Administrative Staff: The First Line of Defense in Information Security

Developing Public Administrative Staff Competencies
VIS!T - Linz | 05.11.2025

National Agency for Information System Security (ANSSI)

Dr. Fatima Ezzahra El Orche

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Outline

- Introduction
- The Central Role of the Public Administrative Stuff
- Core Competencies to Develop
- Implementation of a Skills Development Plan
- Conclusion

Introduction – Digital Transformation and Complexity

Public administrations are rapidly evolving through digital innovation:

- Online services, automation, cloud, and artificial intelligence.
- Greater data interconnectivity and faster workflows.

Yet with innovation comes **greater exposure:** the digital ecosystem is more **interdependent and vulnerable** than ever.

“Every digital advance expands both our possibilities and our attack surface. ”

Introduction – Emerging Complex Threats

The threat landscape is no longer limited to traditional cyberattacks:

- **Hybrid Attacks** combining technical and psychological manipulation.
- **Disinformation** undermining trust in institutions.
- **Insider threats or accidental leaks** caused by human error.
- **Etc.**

These complex threats demand not only technical defenses but also **human vigilance and competence**.

The Human Factor in Resilience

Technology can defend, but people decide.

Human awareness and behavior determine the real level of protection

- 80% of incidents still involve a human element.
- Empowering staff = strengthening resilience.
- Security culture must be **embedded at every organizational level**.

“Security begins with people, not firewalls.”

The Central Role of Administrative Staff

Administrative personnel are often the backbone of public operations.

They:

- ➢ Handle sensitive data (HR, finance, citizen records).
- ➢ Manage critical processes (procurement, communication, archiving).
- ➢ Interface daily with internal and external partners.

Their actions directly affect **data confidentiality, integrity, and availability,** the pillars of information security.

Why They Are the First Line of Defense

Administrative are:

- **The first to be targeted** (phishing, social engineering, fake invoices).
- **The first to detect anomalies** in every workflows.
- **The first to act** when something seems wrong.

Empowering them transforms passive users into **active defenders** of organizational security.

“The front office is also the front line.”

Core Competencies to Develop

To make this defense effective, staff need a foundation of **digital, technical, and behavioral competencies.**

Digital and Cyber Awareness

Secure Use of tools

Critical and Behavioral Skills

Digital and Cyber Awareness

- **Understanding basic information security principles.** Every staff member should grasp key security concepts, confidentiality, integrity, and availability, and understand how they apply in daily tasks. This foundation builds awareness of why rules and protective measures matter.

- **Recognizing suspicious emails, attachement, and messages.** Phishing remains a top threat. Employees must learn to spot red flags such as unusual senders, urgent requests, or strange links, and report them immediately.

- **Maintaining strong passwords and secure habits.** Use unique, complex passwords with multi-factor authentication and avoid reusing credentials. Simple habits — locking screens, updating software, handling data carefully — protect against most common attacks.

Secure Use of tools

- **Proper use of document-sharing and collaboration platforms.** Use official, secure platforms for sharing and storing documents. Avoid unapproved tools to ensure sensitive information remains protected and traceable.

- **Data classification and secure storage.** Always handle information according to its sensitivity. Classify, store, and share data securely to prevent unauthorized access or accidental disclosure.

- **Awareness of privacy and compliance frameworks.** Understand and follow privacy rules and internal security policies. Responsible data handling protects both individuals and the organization.

Critical and Behavioral Skills

- **Thinking critically about information (mis/disinformation).** Question sources and verify facts before sharing. Critical thinking helps prevent the spread of false or manipulated information.

- **Knowing how to react and who to contact in case of a suspected breach.** Stay calm and follow established procedures in case of a suspected breach. Always know who to alert and how to report securely.

- **Confidence to report incidents promptly and responsibly.** Reporting early helps contain damage and protect others. A no-blame culture encourages staff to act quickly and transparently.

Implementing a Skills development Plan

Developing information security skills requires a long-term approach that combines regular training, practical exercises, and role-based learning. Consistency ensures that awareness turns into lasting habits and real resilience across the organization.

More concretely, this relies on coordinated efforts across :

Training and Awareness

Organizational Integration

Cooperation and Recognition

Training and Awareness

- **Regular, mandatory training adapted to each role.** Different roles face different risks. Mandatory, role-specific training ensures that every employee, from administrative staff to IT teams, understands the threats most relevant to their work and how to respond effectively.

- **Short, engaging sessions (e-learning, microlearning, phishing simulations).** Interactive formats make learning more effective and less time-consuming. Short sessions, realistic phishing exercises, and gamified modules keep users alert and help turn awareness into daily reflexes.

- **Ongoing communication through newsletters, posters, intranet reminders.** Awareness doesn't stop after training. Regular communication keeps cybersecurity visible and top-of-mind, reinforcing key messages and maintaining a culture of vigilance across the organization.

Organizational Integration

- **Integrate security practices into onboarding and daily procedures.** Security should be part of the organization’s DNA. Embedding best practices from day one and reinforcing them in daily routines helps make secure behavior automatic.

- **Promote a *no-blame culture* for incident reporting.** Encourage staff to report mistakes or incidents without fear. A transparent, supportive approach allows faster responses, better learning, and stronger collective resilience.

- **Recognize and reward good security behavior.** Positive reinforcement builds engagement. Acknowledging employees who follow best practices motivates others and turns security into a shared value, not a constraint.

Cooperation and Recognition

- **Support internal/external certification programs.** Encourage employees to pursue recognized certifications in cybersecurity. Certification builds credibility, reinforces expertise, and aligns skills with national and international standards.

- **Share best practices between administrations.** Foster collaboration through knowledge exchange and peer learning. Sharing successes and lessons learned strengthens collective resilience across the public sector.

- **Participate in European initiatives to harmonize skill frameworks.** Engage in European-level efforts to align cybersecurity skills and training standards. Cooperation ensures consistency, mutual recognition, and stronger collective defense.

Building a Security Culture

Thecnical security is only as strong as the people who apply it.

A resilient organization must :

- **Values awareness as much as expertise.**
- **Encourages open dialogue about risks.**
- **Embeds cybersecurity in its daily culture and decision-making.**

Conclusion

A trained, aware, and empowered administrative staff transforms the organization's **weakest link** into its **strongest defense**.

"Every administrative agent is a guardian of trust and a defender of resilience."

Together, we build a safer, more confident digital public sector.

NOCH FRAGEN?