1. Record Nr. UNINA9910140870303321

Autore	Howard Doug
Titolo	Security 2020 [[electronic resource]] : reduce security risks this decade / / Doug Howard and Kevin Prince
Pubbl/distr/stampa	Indianapolis, Ind., : Wiley Pub., c2011
ISBN	1-282-94413-4 9786612944130 1-118-25580-1 1-118-00831-6 1-118-00833-2
Edizione	[1st ed.]
Descrizione fisica	1 online resource (338 p.)
Altri autori (Persone)	PrinceKevin
Disciplina	005.8
Soggetti	Computer security Computer security - Forecasting
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Security 2020; Contents; Foreword; Introduction; Chapter 1 What Has History Shown Us?; The History of Data Breach Disclosure; The History of Vulnerability Exploits; The History of Viruses and Worms; The History of Edge-Based Security; The History of Patching; Hacker Methodologies; Inbound Attacks; The History of Malware; Automated Attacks; The History of Hacker Motivation; The History of Botnets; The History of Search Engine Hacking; The History of Data Loss; The History of Security Solutions; The Making of a Cyber-Super-Villain; The Botnet in Action; Hindsight is NOT 20/20 Chapter 2 External Influences on Security Information Security Drivers; The Emotions; World Events; The Impact of Politics; The Impact on Journalism; The Social Engineer; GRC; Litigation; Breach Impact on Public Companies; The Security Culture; The Path to 2020; Chapter 3 Technology Influences on Security; The Movement Toward National Identity Management; Internet Protocol in 2020; 2020: Remote Access Continues to Be a Problem; The Search Engine Impact; The Web Services Impact; The Impact of Virtualization; The Malware Problem; The Web Browser; The Portable Media Debacle, A.K.A. Mobility

Advanced Persistent Threat in 2020 The Network Edge; The Security Software Vendor; Personal Information and Data Correlation; The Domain Name; Chapter 4 Where Security Threats Will Come from in the Future; Spam; Botnets; The Ph-enomenon: Why so many attack methods start with "Ph"; Phishing, Pharming, SMSishing, Vishing; Vulnerability Exploits; Insider Threats; Mobility Threats; Infected Software; Peer-to-Peer (P2P) Software; Third-Party Threats; Social Networking Threats; Digitization; Star Wars; Infrastructure Attacks; Social and Financial Threats; Website Middleware Threats Doppelganger Attacks Chapter 5 Secure Communications and Collaboration; Email, Instant Messaging, and SMS; Online Webinars and Collaboration Tools; Voice over IP; Video over IP; Storage and Retention of User-Generated Content; Digital Rights Management and Content Protection; Digital Rights Management; Watermarking; UCC and UCC Compliance Requirements over the Next Decade; Chapter 6 2020 Revolution or Evolution?; IT Security Revolution; The Missing Deterrent; Security in 20/20 Hindsight; Intrusion Detection Systems, Intrusion Protection Systems, and Data Loss Prevention in 20/20 Hindsight Identity Management/Network Access Control/Single Sign-on Mobility/Wireless/Ultra-Mobile; SaaS and Cloud Computing; Testing Your Information Protection: Penetration Test/Vulnerability Test/Risk Assessments; Chapter 7 Security as a Business Now and Then; The Purpose of IT; Evolving Purpose into Action; The Map to Success; The Relationship: Security and Luck; Security: An Industry or a Feature of IT?; Consolidation of the IT Security Industry; Buying Security: Defining the Value; Budgets and Prioritizations; Venture Capital and Investment in IT Security
Chapter 8 Impact of the Economy over the Next 10 Years

Sommario/riassunto

Identify real security risks and skip the hype After years of focusing on IT security, we find that hackers are as active and effective as ever. This book gives application developers, networking and security professionals, those that create standards, and CIOs a straightforward look at the reality of today's IT security and a sobering forecast of what to expect in the next decade. It debunks the media hype and unnecessary concerns while focusing on the knowledge you need to combat and prioritize the actual risks of today and beyond.IT security needs are constantly evolving;