IT DOESN'T HURT TO ASK…

An MIT xPro Guide to Discussing Professional Development with Your Employer

HOW TO USE THIS GUIDE

1. Take a look at the **Cybersecurity for Technical Leaders** course page. Note which topics and learning outcomes align with your company and team goals.

3. Customize the yellow areas highlighted in the email template on page four of this guide and send the email to your manager.

2. Review the "Why Learn Cybersecurity Now" section on page two of this guide and "Common Objections" on page three to help you develop an email for your manager or initiate a conversation with them.

4. Need any other information about the course that might help your case? Email us at xpro@mit.edu.

WHY LEARN CYBERSECURITY NOW

Bring these facts and figures into the conversation.

> In 2024, the global average cost of a data breach was $4.88 million. **(Source)**

> 95% of IT leaders agree that cyberattacks have reached unprecedented levels of sophistication. **(Source)**

> 87% of businesses reported at least one AI-powered cyber attack in the last year. **(Source)**

> 71% of cyber leaders believe small organizations can no longer adequately defend against today's complex cyber threats. **(Source)**

> 55% of organizations don't have a clear strategy in place to defend against AI-powered cyber threats. **(Source)**

> Two out of three organizations face moderate to critical shortages in essential cybersecurity talent. **(Source)**

> Only 14% of organizations feel confident they have the people and skills to meet today's cybersecurity demands. **(Source)**

COMMON OBJECTIONS

Your employer will have questions. Let's help you answer them.

OBJECTION	RESPONSE
"It costs too much."	It might cost more to neglect workforce training. Companies that prioritize employee development make a median revenue of $169,100 per employee, while companies that don't make less than half of that: $82,800. **(Source)**
"It will take you too much time and distract you from your work."	The course is designed for professionals, with an estimated time commitment of 4-6 hours per week for only 8 weeks. Learning a new skill does take time, but the format is flexible, allowing learners the ability to watch lectures, read case studies, and practice new technologies on their own schedule. Plus, the time a company invests in training will save them in the long run. A study by the National Center on the Educational Quality of the Workforce (EQW) supports this, finding that a 10% increase in educational development produced an 8.6% gain in productivity. **(Source)**
"How is this different from those other online courses?"	MIT xPRO courses are created and taught by MIT faculty and are optimized for learners who are full-time working professionals. The cybersecurity course leverages industry case studies, hands-on projects, and the latest thinking from 13 faculty members from MIT's Computer Science and Artificial Intelligence Lab (CSAIL) to equip learners with the knowledge and skills necessary to confidently navigate today's complex cybersecurity landscape.

EMAIL TEMPLATE

Copy and paste the following text into an email to your manager or HR professional.

Hi [Manager's Name],

I would like to submit a request for professional development through the Massachusetts Institute of Technology's online course, **Cybersecurity for Technical Leaders**. This eight-week online course offers training that I believe is directly relevant and beneficial to what we're trying to accomplish within [Our Company Name].

The course leverages industry case studies, hands-on projects, and the latest thinking from 13 faculty members from MIT's Computer Science and Artificial Intelligence Lab (CSAIL) to equip learners with the knowledge and skills necessary to confidently navigate today's complex cybersecurity landscape.

Here's a brief summary of what I will take away from the course:

- Gain the necessary skills to assess cloud security strategy and design architectures aligned with attainable objectives.

- Prioritize transformative growth by establishing a well-organized, standardized approach to securing hardware, software, and systems.

- Develop a visionary mindset and the aptitude to devise a cohesive strategy that adapts to the dynamic cybersecurity landscape.

- Assess how Large Language Models (LLMs) impact cybersecurity, identifying potential vulnerabilities and proposing mitigation strategies.

- Devise stable and sustainable solutions by interpreting data governance practices that prioritize privacy and security throughout the organization.

- Drive meaningful change in the evolving field of cybersecurity.

The course costs $2,850 and starts on [Start Date]. It is designed for full-time working professionals, so the schedule will not interfere with my current position.

For more information, visit: [link to course page]

Thank you for considering my training request,

[Your Name]