1. Record Nr. UNINA9910823165903321

| | |
|---|---|
| Autore | Touhill Gregory J. |
| Titolo | Cybersecurity for executives : a practical guide / / Gregory J. Touhill and C. Joseph Touhill |
| Pubbl/distr/stampa | Hoboken, New Jersey : , : John Wiley & Sons, Inc., , 2014<br>©2014 |
| ISBN | 1-118-90878-3<br>1-118-90881-3 |
| Descrizione fisica | 1 online resource (412 p.) |
| Disciplina | 658.4/78 |
| Soggetti | Computer networks - Security measures |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Description based upon print version of record. |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Cybersecurity for Executives: A Practical Guide; Contents; Foreword; Preface; Acknowledgments; 1.0 INTRODUCTION; 1.1 DEFINING CYBERSECURITY; 1.2 CYBERSECURITY IS A BUSINESS IMPERATIVE; 1.3 CYBERSECURITY IS AN EXECUTIVE-LEVEL CONCERN; 1.4 QUESTIONS TO ASK; 1.5 VIEWS OF OTHERS; 1.6 CYBERSECURITY IS A FULL-TIME ACTIVITY; 2.0 WHY BE CONCERNED?; 2.1 A CLASSIC HACK; 2.2 WHO WANTS YOUR FORTUNE?; 2.3 NATION-STATE THREATS; 2.3.1 China; 2.3.2 Don't Think that China is the Only One; 2.4 CYBERCRIME IS BIG BUSINESS; 2.4.1 Mercenary Hackers; 2.4.2 Hacktivists; 2.4.3 The Insider Threat<br>2.4.4 Substandard Products and Services2.5 SUMMARY; 3.0 MANAGING RISK; 3.1 WHO OWNS RISK IN YOUR BUSINESS?; 3.2 WHAT ARE YOUR RISKS?; 3.2.1 Threats to Your Intellectual Property and Trade Secrets; 3.2.2 Technical Risks; 3.2.3 Human Risks; 3.3 CALCULATING YOUR RISK; 3.3.1 Quantitative Risk Assessment; 3.3.2 Qualitative Risk Assessment; 3.3.3 Risk Decisions; 3.4 COMMUNICATING RISK; 3.4.1 Communicating Risk Internally; 3.4.2 Regulatory Communications; 3.4.3 Communicating with Shareholders; 3.5 ORGANIZING FOR SUCCESS; 3.5.1 Risk Management Committee; 3.5.2 Chief Risk Officers; 3.6 SUMMARY<br>4.0 BUILD YOUR STRATEGY4.1 HOW MUCH "CYBERSECURITY" DO I NEED?; 4.2 THE MECHANICS OF BUILDING YOUR STRATEGY; 4.2.1 Where |

Sommario/riassunto

Practical guide that can be used by executives to make well-informed decisions on cybersecurity issues to better protect their businessEmphasizes, in a direct and uncomplicated way, how executives can identify, understand, assess, and mitigate risks associated with cybersecurity issuesCovers 'What to Do When You Get Hacked?' including Business Continuity and Disaster Recovery planning, Public Relations, Legal and Regulatory issues, and Notifications and DisclosuresProvides steps for integrating cybersecurity into Strategy; Policy and Guidelines; Change Management and