Sample Training Request Letter

Use the following sample request letter, or elements of it, to justify the time and budget required to complete SANS training to your manager. Simply copy and paste text into an email to your manager, then make any necessary adjustments to personalize the information. Once you hit send, you’ll be one step closer to gaining the skills required to protect your organization and advance your career.

**Subject: Request for cybersecurity training from SANS Institute**

[Decision Maker Name],

### I’m writing to request time and budget approval to take the SANS Institute’s information security course [LDR553: Cyber Incident Management](https://www.sans.org/cyber-security-courses/cyber-incident-management-training/).

**Why we need this course?**

If you are worried about leading or supporting a major cyber incident, then this is the course for you. We look at all the common and major cyber incident types and explain what the key issues are and how plan a recovery. This cyber incident management training course focuses on the challenges facing leaders and incident commanders as they work to bring enterprise networks back online and get business moving again. Whilst you may have a full team of technical staff standing-by to find, understand and remove the attackers, they need information, tasking, managing, supporting, and listening to so you can maximize their utilization and effectiveness. We focus on building a team to remediate the incident, on managing that team, on distilling the critical data for briefing, and how to run that briefing. We look at communication at all levels from the hands-on team to the executives and Board, investigative journalists, and even the attackers.

**Once I’ve completed the course, I’ll be able to:**

* Categorize and scope incidents correctly and the resulting incident management team’s objectives
* Design, draft, proof, release and control all communications when managing a serious incident
* Manage a team under extreme pressure and to recognize the natural human responses that will emerge and what they mean
* Lead the team, win the confidence of the execs and exceed the expectations of everyone involved
* Calculate, coordinate, and execute both system and data counter compromise activities
* Strategize and respond to ransomware incidents including how to develop exercises and training around these devastating attacks
* Structure, manage, and deliver briefings to the team, execs and senior leadership or the board
* Organize the transition from active incident to business as usual and how to execute that plan
* Prepare, setup and run cyber incident management exercises

**Which translate into business benefits for our company of:**

* Cultivate a workforce adept at leading or contributing to cyber incident management teams.
* Streamline incident management processes for quicker resolutions.
* Identify and bridge gaps in security incident plans and response strategies.
* Elevate the performance of security incident teams to meet evolving challenges.
* Strategically plan and navigate through high-stakes attacks, including email compromise and ransomware, fostering a resilient response frameworks
* Promote seamless collaboration between technical and non-technical teams during incident response for a more integrated approach.
* Instill a culture of continuous improvement, leveraging lessons learned from incidents to refine future response strategies.
* Proactively integrate threat intelligence to anticipate and mitigate potential threats before escalation.
* Provide guidance on regulatory compliance and have an awareness of legal considerations, ensuring incident responses align with relevant laws and standards

**Expected Cost**

I’d like to take LDR553 [fill in either: (1) “at [event name], from [start date] through [end date].” or (2) “online, with four months of access to the SANS OnDemand training platform.” or (3) “online, via Live Online from [start date] through [end date].”].

The attached unpaid invoice shows the cost of the course [retrieve this from the course registration page and attach]. Details include:

|  |  |
| --- | --- |
| Course fee  | [$X,XXX] |
| Subtract Early Bird / Online Training Discount | [-$XXX] |
| OnDemand Bundle fee | [$XXX] |
| Travel and Hotel\* (for live training only)                            | [$XXX] |
| Meals (for live training only)                                                                     | [$XXX] |
| **Total estimated cost:** | **[$X,XXX]** |

\*Special hotel rates for conference attendees range from [$XXX]/night, but I must register before [xx/xx/xxxx].

**Testimonials**

**"Probably the most important part to an organization - how to get their operation functioning again and sorted out with the structure and governance to cover the areas."***- Peter Leonhardt*

**The hands-on experiences and assignments have been exceptional and have significantly contributed to my learning experience.”** – Ben Radford, Law and Order

**"Brilliant insight. Excellent content. An absolute must course for anyone dealing with incident management."** *- Gary Smith*

I believe this course will substantially improve my ability to do the specific work we need. It’s written and taught by globally recognized experts and will deliver practical, hands-on training that I can apply as soon as I return to work.

Additional course information can be found on the SANS website at <https://www.sans.org/cyber-security-courses/cyber-incident-management-training/>

Thanks for your consideration,

[Add standard signature]

Attachment:

Unpaid Invoice for SANS training [find at <https://www.sans.org/cyber-security-courses/cyber-incident-management-training/> and attach to email]