**Why Every Program & Project Manager Should Consider Earning the CompTIA Security+ Certification**

Published on 25 February 2025 at 07:52

In today’s digital landscape, cybersecurity is no longer just an IT concern—it’s a **business-critical function** that affects project execution, risk management, and overall organizational success. As a **Program or Project Manager (PM),** understanding security principles is essential for leading successful projects, mitigating cyber risks, and ensuring compliance with industry regulations.

One way to strengthen your knowledge and credibility in this space is by earning the **CompTIA Security+ certification**. While Security+ is often pursued by IT professionals, **it can be a game-changer for PMs as well**. Here’s why.

A person looking down at a person

AI-generated content may be incorrect.

**1. Cybersecurity is a Core Business Risk**

Every program and project involves **data, technology, and security risks**—whether you’re deploying software, migrating systems to the cloud, or managing vendor contracts.

🔹 **Data breaches, ransomware attacks, and compliance failures** can derail projects, increase costs, and damage reputations.  
🔹 Security is no longer just IT’s responsibility—**PMs must factor cybersecurity into project planning, risk assessments, and execution.**  
🔹 Understanding security concepts **helps you ask the right questions** and proactively address vulnerabilities before they become major issues.

By earning Security+, you gain a **fundamental understanding of security best practices**, enabling you to incorporate cybersecurity considerations into your projects from day one.

**2. Security+ Helps PMs Bridge the Gap Between IT & Business**

One of the biggest challenges in tech-driven projects is **communication between IT teams and business stakeholders**. Security is often viewed as a **technical function**, but in reality, it requires **cross-functional collaboration**.

As a PM with Security+ knowledge, you can:  
✔ **Effectively communicate cybersecurity requirements** to non-technical stakeholders.  
✔ **Understand security controls** that impact system design, development, and implementation.  
✔ **Ensure compliance with industry standards** (NIST, ISO 27001, GDPR, HIPAA, etc.).  
✔ **Facilitate risk-based decision-making** that balances security, cost, and business objectives.

By earning Security+, **you become a more valuable liaison between business and IT**—a crucial skill in today’s security-conscious world.

**3. Security+ Enhances Your Risk Management Expertise**

Risk management is **a core competency of both program/project management and cybersecurity**. Security+ teaches you:  
✅ **Threat identification** – Understanding different attack types (phishing, malware, insider threats, etc.).  
✅ **Risk assessment frameworks** – Applying structured approaches to mitigate risks.  
✅ **Incident response planning** – Knowing how to react when security incidents impact project timelines.  
✅ **Compliance and governance** – Ensuring your projects adhere to security regulations and industry standards.

As a PM, you’re already skilled at managing risks—Security+ gives you the **cybersecurity lens** needed to apply that expertise to today’s evolving digital threats.

**4. Competitive Advantage: More Career Opportunities & Higher Earning Potential**

Cybersecurity is one of the **fastest-growing industries**, and companies increasingly seek **PMs who understand security**. Adding Security+ to your credentials can:  
🚀 **Differentiate you from other PMs** competing for roles in IT, software development, or digital transformation projects.  
🚀 **Qualify you for cybersecurity-related PM roles**—such as **Cybersecurity Project Manager** or **Governance, Risk & Compliance (GRC) Manager**.  
🚀 **Increase your earning potential**, as PMs with security expertise often command higher salaries.

In industries like **finance, healthcare, government, and cloud computing**, security knowledge is not just preferred—it’s required.

**5. Security+ is a Stepping Stone for Advanced Certifications**

If you’re interested in diving deeper into **cybersecurity project management**, Security+ provides a solid foundation for advanced certifications like:  
🔹 **CISSP (Certified Information Systems Security Professional)** – Best for senior-level security leadership roles.  
🔹 **CISM (Certified Information Security Manager)** – Focuses on risk management and governance.  
🔹 **CRISC (Certified in Risk and Information Systems Control)** – Ideal for those managing IT and security risks.  
🔹 **PMI-RMP (Risk Management Professional)** – Focuses on broader enterprise risk, including cybersecurity.

Whether you want to specialize in **cybersecurity project management** or just improve your ability to manage tech-driven projects, Security+ is a valuable stepping stone.

**Final Thoughts: Should a PM Get Security+?**

If you manage **IT projects, cloud migrations, application development, or digital transformation initiatives**, then **YES**—Security+ can **enhance your expertise, improve risk management, and make you a stronger leader**.

💡 **Cybersecurity is no longer optional—it’s a critical business function that PMs must understand.** By earning Security+, you position yourself as a well-rounded professional capable of leading secure, compliant, and successful projects in today’s digital economy.

👉 **What do you think?** Should more PMs pursue cybersecurity certifications? Let’s discuss!

💬👇 #CyberSecurity #SecurityPlus #ProjectManagement #RiskManagement #Leadership