Career Connections: Ethics in Automated Security

What You Did Today Connects to Real Careers

You just designed security policies like a Privacy Officer!

What You Did Today

Today you designed governance policies for an AI security system. You decided what the AI should do automatically versus what requires human approval. You balanced security benefits against privacy concerns and discovered that there is no easy "right answer."

This is exactly what cybersecurity policy professionals do when organizations deploy AI systems.

The NICE Framework Work Role: Cybersecurity Policy and Planning

What Policy Planners Do

- **Design governance frameworks** for how AI systems operate
- **Balance competing concerns**: security, privacy, efficiency, fairness
- **Consult stakeholders** to understand different perspectives
- **Write policies** that guide technology decisions

Key Tasks You Practiced

What You Did	What Policy Teams Call It
Decided what AI can do automatically	Automation governance
Balanced security vs. privacy	Risk-benefit analysis
Considered different stakeholder views	Stakeholder engagement
Made decisions without perfect answers	Policy development
Heard the AI's perspective	Technology assessment

Related Careers

Privacy Officer: Ensures organizations protect personal information and comply with privacy laws like FERPA, HIPAA, GDPR.

Security Governance Specialist: Develops policies and procedures that guide security decisions across the organization.

Risk Analyst: Evaluates potential harms and benefits to help organizations make informed decisions.

Compliance Manager: Ensures security practices meet legal and regulatory requirements.

The Big Realization

Why This Matters for AI

The decisions you made today about what AI should do automatically versus when to ask humans first are decisions that organizations are making right now about their AI systems.

There are no easy answers. More automation means faster protection but also more mistakes. More human oversight means fewer errors but slower response times. Every choice involves trade-offs.

The skills you practiced today, including weighing options, considering multiple perspectives, and making decisions under uncertainty, are exactly what cybersecurity policy careers require.

How Policy Professionals Actually Govern AI

> **ℹ Industry Reality Check**
>
> Right now, organizations are wrestling with the exact questions you discussed today. Here is how policy professionals approach AI governance:
>
> | Your Activity | Real-World Practice |
> | --- | --- |
> | "Should AI block automatically?" | Security teams create detection rules specifying when automated blocking is safe versus when human review is required |
> | "What about false positives?" | Incident metrics track false positive rates, and policies adjust thresholds based on business impact |
> | "Who decides when AI is wrong?" | Governance boards include security, legal, HR, and business stakeholders who review AI decisions quarterly |
> | "How do we balance speed vs. accuracy?" | Risk frameworks define acceptable automation levels based on data sensitivity and potential harm |
>
> The key insight is that there is no universal "right answer" to AI governance. Organizations develop policies through stakeholder negotiation, pilot testing, and continuous adjustment, which is exactly the process you practiced today.
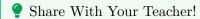>
> AI governance is one of the fastest-growing areas in cybersecurity. Companies need people who understand both the technical capabilities and the ethical implications.

Next Steps

Interested in learning more?

- **Explore NICE Framework**: niccs.cisa.gov/workforce-development/nice-framework (See "Oversight and Governance" roles)
- **Learn about AI governance**: AI policy is a growing field that combines technical and ethical thinking

- **Follow current events**: AI regulation (like the EU AI Act) is making headlines—policy skills are in demand

> **💡 Share With Your Teacher!**
>
> "Today I learned that Privacy Officers and Policy Planners design the rules for how AI systems operate. I practiced making hard decisions about automation and oversight—exactly what organizations are struggling with right now!"