

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 ©2014
ISBN	1-118-90878-3 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 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 4.0 BUILD YOUR STRATEGY4.1 HOW MUCH "CYBERSECURITY" DO I NEED?; 4.2 THE MECHANICS OF BUILDING YOUR STRATEGY; 4.2.1 Where

are We Now?; 4.2.2 What do We have to Work with?; 4.2.3 Where do We Want to be?; 4.2.4 How do We Get There?; 4.2.5 Goals and Objectives; 4.3 AVOIDING STRATEGY FAILURE; 4.3.1 Poor Plans, Poor Execution; 4.3.2 Lack of Communication; 4.3.3 Resistance to Change; 4.3.4 Lack of Leadership and Oversight; 4.4 WAYS TO INCORPORATE CYBERSECURITY INTO YOUR STRATEGY; 4.4.1 Identify the Information Critical to Your Business; 4.4.2 Make Cybersecurity Part of Your Culture 4.4.3 Consider Cybersecurity Impacts in Your Decisions 4.4.4 Measure Your Progress; 4.5 PLAN FOR SUCCESS; 4.6 SUMMARY; 5.0 Plan for Success; 5.1 TURNING VISION INTO REALITY; 5.1.1 Planning for Excellence; 5.1.2 A Plan of Action; 5.1.3 Doing Things; 5.2 POLICIES COMPLEMENT PLANS; 5.2.1 Great Cybersecurity Policies for Everyone; 5.2.2 Be Clear about Your Policies and Who Owns Them; 5.3 PROCEDURES IMPLEMENT PLANS; 5.4 EXERCISE YOUR PLANS; 5.5 LEGAL COMPLIANCE CONCERNs; 5.6 AUDITING; 5.7 SUMMARY; 6.0 CHANGE MANAGEMENT; 6.1 WHY MANAGING CHANGE IS IMPORTANT; 6.2 WHEN TO CHANGE? 6.3 WHAT IS IMPACTED BY CHANGE? 6.4 CHANGE MANAGEMENT AND INTERNAL CONTROLS; 6.5 CHANGE MANAGEMENT AS A PROCESS; 6.5.1 The Touhill Change Management Process; 6.5.2 Following the Process; 6.5.3 Have a Plan B, Plan C, and maybe a Plan D; 6.6 BEST PRACTICES IN CHANGE MANAGEMENT; 6.7 SUMMARY; 7.0 PERSONNEL MANAGEMENT; 7.1 FINDING THE RIGHT FIT; 7.2 CREATING THE TEAM; 7.2.1 Picking the Right Leaders; 7.2.2 Your Cybersecurity Leaders; 7.3 ESTABLISHING PERFORMANCE STANDARDS; 7.4 ORGANIZATIONAL CONSIDERATIONS; 7.5 TRAINING FOR SUCCESS; 7.5.1 Information Every Employee Ought to Know 7.5.2 Special Training for Executives

---

#### Sommario/riassunto

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

---