1. | | |
|---|---|
| Record Nr. | UNINA9910270881303321 |
| Autore | Antonucci Domenic |
| Titolo | The cyber risk handbook : creating and measuring effective cybersecurity capabilities / / Domenic Antonucci |
| Pubbl/distr/stampa | Hoboken, New Jersey : , : Wiley, , 2017
©2017 |
| ISBN | 1-119-30972-7
1-119-30895-X
1-119-30974-3 |
| Edizione | [1st edition] |
| Descrizione fisica | 1 online resource (451 pages) |
| Collana | Wiley Finance
THEi Wiley ebooks |
| Disciplina | 364.168 |
| Soggetti | Computer crimes
Cyberspace - Security measures |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Introduction -- Board cyber risk oversight -- Principles behind cyber risk management -- Cybersecurity policies and procedures -- Cyber strategic performance management -- Standards and frameworks for cybersecurity -- Identifying, analyzing, and evaluating cyber risks -- Treating cyber risks -- Treating cyber risks using process capabilities -- Treating cyber risks - using insurance and finance -- Monitoring and review using key risk indicators (KRIs) -- Cybersecurity incident and crisis management -- Business continuity management and cybersecurity -- External context and supply chain -- Internal organization context -- Culture and human factors -- Legal and compliance -- Assurance and cyber risk management -- Information asset management for cyber -- Physical security -- Cybersecurity for operations and communications -- Access control -- Cybersecurity systems: acquisition, development, and maintenance -- People risk management in the digital age -- Cyber competencies and the cybersecurity officer --Human resources security -- Epilogue. |
| Sommario/riassunto | Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to |

implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.