Supply Chain Cybersecurity & Vendor Risk Management Training Course

Ref: #CYB9685

Course Introduction / Overview:

This comprehensive training course is designed to provide cybersecurity, procurement, and risk management professionals with the essential knowledge and skills needed to secure the supply chain. In today's interconnected global economy, a single weak link in a vendor's security posture can expose an entire organization to catastrophic cyber threats, such as data breaches and operational disruptions. This program goes beyond traditional cybersecurity to focus specifically on the unique challenges of vendor risk management. Participants will learn how to identify, assess, and mitigate risks posed by third-party suppliers, from software vendors to hardware manufacturers. We will cover key topics like threat intelligence, vendor auditing, and contract negotiations from a security perspective. Drawing from the academic research of renowned authors such as Professor Robert W. Handfield, a leading expert on supply chain management, and his co-authored book "Supply Chain Redesign: Transforming Supply Chains into Integrated Value Systems," this program provides a strategic and practical framework for safeguarding your supply chain. This course at BIG BEN Training Center will empower you to build a resilient and secure supply chain.

Target Audience / This training course is suitable for:

- Cybersecurity professionals.
- Supply chain managers.
- Procurement and sourcing specialists.
- IT risk and compliance officers.
- IT auditors.
- Third-party risk managers.
- Legal professionals.

Target Sectors and Industries:

- Manufacturing.
- Defense and aerospace.
- Financial services.
- Retail and e-commerce.
- Technology and software development.
- Government agencies and equivalents.
- Healthcare.

Target Organizations Departments:

- Supply Chain Management.
- Information Security.
- Procurement.
- Risk Management.
- Legal and Compliance.
- IT Audit.
- Operations.

Course Offerings:

By the end of this course, the participants will have able to:

- Assess cybersecurity risks posed by vendors.
- Develop and implement a third-party risk management program.
- Conduct effective security audits of suppliers.
- Negotiate security clauses in vendor contracts.
- Utilize threat intelligence to monitor supply chain risks.
- Respond to and recover from a supply chain cyber-attack.
- Establish a continuous monitoring program for vendors.

Course Methodology:

This training course at BIG BEN Training Center uses a highly practical and case-study-driven methodology. The program combines expert-led sessions with a series of real-world scenarios, such as a simulated supply chain attack on a major retailer. Participants will engage in hands-on activities, including developing a vendor risk assessment questionnaire and analyzing a vendor's security posture. The course emphasizes a collaborative approach, encouraging teams to work together to identify vulnerabilities and propose mitigation strategies. The instructor will provide feedback and lead discussions on best practices, ensuring that participants can apply their skills to their own organizational context. This approach ensures you will leave with the skills and strategic knowledge to build a secure and resilient supply chain.

Course Agenda (Course Units):

Unit One: Fundamentals of Supply Chain Cybersecurity

- The supply chain is a security risk vector.
- Common attack types (e.g., software supply chain attacks).
- The SolarWinds case study and its lessons.
- The need for a proactive security approach.
- Threat intelligence for vendor management.
- Regulatory drivers for supply chain security.
- The role of trust in the supply chain.

Unit Two: Vendor Risk Management Frameworks

- Building a vendor risk management (VRM) program.
- Identifying and classifying vendors by risk level.
- Developing a risk assessment questionnaire.
- Onboarding and offboarding vendors securely.
- Contractual clauses for cybersecurity.
- The importance of service level agreements (SLAs).
- Practical lab: creating a vendor risk questionnaire.

Unit Three: Conducting Vendor Security Audits

- Preparing for a vendor audit.
- On-site vs. remote audits.
- Key areas to audit (e.g., physical security, network controls).
- Analyzing audit results and identifying gaps.
- The role of third-party assessments and certifications.
- Continuous monitoring of vendor security posture.
- Case study: a vendor security audit scenario.

Unit Four: Software Supply Chain Security

- Software Supply Chain Security.
- Securing the software development lifecycle.
- Vulnerability scanning and penetration testing.
- The role of secure coding practices.
- Protecting intellectual property.
- Managing open-source software risks.
- Practical lab: a software vulnerability analysis.

Unit Five: Incident Response and Future Trends

- Developing an incident response plan for supply chain attacks.
- Communicating with vendors during a breach.
- Forensic investigation in a supply chain context.
- Future trends in supply chain security.
- The role of AI and machine learning.
- Final project: a comprehensive supply chain security plan.
- Emerging risks.
- Frequently Asked Questions:

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

With an increasingly globalized and interconnected supply chain, how can organizations ensure the security and integrity of their products and services when vendors are operating in jurisdictions with different legal and security standards?

What unique qualities does this course offer compared to other courses?

This course stands out by providing a unique and vital focus on the intersection of supply chain management and cybersecurity. While many cybersecurity programs focus on internal network defense, this program addresses the critical and often-overlooked risks posed by third-party vendors. The curriculum is specifically designed to bridge the gap between IT security, procurement, and risk management. It gives you the skills to not only identify threats but also to develop a strategic framework for managing vendor relationships and contractual agreements from a security perspective. The use of real-world case studies and practical exercises ensures that you will gain an actionable understanding of how to protect your organization's digital assets from external threats. This course is for professionals who recognize that the modern security perimeter extends far beyond the walls of their own organization.