security
- Ability to **implement cutting-edge solutions** requiring both skill sets
- **Better positioning** for evolving technology landscape and threat vectors

Strategic Edge

Faster incident response

Integrated Security & Network Ops

Support for Zero Trust & SASE

"Breaking down security silos and fostering more cross-team cooperation is essential for responding to the accelerating pace of cyber threats."

- CSO Online

Implementation Guide

Making Cross-Training Work in Your Organization

Step 01

Conduct a Skill Assessment & Gap Analysis

- **Start by mapping your terrain.** Identify where networking and security teams most frequently interact in your environment. Review recent incidents to find cases where cross-domain expertise would have made a difference. This creates your training priority map.
- **Evaluate your team's current capabilities.** Beyond technical assessments, use role-playing scenarios to reveal communication gaps between teams. Look for hidden tribal knowledge that hasn't been shared across domains.
- **Create personalized learning journeys.** Develop clear progression roadmaps showing how professionals can build cross-domain competencies. Establish mentorship pairs between networking and security specialists to accelerate knowledge transfer.

Step 02

Deploy Varied Training Methodologies

- **Balance formal and informal learning.** Sponsor targeted certifications that bridge networking and security domains, but don't stop there. Create internal certification programs specific to your environment.
- **Prioritize hands-on experience.** Implement dedicated lab environments where professionals can safely experiment. Create scenario-based challenges that require both networking and security expertise to solve.
- **Make learning experiential.** Establish job rotation programs where team members spend time in complementary roles. Create cross-functional project teams rather than siloed implementation groups.
- **Practice collaborative response.** Conduct regular exercises with mixed teams responding to simulated incidents. Create playbooks that define integrated roles and responsibilities rather than segregated workflows.

Step 03

Measure Impact and ROI

- **Track performance improvements.** Monitor incident response times before and after cross-training. Measure reductions in change management cycles and implementation rework. Watch project timelines and success rates improve.
- **Calculate business value.** Document direct cost savings from reduced downtime and emergency remediation. Capture efficiency gains from streamlined operations. Don't overlook retention value from increased job satisfaction and career growth opportunities.

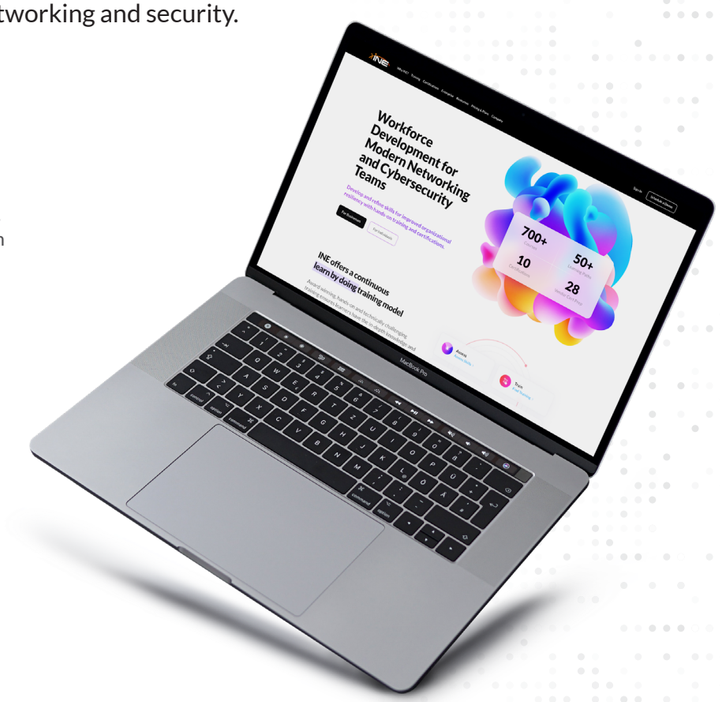
Step 04

Scale Your Success

- **Start with pilot programs.** Focus on high-priority areas to demonstrate value quickly. Use these early wins to secure executive sponsorship and additional resources. Build cultural reinforcement by recognizing and rewarding cross-domain expertise.
- **Deliver real value.** Remember that successful cross-training isn't just about technical skills—it's about transforming how your teams communicate, collaborate, and deliver value to the organization.

INE's Cross-Training Solution

Implementing effective cross-training requires the right partner. INE offers a comprehensive solution specifically designed to address the critical intersection points between networking and security.



Targeted Learning Experience

INE's approach stands apart through:

- ✓ **Domain-Bridging Curriculum** that directly addresses key overlap areas: monitoring, firewalls, configuration management, detection, and access control
- ✓ **Role-Specific Pathways** customized for both networking and security professionals
- ✓ **Real-World Scenarios** built around actual friction points organizations experience

Practical Skills Development

Our "learn by doing" model delivers:

- ✓ **Immersive Environments** through the Skill Dive platform that simulates enterprise networks
- ✓ **Industry-Standard Tools** used in production environments
- ✓ **Respected Certifications** that validate cross-domain expertise, not just siloed knowledge

Measurable Business Results

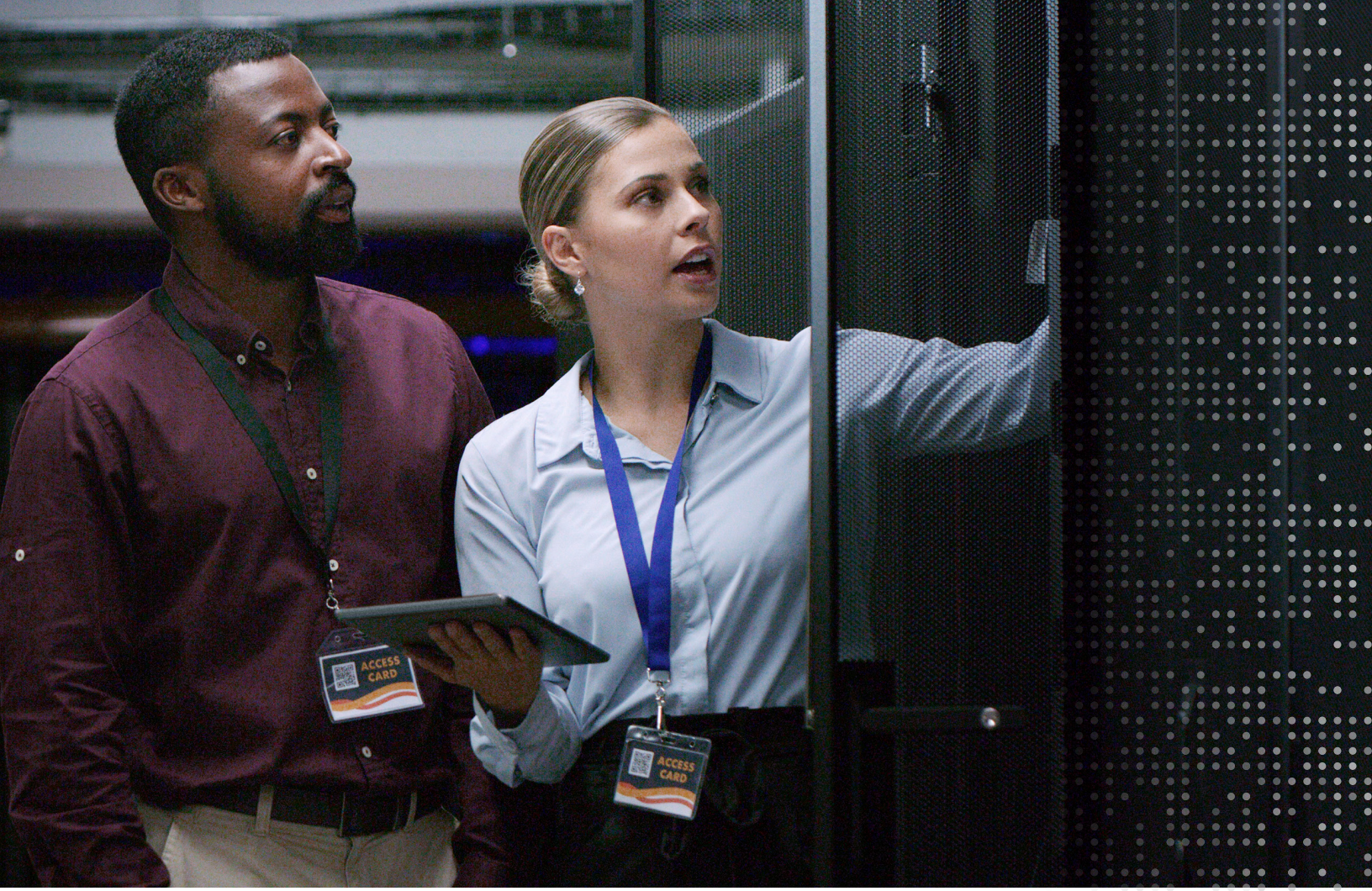
Organizations implementing INE's solutions report:

- ✓ **Faster operations:** Reduced incident response times and streamlined change management
- ✓ **Enhanced Collaboration:** Less friction between departments, especially during critical incidents
- ✓ **Career Growth:** Professional advancement for team members with expanded skill sets

By partnering with INE, organizations transform siloed teams into an integrated force capable of addressing today's complex technical challenges - reducing costs, improving security, and building stronger technical teams.

Schedule Your Team Pilot with INE

learn.ine.com/schedule-a-demo



About INE

INE is a leading provider of online cybersecurity education, offering a comprehensive suite of hands-on courses and certification programs designed to meet the needs of professionals at all levels. INE is the top training choice for Fortune 500 companies worldwide for cybersecurity training in business and for IS/IT professionals looking to advance their careers. With a global community of learners, INE equips individuals and organizations with the skills necessary to defend against and combat modern cyber threats, offering a wide range of security certifications to build and elevate cybersecurity careers.