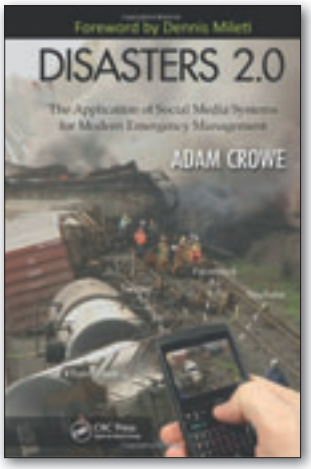
Aktuální normy a publikace o bezpečnosti

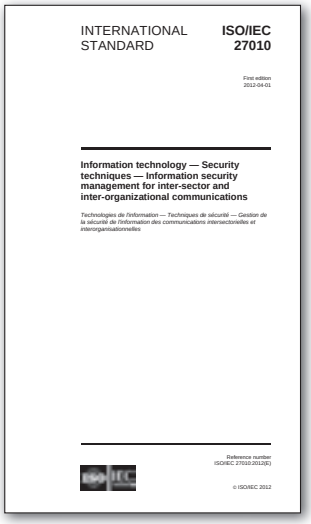
Krizové řízení a sociální média



Publikace *Disasters 2.0: The Application of Social Media Systems for Modern Emergency Management* připraví vedoucí krizových štábů a ostatní co stojí v první linii odezvy na to, jak úspěšně a efektivně využít možností sociálních médií při zvládání mimořádných událostí. Každá kapitola knihy se věnuje jednomu z aspektů sociálních médií, který je využitelný při krizové situaci. Jednou z efektivních možností při získávání informací a různých pohledů na určitou událost je využití tzv. crowdsourcingu (využívání mas jako zdroje informací o dané události), kterou umožňují dnešní technologie web 2.0. Kromě klasické knihy je také k dispozici verze určená pro čtečky Kindle.

http://www.crcpress.com/

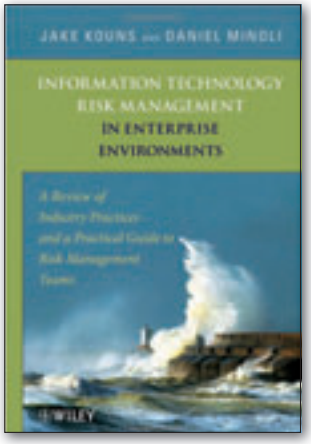
Bezpečnost sdílených informací



Prvním letošním přírůstkem do rodiny norem ISO 27k je ISO/IEC 27010:2012 Information technology – Security techniques – *Information security management for inter-sector and inter-organisational communications*. Norma poskytuje opatření a best practice pro organizace, které čas od času potřebují sdílet citlivé firemní informace s jinými organizacemi (např. při šetření bezpečnostních incidentů) a hledají doporučení, jak zajistit jejich bezpečnost. Zatímco ISO/IEC 27001:2005 a ISO/IEC 27002:2005 se věnují bezpečnostním opatřením při výměně informací mezi organizacemi jen v obecné rovině, tak ISO/IEC 27010 na tato doporučení navazuje a dále je rozšiřuje. Norma drží strukturu ISO/IEC 27002.

http://www.iso.org/

Metodiky a standardy řízení rizik

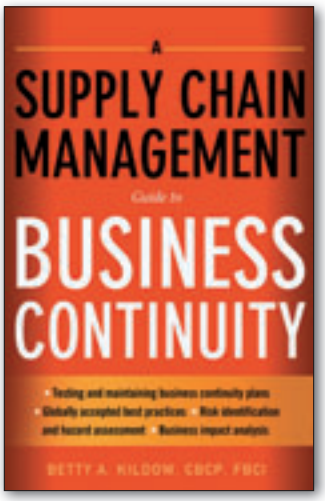


Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams je vyčerpávajícím zdrojem praktických doporučení a přístupů k řízení rizik napříč jednotlivými odvětvími. Klíčové pojmy a metody jsou vždy podrobně vysvětleny a pro ilustraci často dokresleny na příkladech z praxe, doplněny o tabulky, diagramy a grafy. Kniha obsahuje detailní přehled existujících standardů pro řízení rizik. Výborným zdrojem informací je také kapitola, která se věnuje méně či více známým metodikám a nástrojům pro řízení rizik (např. OCTAVE, MEHARI, CRAMM apod.).

http:// www.wiley.com /

Ing. Libor Široký, CISM, CRISC, *siroky@rac.cz*

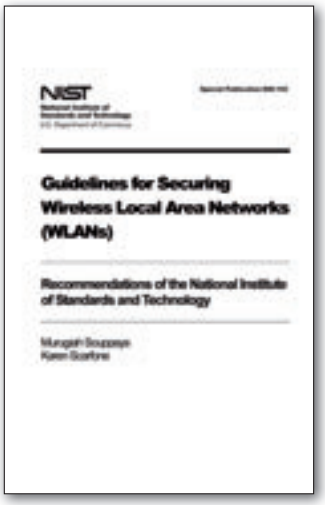
BCM v dodavatelských řetězcích



Dnešní společnosti jsou čím dál více závislé na externích dodavatelích. V řadě případů existuje jen jeden dodavatel u těch nejkritičtějších položek, jejichž výpadek může narušit, v horším případě zcela přerušit klíčové firemní procesy. Kniha *A Supply Chain Management Guide to Business Continuity* je cílena přesně na tyto případy a společnosti. Autorce (Betty A. Kildow) se podařilo rozšířit principy řízení kontinuity činností (business continuity management) o požadavky směřující na řízení dodavatelských řetězců (supply chain management). Jedním z klíčových kroků je identifikace kritických položek a následků spojených s výpadky výhradních dodavatelů.

http://www.amacombooks.org/

Bezpečnost bezdrátových sítí



SP 800-153 *Guidelines for Securing Wireless Local Area Networks* je standard z dílny amerického Národního institutu pro standardy a technologii (National Institute of Standards and Technology, NIST). Účelem normy je poskytnout organizacím doporučení a metody pro zabezpečení bezdrátových sítí a zařízení k nim připojeným. Věnuje se konfiguraci a architektuře WiFi sítí. Dává doporučení ohledně monitorování jejich provozu a zabezpečení (aktivní vyhledávání zranitelností, blokování neoprávněných přístupů a další). Na rozdíl od mezinárodních standardů ISO jsou standardy NIST volně ke stažení na webových stránkách Computer Security Resource Center.

http://csrc.nist.gov/publications/

Hrozba zevnitř

Stále aktuálnějším tématem posledních let je zabezpečení proti hrozbám pocházejícím z řad vlastních zaměstnanců. Autor květnové novinky *Managing the Insider Threat: No Dark Corners* na základě různých sociálních průzkumů dokládá, proč klasické metody obrany selhávají v případě vnitřních škůdců. Věnuje se různým technikám prověřování zaměstnanců (např. psychologické profilování), detekčním a prevenčním mechanizmům k včasnému odhalení potenciálních vnitřních škůdců a opatřením, které pomohou snížit pravděpodobnost úspěchu hrozby zevnitř. Autor navrhuje, jak nastavit a implementovat vhodné strategie efektivního a úspěšného boje proti vnitřnímu nepříteli.

http://www.crcpress.com/